《从0到1：CTFer成长之路》常见的搜集

原创

ZhShy23 于 2022-01-09 22:01:57 发布 600 收藏

分类专栏： 《从0到1：CTFer成长之路》 文章标签： 安全 linux ctf web安全

本文链接：https://blog.csdn.net/weixin_43651049/article/details/122400225

靶场：常见的搜集

i春秋 《从0到1：CTFer成长之路》

敏感文件

Hello, CTFer!

信息搜集之所以重要，是因为其往往会带给我们一些意想不到的东西

---

hack fun

知识点

dirsearch

下载：

```
┌──(root㉿kali)-[/tools]
└─# git clone git://github.com/maurosoria/dirsearch.git
```

扫描：

```
┌──(root㉿kali)-[/tools/dirsearch]
└─# python3 dirsearch.py -u 网址 -i 200
```

swp文件

打开：

```
┌──(root㉿kali)-[~/download]
└─# vim -r index.php.swp
```

解题过程

1 使用dirsearch进行扫描

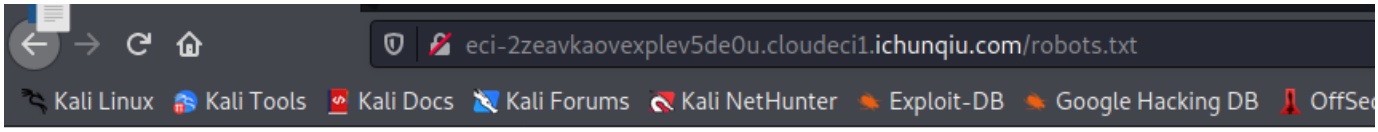
```
┌──(root㉿kali)-[/tools/dirsearch]
└─# python3 dirsearch.py -u http://eci-2zeavkaovexplev5de0u.cloudeci1.ichunqiu.com/ -i 200

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10991

Output File: /tools/dirsearch/reports/eci-2zeavkaovexplev5de0u.cloudeci1.ichunqiu.com/-_22-01-09_21-29-52.txt

Error Log: /tools/dirsearch/logs/errors-22-01-09_21-29-52.log

Target: http://eci-2zeavkaovexplev5de0u.cloudeci1.ichunqiu.com/

[21:29:52] Starting:
[21:29:55] 200 -   10KB - /.DS_Store
[21:29:57] 200 -   12KB - /.index.php.swp
[21:30:46] 200 -    2KB - /index.php
[21:30:46] 200 -    2KB - /index.php/login/
[21:30:46] 200 -    2KB - /index.php~
CTRL+C detected: Pausing threads, please wait...
[q]uit / [c]ontinue: c
[21:32:35] 200 -   47B  - /robots.txt

Task Completed
```

扫描结果

```
[21:29:52] Starting:
[21:29:55] 200 -   10KB - /.DS_Store
[21:29:57] 200 -   12KB - /.index.php.swp
[21:30:46] 200 -    2KB - /index.php
[21:30:46] 200 -    2KB - /index.php/login/
[21:30:46] 200 -    2KB - /index.php~
CTRL+C detected: Pausing threads, please wait...
[q]uit / [c]ontinue: c
[21:32:35] 200 -   47B  - /robots.txt
```

