

# i春秋 afr2 任意文件读取漏洞 目录穿越 题解+原理

原创

[AAAAAAAAAAAAA66](#) 于 2021-11-20 13:08:56 发布 2213 收藏

分类专栏: [CTF-WEB学习](#) 文章标签: [php](#) [apache](#) [网络安全](#)

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/AAAAAAAAAAAAA66/article/details/121437471>

版权



[CTF-WEB学习](#) 专栏收录该内容

34 篇文章 1 订阅

订阅专栏

继续扩充知识储备。

---

目录

知识点

目录穿越漏洞

题目

解题过程

(补充一点HTML知识) `<img>` 标签 代表 图片, `img` 标签的作用是向网页中插入一张图片, 并不是将图片绘制到网页中。

---

知识点

目录穿越漏洞

目录遍历(目录穿越)是一个Web安全漏洞, 攻击者可以利用该漏洞读取运行应用程序的服务器上的任意文件。这可能包括应用程序代码和数据, 后端系统的登录信息以及敏感的操作系统文件。

说人话就是知道一个文件的路径后, 在url上加上`../`可以访问上一级路径。

(当然本题这个漏洞是nginx服务器配置不当产生的, 修改代码可以防御)

\*在Unix操作系统上, `../` 是一个标准的返回上一级路径的语法;

\*在Windows操作系统上, `../` 和 `..\` 都是返回上一级的语句。

题目

分值: 100分

类型: Web

题目名称: afr\_2

未解答

题目内容: afr\_2

http://eci-2ze02m5x7onib4n37ezu.cloudeci1.ichunqiu.com:80

00 : 56 : 40

延长时间(3)

重新创建

Flag:

提交

解题排名:

1 忧郁小猫猫

2 PASSERFBER

3 vFREE

CSDN @AAAAAAAAAAAAA66

## 解题过程

进来就一张吊图。



+

CSDN @AAAAAAAAAAAAA66

老规矩，流程走一遍，URL输入robot.txt, ""（单引号 目的是为了报错界面）

2种方式都出现报错

# 404 Not Found

nginx/1.14.0 (Ubuntu)

CSDN @AAAAAAAAAAAAA66

不过爆出了服务器版本。

dirsearch (文件目录扫描器) (解这道题不是必须, 但还是推荐一下, 这里附上一道需要使用dirsearch的题目 (包含下载的教程))

dirsearch扫一下

```
[16:36:25] Starting:
[16:36:26] 400 - 150B - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[16:36:48] 400 - 150B - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[16:36:55] 301 - 194B - /img → http://eci-2ze02m5x7onib4n37ezu.cloudeci1.ichunqiu.com/img/
[16:36:55] 200 - 99B - /index.html
CSDN @AAAAAAAAAAAAA66
```

F12查看源码

```
<html>
  <head>...</head>
  <body> == $0
    "
    HELLO!
    "
    
  </body>
</html>
```

