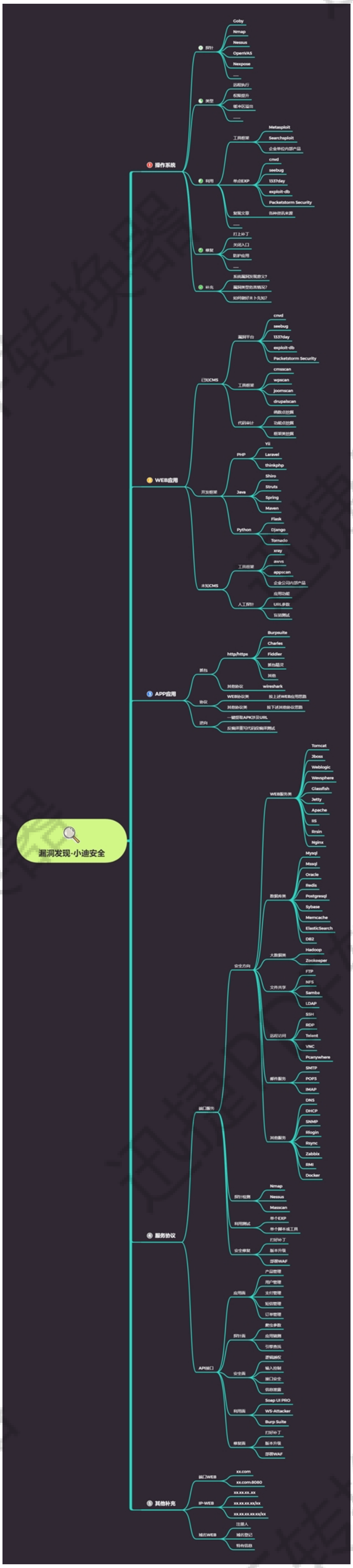
漏洞发现-API 接口服务之漏洞探针类型利用修复


漏洞发现-小迪安全
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?
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
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
APP应用
抓包
http/https
Burpsuite
Charles
Fiddler
抓包精灵
其他
其他协议
wireshark
协议
WEB协议类
按上述WEB应用思路
其他协议类
按下述其他协议思路
逆向
一键提取APK涉及URL
反编译重写代码反编译测试
服务协议
端口服务
安全方向
WEB服务类
Tomcat
Jboss
Weblogic
Wevsphere
Glassfish
Jetty
Apache
IIS
Rrsin
Nginx
数据库类
Mysql
Mssql
Oracle
Redis
Postgresql
Sybase
Memcache
ElasticSearch
DB2
大数据类
Hadoop
Zookeeper
文件共享
FTP
NFS
Samba
LDAP
远程访问
SSH
RDP
Telent
VNC
Pcanywhere
邮件服务
SMTP
POP3
IMAP
其他服务
DNS
DHCP
SNMP
Rlogin
Rsync
Zabbix
RMI
Docker
探针检测
Nmap
Nessus
Masscan
利用测试
单个EXP
单个脚本或工具
安全修复
打好补丁
版本升级
部署WAF
API接口
应用面
产品管理
用户管理
支付管理
短信管理
订单管理
探针面
安全面
输入控制
接口安全
信息泄露
利用面
Soap UI PRO
WS-Attacker
Burp Suite
修复面
打好补丁
版本升级
部署WAF
其他补充
端口WEB
xx.com
xx.com:8080
IP-WEB
xx.xx.xx..xx
xx.xx.xx.xx/xx
xx.xx.xx.xx.xx/xx
域名WEB
注册人
域名登记
特有信息

#端口服务类安全测试
根据前期信息收集针对目标端口服务类探针后进行的安全测试，主要涉及攻击方法：口令安全，WEB 类漏洞，版本漏洞等，其中产生的危害可大可小。属于端口服务/第三方服务类安全测试面。一般在已知应用无思路的情况下选用的安全测试方案。

#API 接口-WebServiceRESTful API
https://xz.aliyun.com/t/2412
根据应用自身的功能方向决定，安全测试目标需有 API 接口调用才能进行此类测试，主要涉及的安全问题：自身安全，配合 WEB，业务逻辑等，其中产生的危害可大可小，属于应用 API 接口网络服务测试面，一般也是在存在接口调用的情况下的测试方案。

WSDL（网络服务描述语言，Web Services Description Language）是一门基于 XML 的语言，用于描述 Web Services 以及如何对它们进行访问。

#漏洞关键字：
配合 shodan，fofa,zoomeye 搜索也不错哦~
inurl:jws?wsdl
inurl:asmx?wsdl
inurl:aspx?wsdl
inurl:ascx?wsdl
inurl:ashx?wsdl
inurl:dll?wsdl
inurl:exe?wsdl
inurl:php?wsdl
inurl:pl?wsdl
inurl:?wsdl
filetype:wsdl wsdl

http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL

1、web服务类

```
    tomcat--80/8080/8009
            manager弱口令
            put上传webshell
            HTTP慢速攻击
            ajr文件包含漏洞-CVE-2020-1938
Jboss--8080
            后台弱口令
            console后台部署war包
            JAVA反序列化
            远程代码执行
webSphere--9080
            后台弱口令
            任意文件泄露
            JAVA反序列化
weblogic--7001/7002
            后台弱口令
            console后台部署war包
            SSRF
            测试页面上传webshell
                    JAVA反序列化
                        CVE-2018-2628
                        CVE-2018-2893
                        CVE-2017-10271
                        CVE-2019-2725
                        CVE-2019-2729
Glassfish--8080/4848
            暴力破解
            任意文件读取
            认证绕过
Jetty--8080
            远程共享缓冲区溢出
Apache--80/8080
            HTTP慢速攻击
            解析漏洞
            目录遍历
Apache Solr--8983
            远程命令执行
            CVE-2017-12629
            CVE-2019-0193
 IIS--80
            put上传webshell
            IIS解析漏洞
            IIS提权
            IIS远程远程代码执行-CVE-2017-7269
 Resin--8080
            目录遍历
            远程文件读取
 Axis2--8080
            后台弱口令
 Lutos--1352
            后台弱口令
            信息泄露
            跨站脚本攻击
 Nginx--80/443
            HTTP慢速攻击
            解析漏洞
```

2、数据库类

```
Mysql--3306
        弱口令
        身份认证漏洞-cve-2012-2122
        拒绝服务攻击
        phpmyadmin万能密码or弱口令
        UDF/MOF提权
Mssql--1433
        弱口令
        存储过程提权
Oralce--1521
        弱口令
        TNS漏洞
Redis--6379
        弱口令
        未经授权访问
PostgreSQL--5432
        弱口令
        缓冲区溢出-cve-2014-2669
MongoDB--27001
        弱口令
        未经授权访问
DB2--5000
        安全限制绕过进行未经授权操作-cve-2015-1922
SysBase--5000/4100
        弱口令
        命令注入
Memcache--11211
        未经授权访问
        配置漏洞
ElasticSearch--9200/9300
        未经授权访问
        远程代码执行
        文件办理
        写入webshell
```

3、大数据类

```
Hadoop--50010
        远程命令执行
Zookeeper--2181
        未经授权访问
```