CTF-web-robots协议

原创

杰西啊杰西 于 2019-04-30 15:37:06 发布 1862 收藏 2

文章标签： ctf

本文链接：https://blog.csdn.net/qq_43681877/article/details/89710700

Robots协议

环境网址http://111.198.29.45:59344

首先安装dirsearch_master

下载地址（https://github.com/maurosoria/dirsearch）

运行环境为python3

在解压后的dirsearch_master文件夹里打开命令行

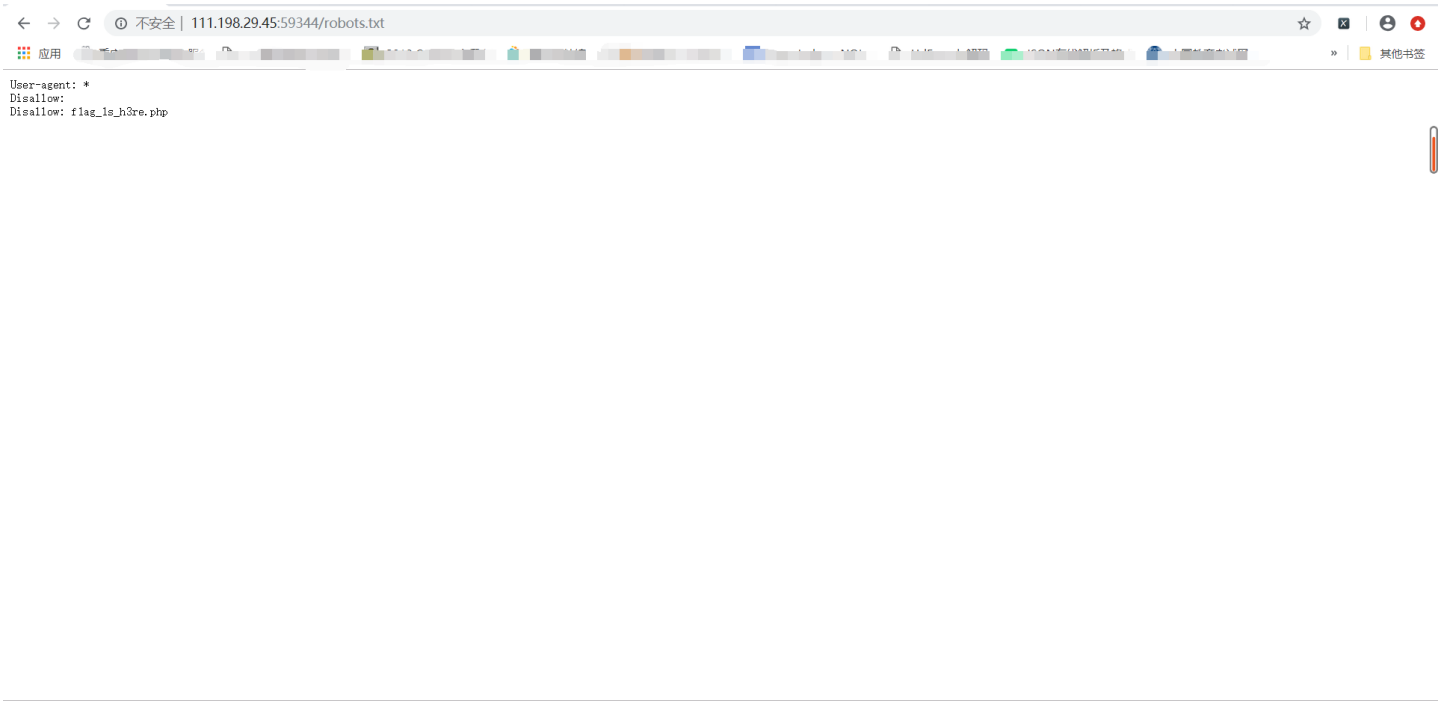
输入

```
python dirsearch.py -u http://111.198.29.45:59344/ -e *
```

即开始进行目录扫描

```
E:\ctf工具\dirsearch-master>python dirsearch.py -u http://111.198.29.45:59344/ -e *

 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: * | Threads: 10 | Wordlist size: 6086

Error Log: E:\ctf工具\dirsearch-master\logs\errors-19-04-30_15-07-12.log

Target: http://111.198.29.45:59344/

[15:07:12] Starting:
[15:07:15] 403 -  294B  - /.ht_wsr.txt
[15:07:15] 403 -  287B  - /.hta
[15:07:15] 403 -  296B  - /.htaccess-dev
[15:07:15] 403 -  298B  - /.htaccess-local
[15:07:15] 403 -  298B  - /.htaccess-marco
[15:07:15] 403 -  296B  - /.htaccess.BAK
[15:07:15] 403 -  297B  - /.htaccess.bak1
[15:07:15] 403 -  296B  - /.htaccess.old
[15:07:15] 403 -  297B  - /.htaccess.orig
[15:07:15] 403 -  299B  - /.htaccess.sample
[15:07:15] 403 -  297B  - /.htaccess.save
[15:07:15] 403 -  296B  - /.htaccess.txt
[15:07:15] 403 -  297B  - /.htaccess_orig
[15:07:15] 403 -  298B  - /.htaccess_extra
[15:07:15] 403 -  295B  - /.htaccess_sc
[15:07:15] 403 -  295B  - /.htaccessOLD
[15:07:15] 403 -  295B  - /.htaccessBAK
[15:07:15] 403 -  296B  - /.htaccessOLD2
[15:07:15] 403 -  293B  - /.htaccess~
[15:07:15] 403 -  291B  - /.htgroup
[15:07:15] 403 -  296B  - /.htpasswd-old
[15:07:15] 403 -  297B  - /.htpasswd_test
[15:07:15] 403 -  293B  - /.htpasswds
[15:07:15] 403 -  291B  - /.htusers
[15:07:40] 200 -  176B  - /index.php
[15:07:40] 200 -  176B  - /index.php/login/
[15:07:51] 200 -   53B  - /robots.txt
[15:07:52] 403 -  296B  - /server-status
[15:07:52] 403 -  297B  - /server-status/

Task Completed

E:\ctf工具\dirsearch-master>
```

由于是robots使我们无法访问网页，所以考虑是robots协议
爆破扫描后发现有robots.txt
所以开始奇思妙想2333
由于最开始不知道怎么样才能访问到robots.txt，于是决定直接在网址后加后缀
emmm…算一种小经验吧



果然出现了flag的小痕迹
看到了Disallow: f1ag_1s_h3re.php 了吗
然后又像刚刚那样将后缀改为f1ag_1s_h3re.php
完美找到flag