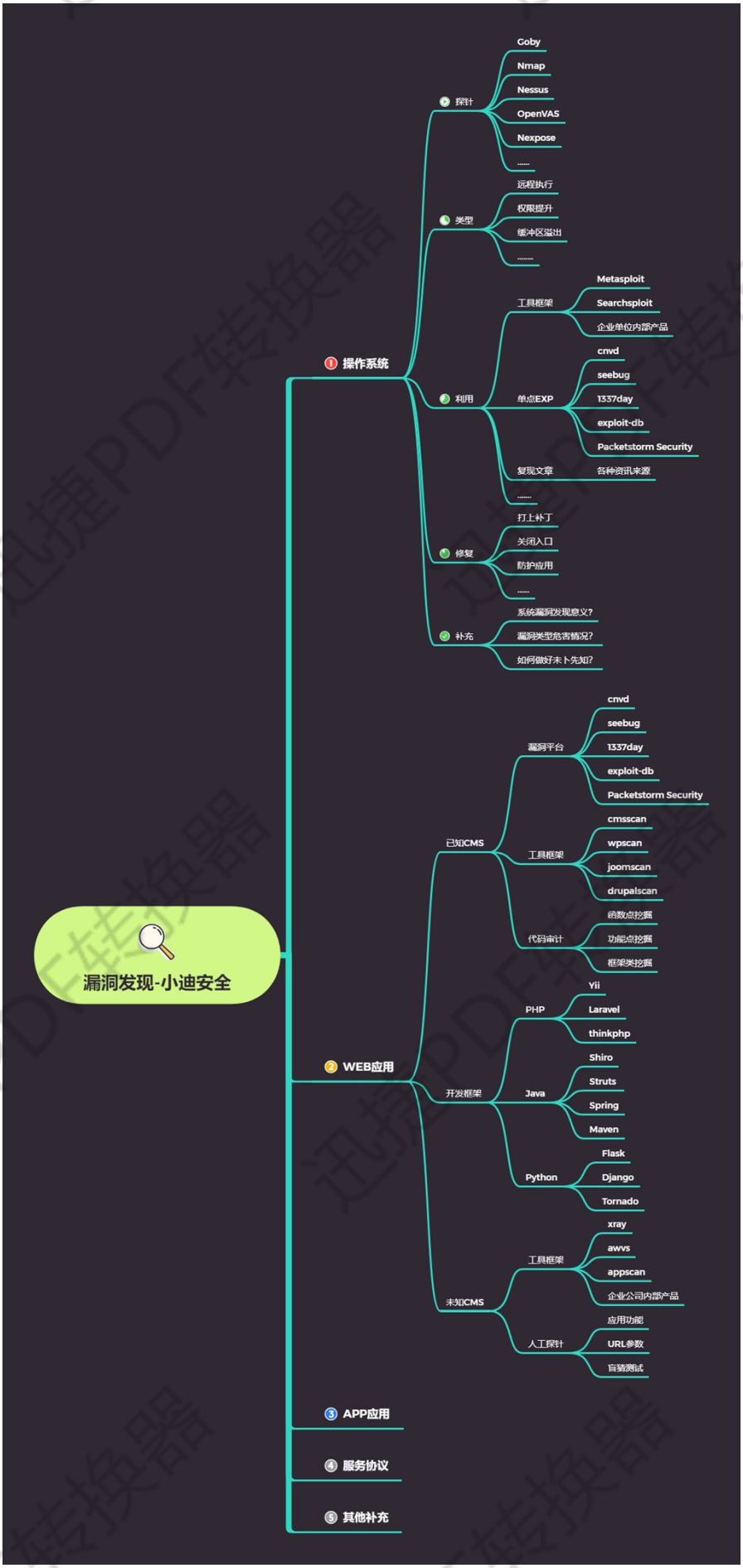
漏洞发现-WEB 应用之漏洞探针类型利用修复


漏洞发现-小迪安全
1 操作系统
探针
Goby
Nmap
Nessus
OpenVAS
Nexpose
.....
类型
远程执行
权限提升
缓冲区溢出
.....
利用
工具框架
Metasploit
Searchsploit
企业单位内部产品
单点EXP
cnvd
seebug
1337day
exploit-db
Packetstorm Security
复现文章
各种资讯来源
.....
修复
打上补丁
关闭入口
防护应用
.....
补充
系统漏洞发现意义?
漏洞类型危害情况?
如何做好未卜先知?
2 WEB应用
已知CMS
漏洞平台
cnvd
seebug
1337day
exploit-db
Packetstorm Security
工具框架
cmsscan
wpscan
joomscan
drupalscan
代码审计
函数点挖掘
功能点挖掘
框架类挖掘
开发框架
PHP
Yii
Laravel
thinkphp
Java
Shiro
Struts
Spring
Maven
Python
Flask
Django
Tornado
未知CMS
工具框架
xray
awvs
appscan
企业公司内部产品
人工探针
应用功能
URL参数
盲猜测试
3 APP应用
4 服务协议
5 其他补充

#已知 CMS
如常见的 dedecms.discuz,wordpress 等源码结构，这种一般采用非框架类开发，但也有少部分采用的是框架类开发，针对此类源码程序的安全检测，我们要利用公开的漏洞进行测试，如不存在可采用白盒代码审计自行挖掘。

#开发框架
如常见的 thinkphp，spring,flask 等开发的源码程序，这种源码程序正常的安全测试思路：先获取对应的开发框架信息(名字，版本)，通过公开的框架类安全问题进行测试，如不存在可采用白盒代码审计自行挖掘。

#未知 CMS
如常见的企业或个人内部程序源码，也可以是某 CMS 二次开发的源码结构，针对此类的源码程序测试思路：能识别二次开发就按已知 CMS 思路进行，不能确定二次开发的话可以采用常规综合类扫描工具或脚本进行探针，也可以采用人工探针（功能点，参数，盲猜），同样在有源码的情况下也可以进行代码审计自行挖掘。

演示案例：

- ✧ 开发框架类源码渗透测试报告-资讯-thinkphp,spring
- ✧ 已知 CMS 非框架类渗透测试报告-工具脚本-wordpress
- ✧ 已知 CMS 非框架类渗透测试报告-代码审计-qqyewu_php
- ✧ 未知 CMS 非框架类渗透测试报告-人工-你我都爱的 wg 哦~

涉及资源：

https://vulhub.org/

https://wpvulndb.com/users/sign_up

https://github.com/wpscanteam/wpscan

https://github.com/ajinabraham/CMSScan

https://pan.baidu.com/s/1KCa-5gU8R8jPXYY19vyvZA 提取码：xiao

https://www.mozhe.cn/bug/detail/S0JTL0F4RE1sY2hGdHdwcUJ6aUFCQT09bW96aGUmozhe

---