

ctf-wscan 为ctf而生的web扫描器

原创

Le叶a子f 于 2021-10-12 14:18:20 发布 206 收藏

分类专栏: [ctf工具](#) 文章标签: [python web](#)

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/qq_38850916/article/details/120722462

版权



ctf同时被 2 个专栏收录

11 篇文章 0 订阅

订阅专栏



工具

4 篇文章 0 订阅

订阅专栏

```
>python ctf-wscan.py http://e4189dee-b31e-4508-996d-656e82b137ed.node4.buuoj
[404] => source.php
[404] => phpinfo.php
[429] => .bash_history
[429] => .svn/
[429] => .git/
[429] => .index.php.swp
[429] => index.php.swp
[429] => index.php.bak
[429] => .index.php
[429] => index.php.bak_Edietplus
[429] => index.php.~1
[429] => index.php
[429] => index.php.rar
[429] => index.php
[429] => index.php.zip
[429] => index.php.7z
[429] => index.php.tar.gz
[429] => login.php
[429] => index.php.txt
[429] => test.php
[429] => upload.php
[429] => phpinfo.php
[404] => phpinfo.php
```

CSDN @Le叶a子f

ctf-wscan

一个为ctf而生的web扫描器

基于多线程的扫描器, 可添加关键字, 扫描一些备份文件和路径

使用方式

Usage : python ctf-wscan.py [website url]

Example: python ctf-wscan.py http://ctf.test.com

新增-k参数

Usage : python ctf-wscan.py [website url] [-k key words]

由于觉得添加关键字这个功能还是蛮常用的, 于是添加了个-k参数, 可以在命令行中添加参数

新增对404页面的判断

由于python中404页面的返回码也是200，对于固定页面长度的，新增判断方式，检测效果更加

一些设置

可修改config.py下的一些设置，进行自定义扫描

```
# 关键字
# 用于生成一些特定字符，进行进一步扫描，如可以输入一些 xxctf的关键词
KEY_WORDS = ['flag', 'ctf', 'kzhan.php']

# 线程数
NUMBER_OF_THREAD = 10

# 请求方式
# 1 => HEAD 2 => GET
REQUEST_METHOD = 1

# 无效的状态码
# 自定义一些无效的状态码，作为判断的标准
INVALID_CODE = [404, 403]

# 超时时间
TIME_OUT = 3

# 记录缓存日志
CACHE_LOG = Truegithub下载地址https://github.com/mydragon/ctf-wscan/tree/master/lib
```