

CTF 解题记录

作者：shijy16

时间：March 13, 2021

特别声明

本册是 CTF 解题记录，题目来自于从 0 到 1: CTFeR 成长之路的配套平台。在各章节子文件夹中也直接存放了题目的 docker 文件。

供初学 CTF 的同学们参考交流。

shijy16

目录

1	web 入门	2
1.1	信息收集	2
1.2	总结	3

第一章 web 入门

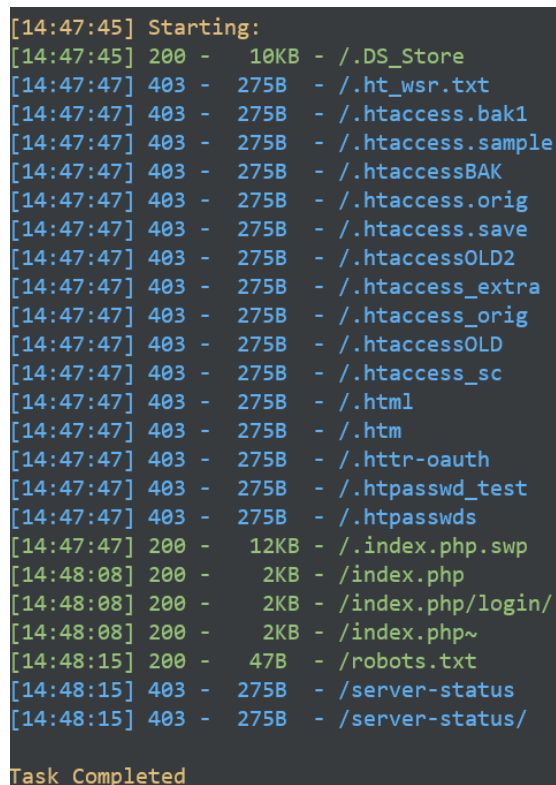
1.1 信息收集

1.1.1 常见的搜集

直接进入网页后提示是敏感文件题目，页面没有任何按钮。那么直接使用目录扫描工具扫一遍：

```
1 python3 dirsearch.py -u http://172.17.0.1/
```

结果如图 1.1。



```
[14:47:45] Starting:
[14:47:45] 200 - 10KB - /.DS_Store
[14:47:47] 403 - 275B - /.ht_wsr.txt
[14:47:47] 403 - 275B - /.htaccess.bak1
[14:47:47] 403 - 275B - /.htaccess.sample
[14:47:47] 403 - 275B - /.htaccessBAK
[14:47:47] 403 - 275B - /.htaccess.orig
[14:47:47] 403 - 275B - /.htaccess.save
[14:47:47] 403 - 275B - /.htaccessOLD2
[14:47:47] 403 - 275B - /.htaccess_extra
[14:47:47] 403 - 275B - /.htaccess_orig
[14:47:47] 403 - 275B - /.htaccessOLD
[14:47:47] 403 - 275B - /.htaccess_sc
[14:47:47] 403 - 275B - /.html
[14:47:47] 403 - 275B - /.htm
[14:47:47] 403 - 275B - /.httr-oauth
[14:47:47] 403 - 275B - /.htpasswd_test
[14:47:47] 403 - 275B - /.htpasswd
[14:47:47] 200 - 12KB - /.index.php.swp
[14:48:08] 200 - 2KB - /index.php
[14:48:08] 200 - 2KB - /index.php/login/
[14:48:08] 200 - 2KB - /index.php~
[14:48:15] 200 - 47B - /robots.txt
[14:48:15] 403 - 275B - /server-status
[14:48:15] 403 - 275B - /server-status/
Task Completed
```

图 1.1: 扫描结果

那么把这些目录全部访问一遍。

- 直接访问 robots.txt: 提示 flag 在另一个文件中，再次访问得 *flag1 : n1book{info_1*
- 直接访问 index.php~: *flag2 : s_v3ry_im*
- 恢复.index.php.swp: *flag3 : p0rtant_hack}*

拼凑起来，最终 flag 为：

```
1 n1book{info_1s_v3ry_imp0rtant_hack}
```

1.1.2 粗心的小李

网页提示是很简单的 git 泄露，那么直接用scrabble尝试恢复一下：

```
1  ./scrabble http://172.17.0.1
2  重新初始化已存在的 Git 仓库于 /home/shijy/ctf/tools/web/
   scrabble/.git/
3  parseCommit 213b7e386e9b0b406d91fae58bf8be11a58c3f88
4  downloadBlob 213b7e386e9b0b406d91fae58bf8be11a58c3f88
5  parseTree f46fbac4149604ca13a765950f9a2d1fd8c1c7ad
6  downloadBlob f46fbac4149604ca13a765950f9a2d1fd8c1c7ad
7  downloadBlob 1e0db5d96b5cc9785055c14bbec0e7ad14f48151
8  HEAD 现在位于 213b7e3 flag
```

恢复成功，获得一个 index.html 文件，直接打开，搜索到 flag:

```
1  n1book{git_looks_s0_easyfun}
```

1.2 总结

这两个问题都是有隐藏路径暴露在外网中，按道理上来直接目录扫描工具扫一下，之后再按情况分析即可。