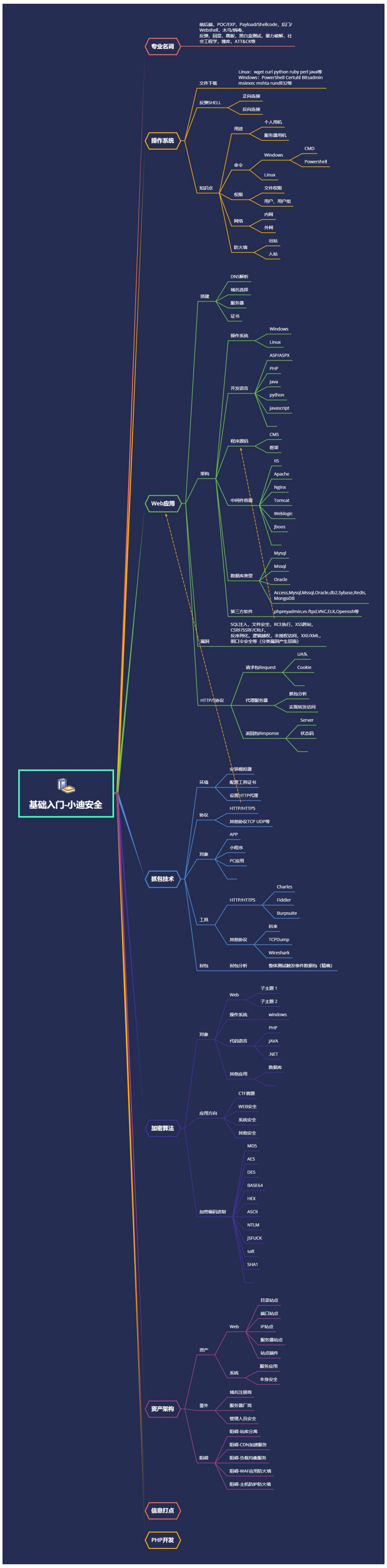
信息打点-资产泄漏&CMS 识别&Git 监控&SVN&DS_Store&备份


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，跳板，黑白盒测试，暴力破解，社会工程学，撞库，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，
弱口令安全等（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
安装模拟器
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
对象
Web
子主题 1
子主题 2
操作系统
windows
代码语言
PHP
JAVA
.NET
其他应用
数据库
应用方向
CTF赛题
WEB安全
系统安全
其他安全
加密编码进制
MD5
AES
DES
BASE64
HEX
ASCII
NTLM
JSFUCK
salt
SHA1
资产架构
资产
Web
目录站点
端口站点
IP站点
服务器站点
站点插件
系统
服务应用
本身安全
番外
域名注册商
服务器厂商
管理人员安全
阻碍
阻碍-站库分离
阻碍-CDN加速服务
阻碍-负载均衡服务
阻碍-WAF应用防火墙
阻碍-主机防护防火墙
信息打点
PHP开发

#知识点：
CMS 指纹识别源码获取方式
习惯&配置&特性等获取方式
3、托管资产平台资源搜索监控

#详细点：
参考：https://www.secpulse.com/archives/124398.html
源码泄漏原因：
1、从源码本身的特性入口
2、从管理员不好的习惯入口
3、从管理员不好的配置入口
4、从管理员不好的意识入口
5、从管理员资源信息搜集入口
源码泄漏集合：
composer.json
git 源码泄露
svn 源码泄露
hg 源码泄漏
网站备份压缩文件
WEB-INF/web.xml 泄露
DS_Store 文件泄露
SWP 文件泄露
CVS 泄露
Bzr 泄露
GitHub 源码泄漏

演示案例：

- 直接获取-CMS 识别-云悉指纹识别平台
- 习惯不好-备份文件-某黑阔博客源码泄漏
- 配置不当-GIT 泄漏-某程序员博客源码泄漏
- 配置不当-SVN 泄漏-某国外小伙子源码泄漏
- 配置不当-DS_Store 泄漏-某开发 Mac 源码泄漏
- PHP 特性-composer.json 泄漏-某直接搭建源码泄漏
- 下载配合-WEB-INF 泄露-RoarCTF-2019-EasyJava

➢ 资源监控-GITHUB 泄漏-语法搜索&关键字搜索&社工

相关利用项目：
CMS 识别：https://www.yunsee.cn/
备份：敏感目录文件扫描-7kbscan-WebPathBrute
CVS：https://github.com/kost/dvcs-ripper
GIT：https://github.com/lijiejie/GitHack
SVN：https://github.com/callmefeifei/SvnHack
DS_Store：https://github.com/lijiejie/ds_store_exp

GITHUB 资源搜索：
in:name test #仓库标题搜索含有关键字
in:descripton test #仓库描述搜索含有关键字
in:readme test #Readme 文件搜素含有关键字
stars:>3000 test #stars 数量大于 3000 的搜索关键字
stars:1000..3000 test #stars 数量大于 1000 小于 3000 的搜索关键字 forks:>1000 test #forks 数量大于 1000 的搜索关键字
forks:1000..3000 test #forks 数量大于 1000 小于 3000 的搜索关键字 size:>=5000 test #指定仓库大于 5000k(5M)的搜索关键字 pushed:>2019-02-12 test #发布时间大于 2019-02-12 的搜索关键字 created:>2019-02-12 test #创建时间大于 2019-02-12 的搜索关键字 user:test #用户名搜素
license:apache-2.0 test #明确仓库的 LICENSE 搜索关键字 language:java test #在 java 语言的代码中搜索关键字
user:test in:name test #组合搜索,用户名 test 的标题含有 test 的
关键字配合谷歌搜索：
site:Github.com smtp
site:Github.com smtp @qq.com
site:Github.com smtp @126.com
site:Github.com smtp @163.com
site:Github.com smtp @sina.com.cn
site:Github.com smtp password
site:Github.com String password smtp

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
