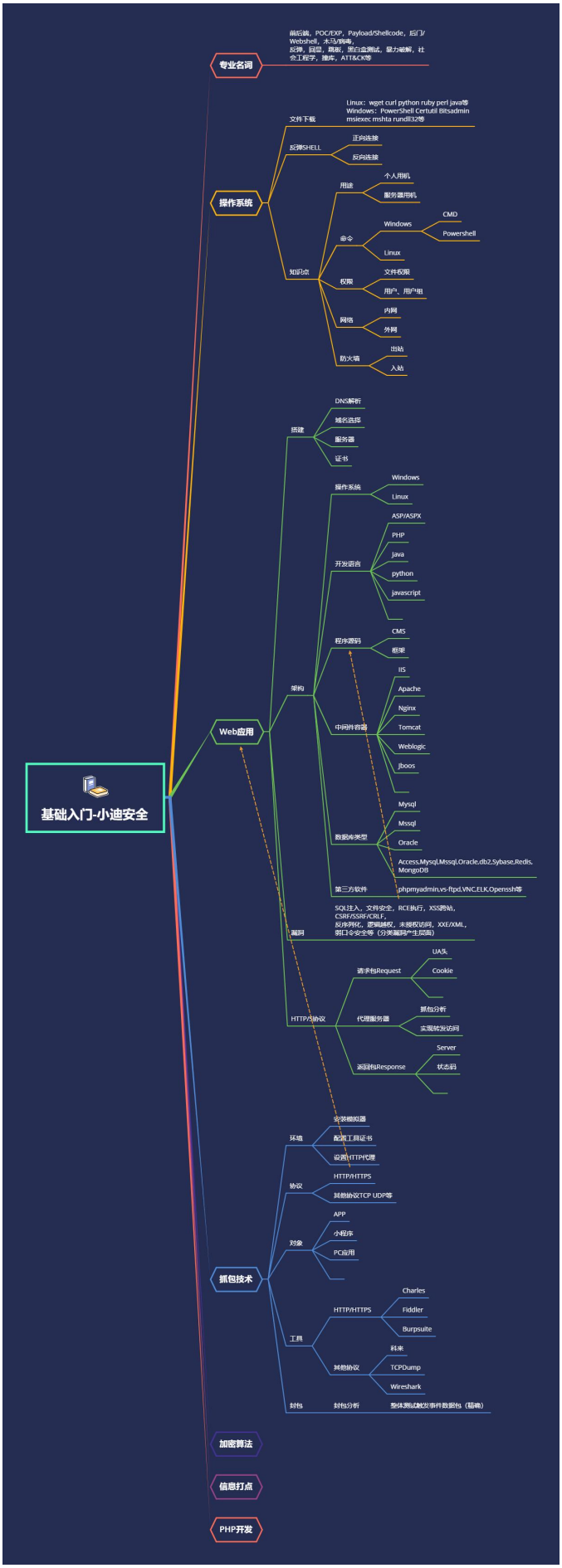
基础入门-30 余种加密编码进制&Web&数据库&系统&代码&参数值


基础入门-小迪安全
专业名词
前后端，POC/EXP，Payload/Shellcode，后门/Webshell，木马/病毒，
反弹，回显，靶场，黑白盒测试，暴力破解，社会工程学，指南，ATT&CK等
操作系统
文件下载
Linux：wget curl python ruby perl java等
Windows：PowerShell Certutil Bitsadmin msiexec mshta rundll32等
反弹SHELL
正向连接
反向连接
知识点
用途
个人用机
服务器用机
命令
Windows
CMD
Powershell
Linux
权限
文件权限
用户、用户组
网络
内网
外网
防火墙
出站
入站
Web应用
搭建
DNS解析
域名选择
服务器
证书
架构
操作系统
Windows
Linux
开发语言
ASP/ASPX
PHP
Java
python
javascript
程序源码
CMS
框架
中间件容器
IIS
Apache
Nginx
Tomcat
Weblogic
Jboos
数据库类型
Mysql
Mssql
Oracle
Access,Mysql,Mssql,Oracle,db2,Sybase,Redis,MongoDB
第三方软件
phpmyadmin,vs-ftpd,VNC,ELK,Openssh等
漏洞
SQL注入，文件安全，RCE执行，XSS跨站，CSRF/SSRF/CRLF，
反序列化，逻辑越权，未授权访问，XXE/XML，
命令安全等（分类漏洞产生层面）
HTTP/S协议
请求包Request
UA头
Cookie
代理服务器
抓包分析
实现转发访问
返回包Response
Server
状态码
抓包技术
环境
完美模拟器
配置工具证书
设置HTTP代理
协议
HTTP/HTTPS
其他协议TCP UDP等
对象
APP
小程序
PC应用
工具
HTTP/HTTPS
Charles
Fiddler
Burpsuite
其他协议
科来
TCPDump
Wireshark
封包
封包分析
整体测试触发事件数据包（精确）
加密算法
信息打点
PHP开发