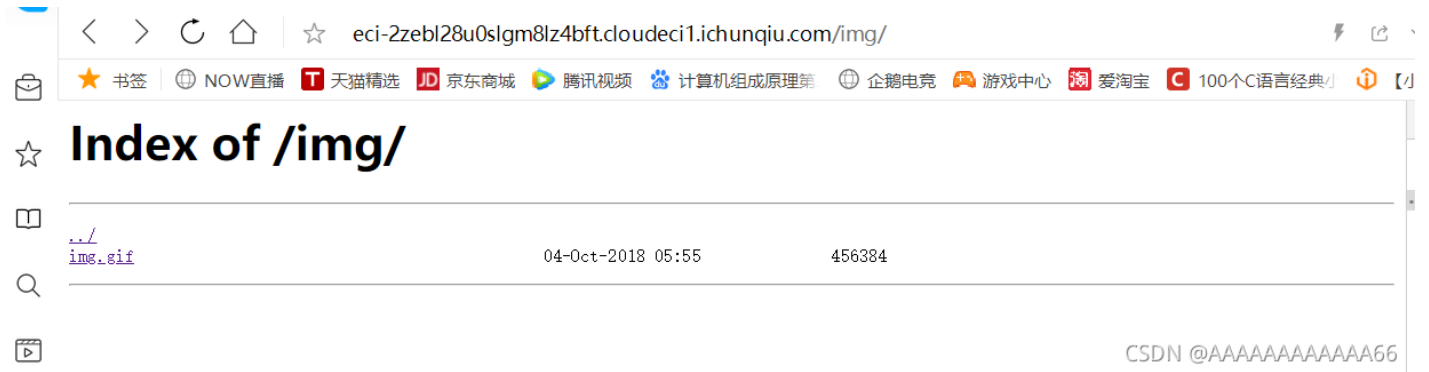
CSDN @AAAAAAAAAAAAA66

(补充一点HTML知识) <img>标签 代表 图片, img标签的作用是向网页中插入一张图片, 并不是将图片绘制到网页中。

这里附上[的使用!!》" data-link-title="《关于html中的使用!!》">《关于html中的使用!!》  
<https://blog.csdn.net/x1198928367/article/details/52624463>](https://blog.csdn.net/x1198928367/article/details/52624463)

