BREACHER - Python Based Directory Brute Forcer

Description:

The **Breacher** tool is a Python-based directory brute-forcing script designed to detect **admin login pages** and potential **External Authentication Redirection (EAR) vulnerabilities** on web applications. It works by sending HTTP requests to predefined paths and analyzing the server's response status codes to determine whether an accessible admin panel or an EAR vulnerability exists.

Usage:

Basic Usage: python breacher.py -u <target_url>

To scan for specific extensions: python breacher.py -u example.com --type php

Multi-Threading: python breacher.py -u example.com --type php --fast

Adding custom path prefixes: python breacher.py -u example.com --path /data

Advantages:

It can be used to scan small applications quickly.

Disadvantages:

Analyzing the source code of the script, I found that the methodology to detect EAR vulnerabilities is solely based on 302 redirects which may contain a lot of false positives.

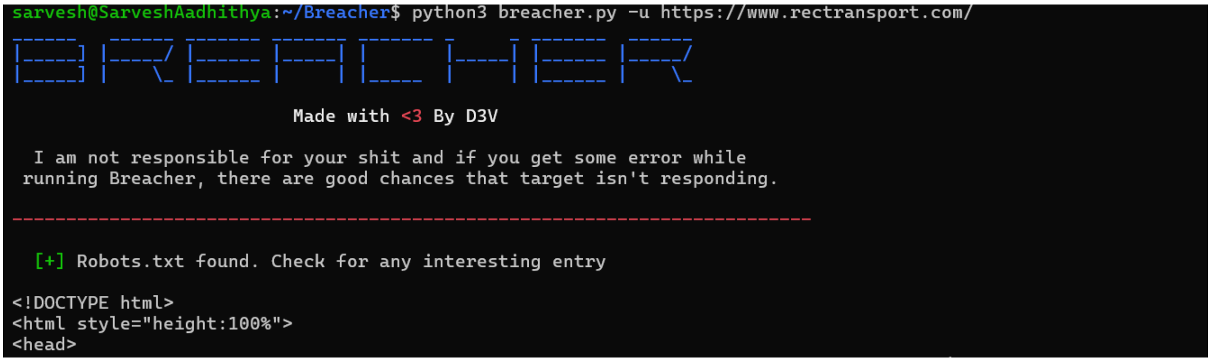
Maximum multi-threading allowed per scanning is 2 threads which is significantly lower than other existing tools like FUFF, Dirbuster, or Dirsearch.

It does not perform recursive directory brute-forcing and heavily depends on a pre-configured wordlist. However, the wordlist can be modified.

The URL is hardcoded with **HTTP** which means it only supports the unencrypted protocol and does not support **HTTPS**

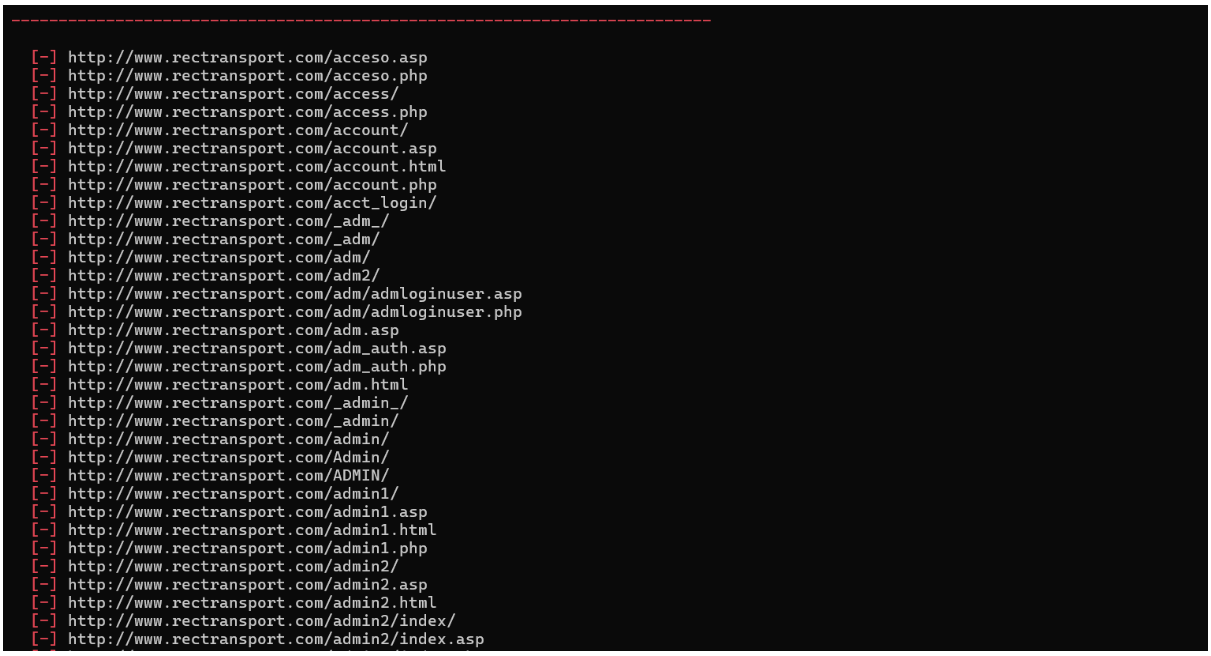
Other than this, a lot of efficient filtering mechanisms and customization are lacking in the Breacher toolkit which makes it not a replacement to any of the existing powerful tools