#知识点：
存储密码加密-Web&数据库&系统
传输数据编码-各类组合传输参数值
代码特性加密-JS&PHP&NET&JAVA
数据显示编码-字符串数据显示编码

#本课意义：
1.了解加密编码进制在安全测试中的存在
2.掌握常见的加密解密编码解码进制互转的操作
3.了解常见的加密解密编码解密进制互转的影响
旨在解决类似疑问，提供思路：
你是否碰到不知道的加密方式？
你是否碰到无法找到的解密平台？
你是否碰到不知道如何解密的字符串？
你是否准备参加 CTF 比赛补充此类知识点？

#详细点：
密码存储加密：
MD5 SHA1 NTLM AES DES RC4
MD5 值是 32 或 16 位位由数字"0-9"和字母"a-f"所组成的字符串
SHA1 这种加密的密文特征跟 MD5 差不多，只不过位数是 40
NTLM 这种加密是 Windows 的哈希密码，标准通讯安全协议
AES,DES,RC4 这些都是非对称性加密算法，引入密钥，密文特征与 Base64 类似
应用场景：各类应用密文，自定义算法，代码分析，CTF 安全比赛等

传输数据编码：
BASE64 URL HEX ASCII
BASE64 值是由数字"0-9"和字母"a-f"所组成的字符串,大小写敏感,结尾通常有符号=
URL 编码是由数字"0-9"和字母"a-f"所组成的字符串,大小写敏感,通常以%数字字母间隔
HEX 编码是计算机中数据的一种表示方法,将数据进行十六进制转换,它由 0-9,A-F,组成
ASCII 编码是将 128 个字符进行进制数来表示,常见 ASCII 码表大小规则：0~9<A~Z<a~z
举例：
个人博客-URL 解码
国外 WEB-BASE64 解码
搜狐视频-BASE64 解码
应用场景：参数传递(如注入影响)，后期 WAF 绕过干扰写法应用，视频地址还原等

JS 前端代码加密：
JS 颜文字 jother JSFUCK
颜文字特征：一堆颜文字构成的 js 代码，在 F12 中可直接解密执行
jother 特征：只用! + ( ) [ ] { }这八个字符就能完成对任意字符串的编码。也可在 F12 中解密执行
JSFUCK 特征：与 jother 很像，只是少了{ }

后端代码加密：
PHP .NET JAVA

PHP：乱码，头部有信息
.NET：DLL 封装代码文件
JAVA：JAR&CLASS 文件
举例：Zend ILSpy IDEA
应用场景：版权代码加密，开发特性，CTF 比赛等

数据库密文加密：
MYSQL MSSQL 等

数据显示编码：
UTF-8 GBK2312 等

识别算法编码类型：
看密文位数
2、看密文的特征（数字，字母，大小写，符号等）
3、看当前密文存在的地方（Web，数据库，操作系统等应用）

演示案例：

- Web-ZZCMS-密文-MD5
- Web-Discuz-密文-MD5&Salt
- 系统-Windows-密文-NTLM&HASH
- 综合-参数-密文传输-AES&BASE64
- 代码-解密-解密反编译-Zend&Dll&Jar
- CTF 赛题-buuoj-single dog-JS 颜文字
- CTF 赛题-xuenixiang-Jsfuck-JSFUCK

#补充点：
1.常见加密编码进制等算法解析
MD5，SHA，ASC，进制，时间戳，URL，BASE64，Unescape，AES，DES 等
2.常见加密编码形式算法解析
直接加密，带 salt，带密码，带偏移，带位数，带模式，带干扰，自定义组合等
3.常见解密解码方式（针对）
枚举，自定义逆向算法，可逆向
4.常见加密解码算法的特性
长度位数，字符规律，代码分析，搜索获取等

#拓展补充参考资料：

部分资源：
https://www.cmd5.com
http://tmxk.org/jother
http://www.jsfuck.com
http://www.hiencode.com
http://tool.chacuo.net/cryptaes
https://utf-8.jp/public/aaencode.html

1.30 余种加密编码类型的密文特征分析（建议收藏）
https://mp.weixin.qq.com/s?__biz=MzAwNDcxMjI2MA==&mid=2247484455&idx=1&sn=e1b4324ddcf7d6123be30d9a5613e17b&chksm=9b26f60cac517f1a920cf3b73b3212a645aeef78882c47957b9f3c2135cb7ce051c73fe77bb2&mpshare=1&scene=23&srcid=1111auAYWmr1N0NAs9Wp2hGz&sharer_sharetime=1605145141579&sharer_shareid=5051b3eddbbe2cb698aedf9452370026#rd

2.CTF 中常见密码题解密网站总结（建议收藏）
https://blog.csdn.net/qq_41638851/article/details/100526839

3.CTF 密码学常见加密解密总结（建议收藏）
https://blog.csdn.net/qq_40837276/article/details/83080460

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
