攻防世界 web高手进阶区 10分题 url

原创

思源湖的鱼 于 2020-10-19 18:18:09 发布 692 收藏

分类专栏： ctf 文章标签： 网络安全 ctf 攻防世界 ssrf web

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109163135

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

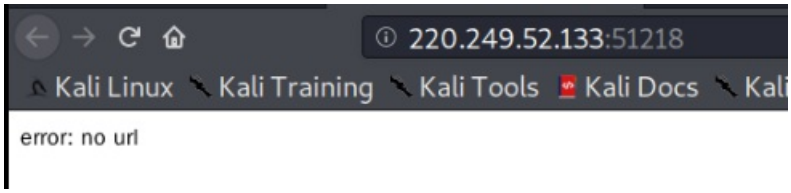
继续ctf的旅程

开始攻防世界web高手进阶区的10分题

本文是url的writeup

解题过程

进入界面



惯例源码+御剑

源码是空的

御剑如下

1	http://220.249.52.133:51218/server-status/	403
2	http://220.249.52.133:51218/icons/	403
3	http://220.249.52.133:51218/index.php	200
3	http://220.249.52.133:51218/index.php?chemin=..%2f..%2f..%2f..%2f..%2f%2fetc	200
5	http://220.249.52.133:51218/index.php?option=com_user&view=reset&layout=confirm	200
6	http://220.249.52.133:51218/index.php?s=admin-login	200
7	http://220.249.52.133:51218/.htaccess	403
8	http://220.249.52.133:51218/index.php.	200
9	http://220.249.52.133:51218/index.php?	200
10	http://220.249.52.133:51218/index.php?pymembs=admin	200
11	http://220.249.52.133:51218/%2ehtpasswd/	403
12	http://220.249.52.133:51218/8010/Guide/../../../../../../../..	200
13	http://220.249.52.133:51218/cgi-bin/ssi/../../../../../../../../.	200
14	http://220.249.52.133:51218/flag.php	200
15	http://220.249.52.133:51218/index.php	200
16	http://220.249.52.133:51218/index.php%2e	200
17	http://220.249.52.133:51218/index.php?option=com_user&view=res	200
18	http://220.249.52.133:51218/index.php?pymembs=admin	200
19	http://220.249.52.133:51218/index.php?chemin=..%2f..%2f..%2f..	200
20	http://220.249.52.133:51218/?.asp	200

14	http://220.249.52.133:51218/flag.php	200
15	http://220.249.52.133:51218/index.php	200
16	http://220.249.52.133:51218/index.php%2e	200
17	http://220.249.52.133:51218/index.php?option=com_user&view=res	200
18	http://220.249.52.133:51218/index.php?pymembs=admin	200
19	http://220.249.52.133:51218/index.php?chemin=..%2f..%2f..%2f..	200
20	http://220.249.52.133:51218/?.asp	200
21	http://220.249.52.133:51218/index.php?.php	200
22	http://220.249.52.133:51218/?.php	200
23	http://220.249.52.133:51218/?.jsp	200

发现一个flag
访问看看
是个全空的页面
。。。

抓包试试
也没有信息

抓瞎了
做了一些尝试
伪协议啥的
但也没效果

头秃
无处下手

看了眼wp

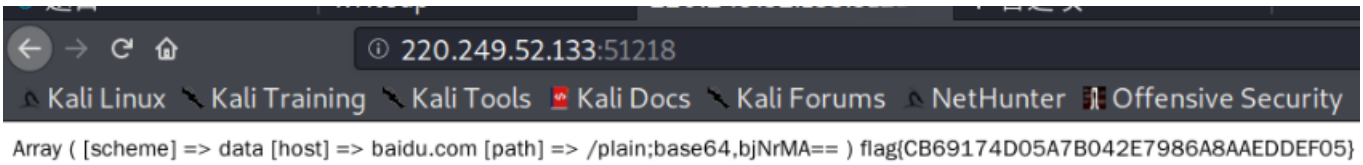
post:

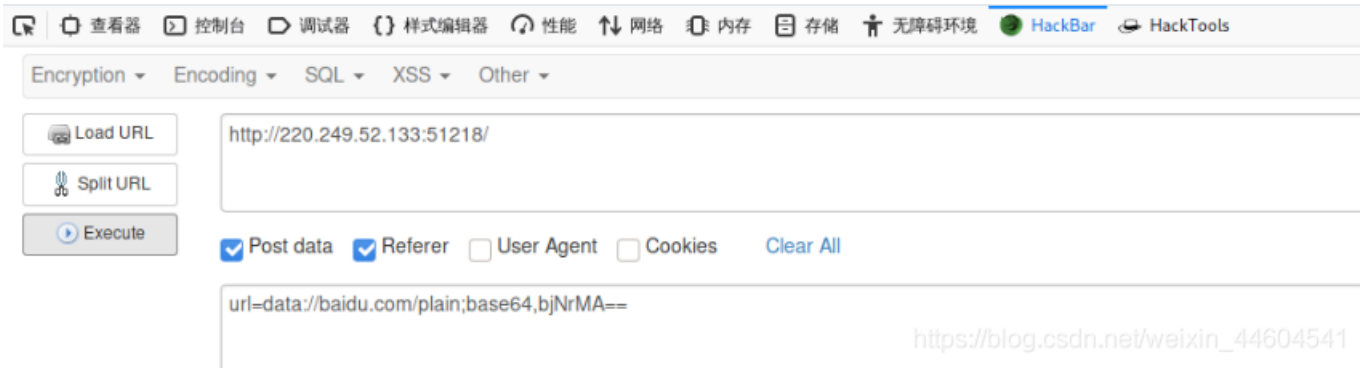
```
url=data://baidu.com/plain;base64,bjNrMA==
```

。。。。。。
。。。。。
。。。。
。。。
。。
。

哽住
这没头没尾的
data伪协议我懂
但为什么会用这个
为什么是base64
为什么原字符串是`n3k0`
懵逼

试一下





得到flag
骚气的ssrf

结语

人傻了
懵逼的进来
懵逼的出去
也没学到啥
都不好意思发这篇wp

看了眼评论
集体懵逼


Darklee 5 个月前
一脸懵逼的看完writeup，然后看看评论，原来不止我一个。
回复 0
YeFeng 6 个月前
没有代码审计，没有明确目标，抓包也没有，url加data我可以理解，plain也可以理解，但是为什么是base64 为什么是n3ko字符串，一点头绪没有啊
回复 0
1eng 7 个月前
懵懵的
回复 0
幻影 8 个月前
有大佬给解释一下吗？感谢
回复 1
黄金蟒 回复 幻影 3 个月前
找到url，post一下url
回复 1
lz2y 8 个月前
有大佬解释一下吗？
回复 0
紫色皓月 8 个月前
这题我也懵逼
回复 0
https://blog.csdn.net/weixin_44604541

求大师傅们教下