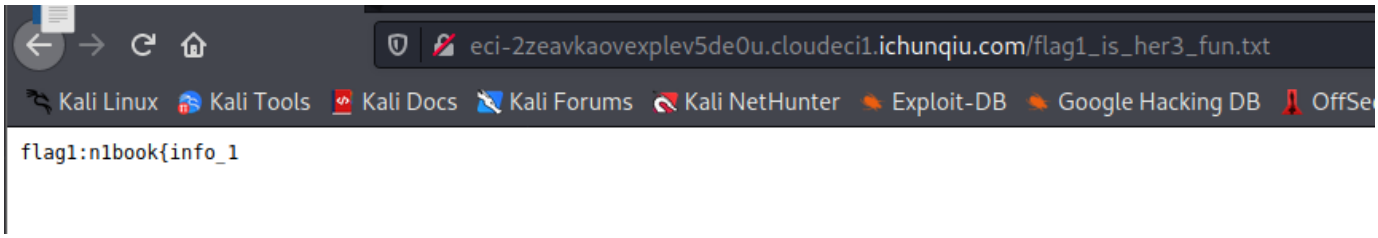
2 挨个访问

robots.txt



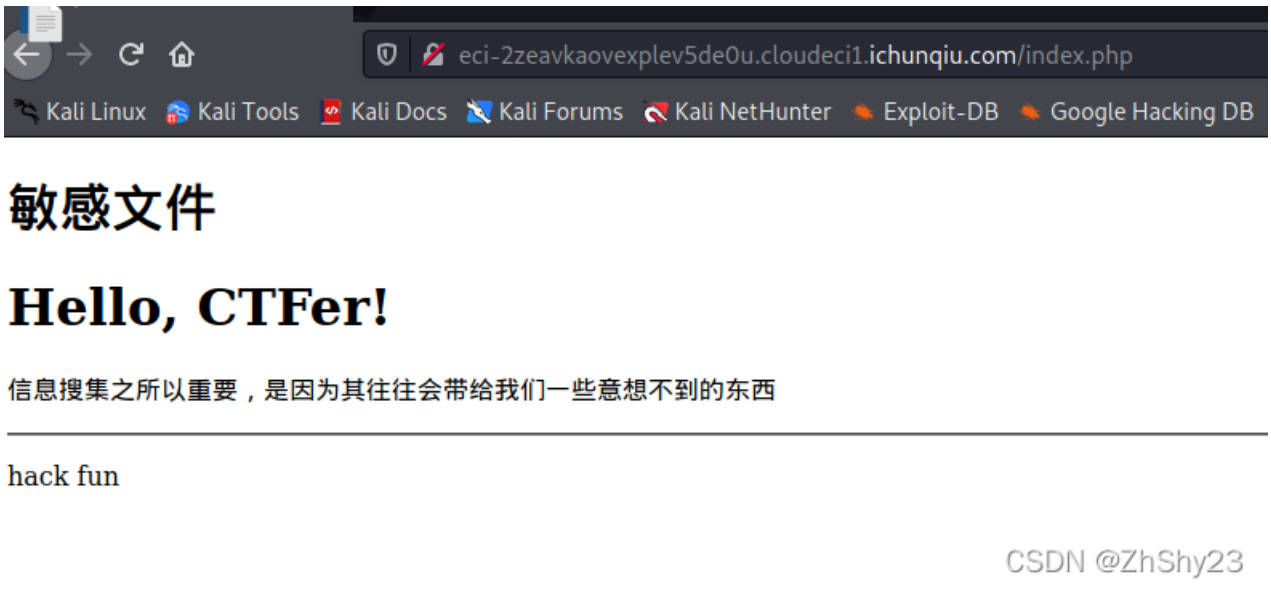

```
User-agent: *
Disallow:
/flag1_is_her3_fun.txt
```

打开 `/flag1_is_her3_fun.txt`

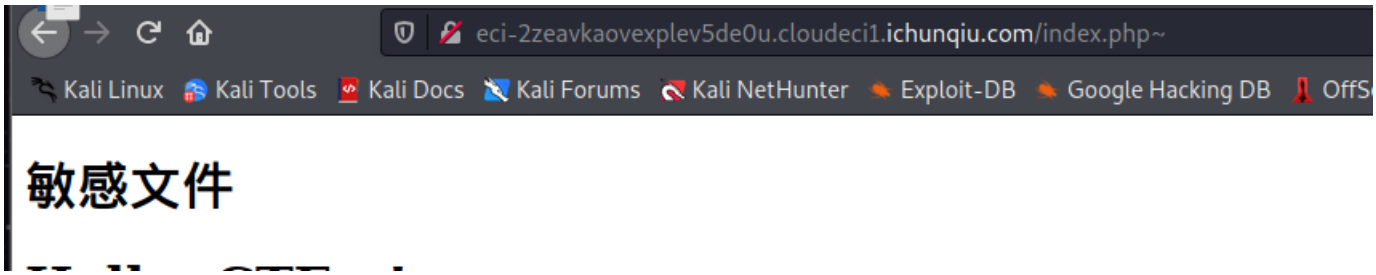


`flag1:n1book{info_1`

index.php



index.php~



Hello, CTFer!

信息搜集之所以重要，是因为其往往会带给我们一些意想不到的东西

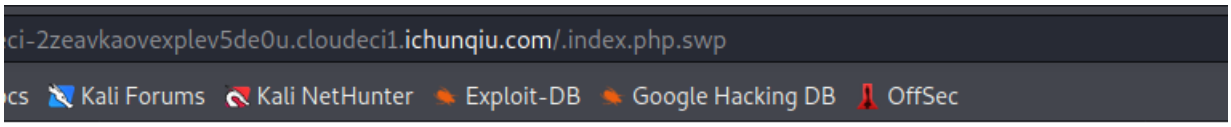
---

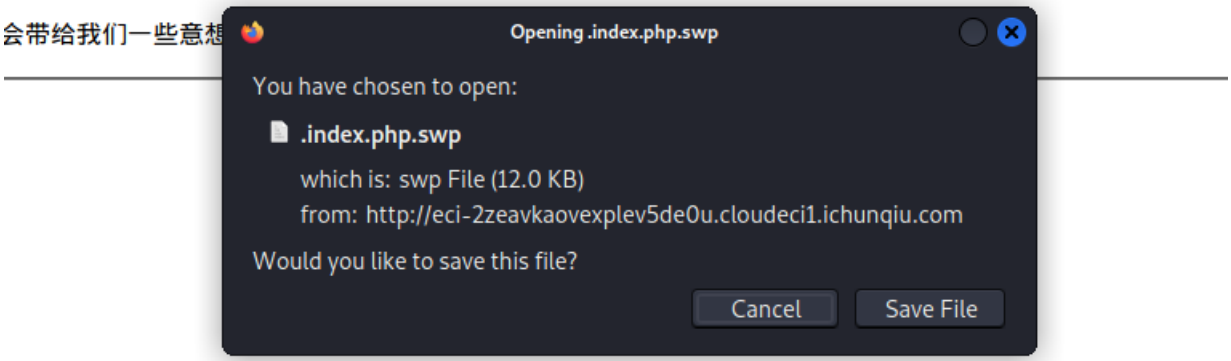
hack fun

flag2:s_v3ry_im

`flag2:s_v3ry_im`

.index.php.swp





使用`vim -r`命令打开swp文件，并使用`/flag`搜索

`flag3:p0rtant_hack}`

整合起来：

```
n1book{info_1s_v3ry_imp0rtant_hack}
```