相信看完对图片获取路径有着新的理解。

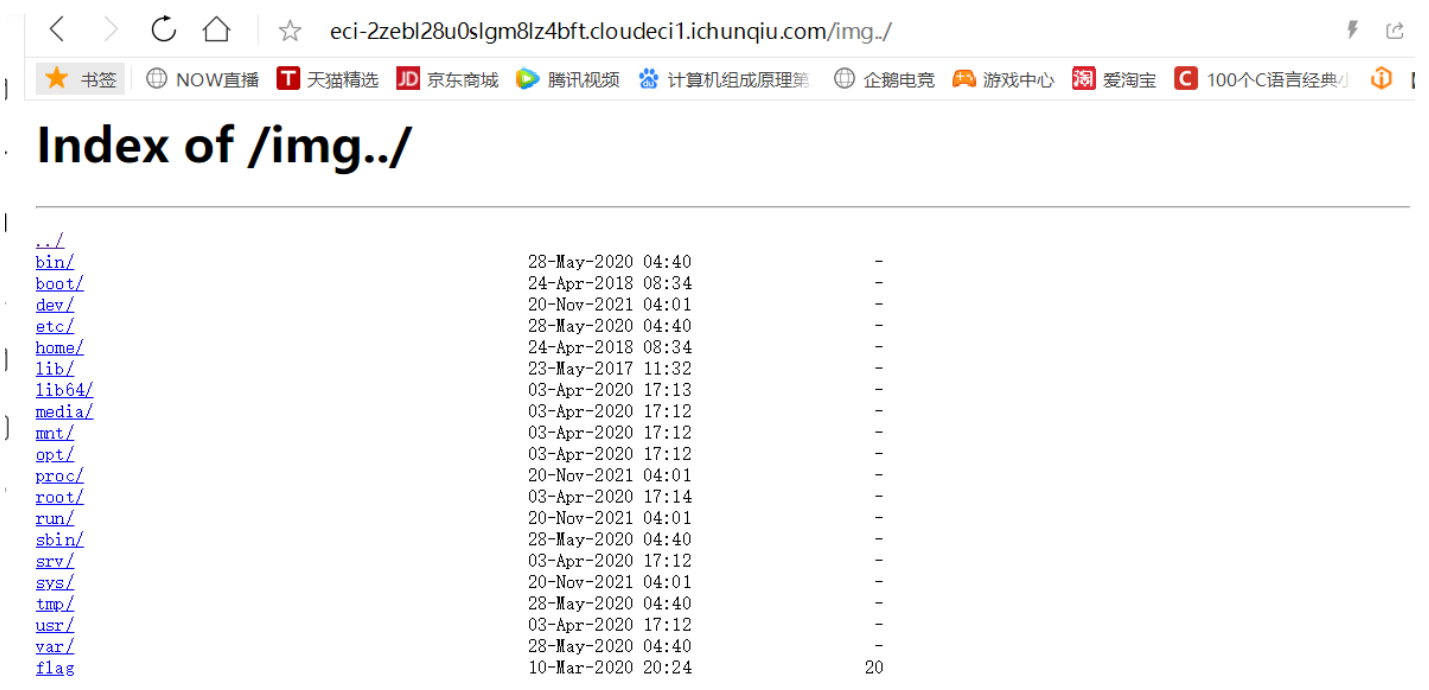
所以我们尝试查看一下img文件夹



点击 ../ 返回了首页面，和dirsearch扫描的一样。

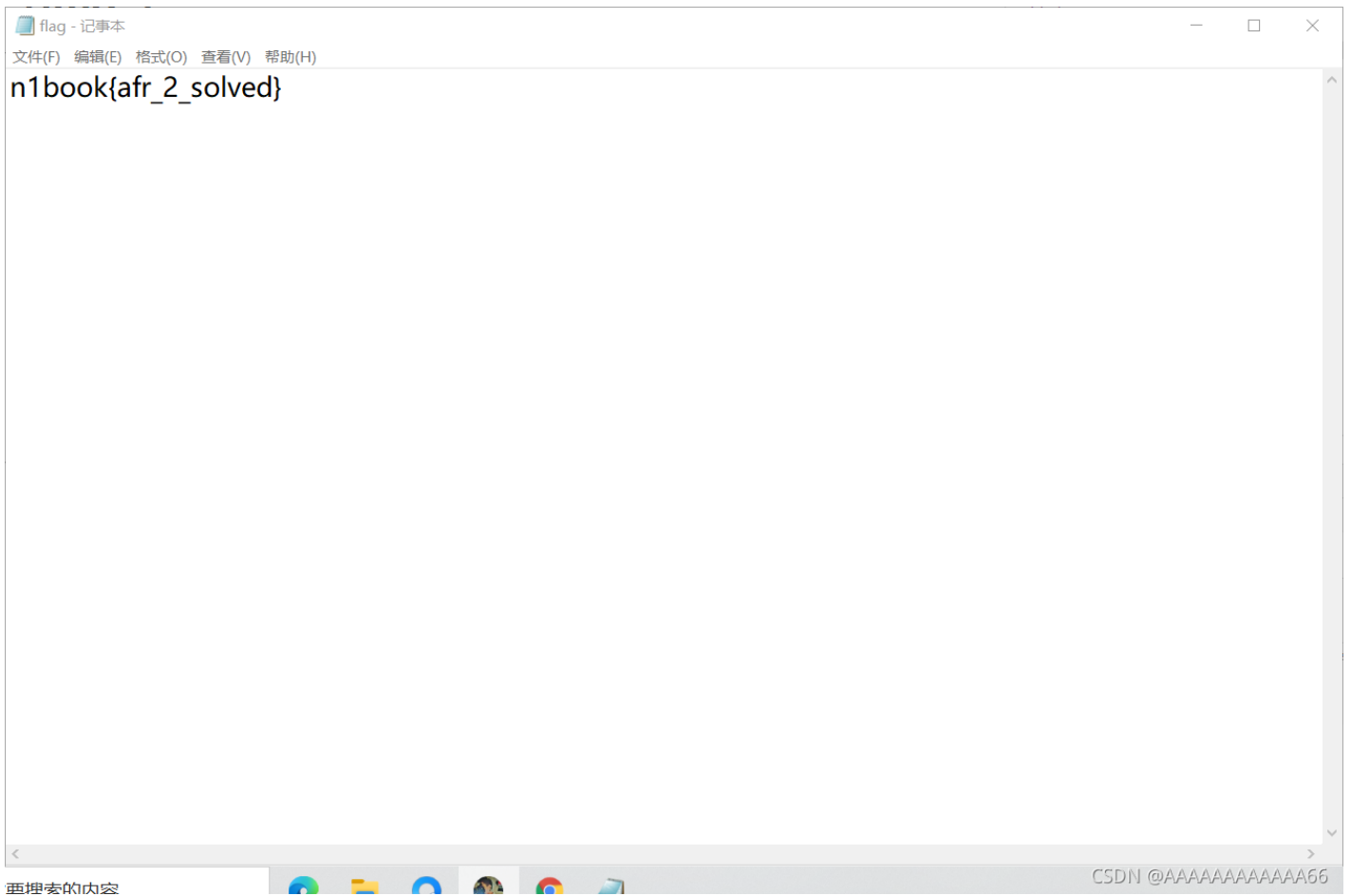
当然这里../暗示的很明显了，结合知道是nginx服务器，构造payload

```
http://eci-2zebl28u0slgm8lz4bft.cloudec11.ichunqiu.com/img../
```



CSDN @AAAAAAAAAAAAA66

点击flag文件下载，记事本打开



这道题偏简单，就是在文件夹后面加上../，就可以查看文件的上一级了，但实际上这种漏洞因该很少（很容易修复),做这道题主要是能扩充下知识面。（get）

---

emm 水平有限，写的不好欢迎指正。