Screenshots of tool usage:



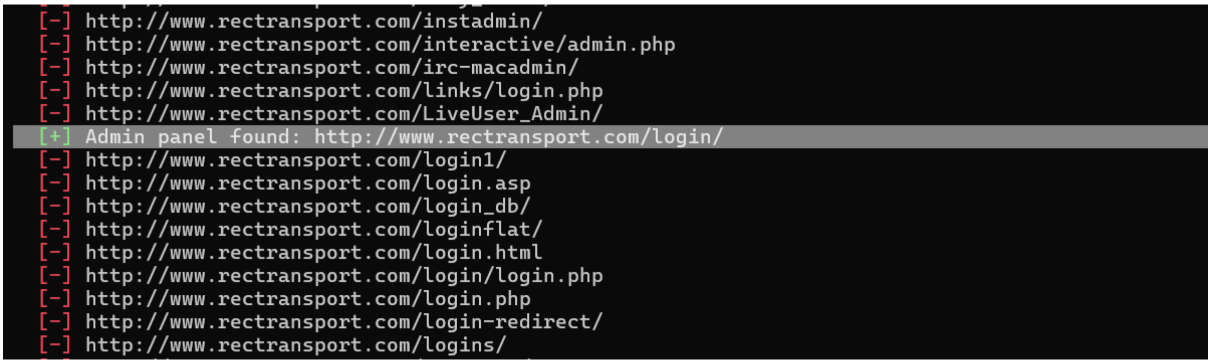
```
sarvesh@SarveshAadhithya:~/Breacher$ python3 breacher.py -u https://www.rectransport.com/
______  ______ _______ _______ _______ _      _ _______ ______
|_____] |_____/ |______ |_____| |       |_____| |______ |_____/
|_____] |    \_ |______ |     | |_____  |     | |______ |    \_

                          Made with <3 By D3V

  I am not responsible for your shit and if you get some error while
 running Breacher, there are good chances that target isn't responding.

--------------------------------------------------------------------------

  [+] Robots.txt found. Check for any interesting entry

<!DOCTYPE html>
<html style="height:100%">
<head>
```

.



```
--------------------------------------------------------------------------

  [-] http://www.rectransport.com/acceso.asp
  [-] http://www.rectransport.com/acceso.php
  [-] http://www.rectransport.com/access/
  [-] http://www.rectransport.com/access.php
  [-] http://www.rectransport.com/account/
  [-] http://www.rectransport.com/account.asp
  [-] http://www.rectransport.com/account.html
  [-] http://www.rectransport.com/account.php
  [-] http://www.rectransport.com/acct_login/
  [-] http://www.rectransport.com/_adm_/
  [-] http://www.rectransport.com/_adm/
  [-] http://www.rectransport.com/adm/
  [-] http://www.rectransport.com/adm2/
  [-] http://www.rectransport.com/adm/admloginuser.asp
  [-] http://www.rectransport.com/adm/admloginuser.php
  [-] http://www.rectransport.com/adm.asp
  [-] http://www.rectransport.com/adm_auth.asp
  [-] http://www.rectransport.com/adm_auth.php
  [-] http://www.rectransport.com/adm.html
  [-] http://www.rectransport.com/_admin_/
  [-] http://www.rectransport.com/_admin/
  [-] http://www.rectransport.com/admin/
  [-] http://www.rectransport.com/Admin/
  [-] http://www.rectransport.com/ADMIN/
  [-] http://www.rectransport.com/admin1/
  [-] http://www.rectransport.com/admin1.asp
  [-] http://www.rectransport.com/admin1.html
  [-] http://www.rectransport.com/admin1.php
  [-] http://www.rectransport.com/admin2/
  [-] http://www.rectransport.com/admin2.asp
  [-] http://www.rectransport.com/admin2.html
  [-] http://www.rectransport.com/admin2/index/
  [-] http://www.rectransport.com/admin2/index.asp
```

Used the tool to find a hidden endpoint



```
  [-] http://www.rectransport.com/instadmin/
  [-] http://www.rectransport.com/interactive/admin.php
  [-] http://www.rectransport.com/irc-macadmin/
  [-] http://www.rectransport.com/links/login.php
  [-] http://www.rectransport.com/LiveUser_Admin/
  [+] Admin panel found: http://www.rectransport.com/login/
  [-] http://www.rectransport.com/login1/
  [-] http://www.rectransport.com/login.asp
  [-] http://www.rectransport.com/login_db/
  [-] http://www.rectransport.com/loginflat/
  [-] http://www.rectransport.com/login.html
  [-] http://www.rectransport.com/login/login.php
  [-] http://www.rectransport.com/login.php
  [-] http://www.rectransport.com/login-redirect/
  [-] http://www.rectransport.com/logins/
```