\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_ \_\_\_\_\_\_\_ \_\_\_\_\_

\ \ / / \_\_ \ / \_\_\_\_|

\ \ /\ / /| |\_\_) | (\_\_\_ \_\_\_ \_\_ \_ \_ \_\_

\ \/ \/ / | \_\_\_/ \\_\_\_ \ / \_\_|/ \_` | '\_ \

\ /\ / | | \_\_\_\_) | (\_\_| (\_| | | | |

\/ \/ |\_| |\_\_\_\_\_/ \\_\_\_|\\_\_,\_|\_| |\_|

WordPress Security Scanner by the WPScan Team

版本： 2.9.1

Sponsored by Sucuri - https://sucuri.net

@\_WPScan\_, @ethicalhack3r, @erwan\_lr, pvdl, @\_FireFart\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

帮助 :

一些值设定在一个配置文件, see the example.conf.json

--update 更新数据库到最新版本。

--url | -u <target url> WordPress的URL /域扫描。

--force | -f 启动wpscan不检查远程站点运行WordPress。

--enumerate | -e [option(s)] 枚举。

参数 :

u 从1到10的用户名ID

u[10-20] 从10到20的用户名ID (你必须写[ ]数值)

p 插件

vp 只有简单的插件

ap 所有的插件 (可能需要很长时间)

tt timthumbs

t themes

vt 只有简单的主题

at 所有的主题 (可能需要很长时间)

允许多个值 : "-e tt,p" 将枚举timthumbs和插件

如果没有提供选项，默认为"vt,tt,u,vp"

--exclude-content-based "<regexp or string>"

用枚举选项，将排除所有出现的基于正则表达式或字符串提供。

你不需要提供正则表达式分隔符，但你必须加引号 (simple or double).

--config-file | -c <config file> 使用指定的配置文件, see the example.conf.json.

--user-agent | -a <User-Agent> 使用指定的用户代理。

--cookie <String> 从字符串读取。

--random-agent | -r 使用随机用户代理。

--follow-redirection 如果目标的网址有重定向，它会被跟踪，而不询问你是否想这样做

--batch 从来没有要求用户输入，使用默认的行为。

--no-color 不要在输出中使用颜色

--wp-content-dir <wp content dir> wpscan寻找内容目录（即WP的内容）通过扫描索引页面，但是你可以指定它。 子目录是允许的.

--wp-plugins-dir <wp plugins dir> 同样的事情，但比wp-content目录的插件目录。 如果没有提供，wpscan将wp-content目录/插件。子目录是允许的

--proxy <[protocol://]host:port> 供应代理. HTTP, SOCKS4 SOCKS4A and SOCKS5 are supported.

如果没有协议了（格式主机：端口），会使用HTTP。--proxy-auth <username:password> 提供代理登录凭据。

--basic-auth <username:password> 设置HTTP基本认证。

--wordlist | -w <wordlist> 对于密码暴力破解器供应一个词表。

--username | -U <username> 只有蛮力提供的用户名。

--usernames <path-to-file> 只有蛮力从文件的用户名。

--threads | -t <number of threads> 当多线程请求时使用的线程数。

--cache-ttl <cache-ttl> Typhoeus cache TTL.

--request-timeout <request-timeout> 请求超时。

--connect-timeout <connect-timeout> 连接超时。

--max-threads <max-threads> 最大线程。

--throttle <milliseconds> 在做另一个Web请求之前等待的毫秒。如果使用的话，线程应该设置为1。

--help | -h 此帮助屏幕。

--verbose | -v 详细输出。

--version 输出当前版本和退出。

例子 :

-进一步的帮助 ...

ruby ./wpscan.rb --help

-做'非侵入性的检查 ...

ruby ./wpscan.rb --url www.example.com

-做单词表密码暴力破解枚举用户使用50个线程 ...

ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

-做单词表密码暴力破解的“管理员”用户只...

ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin

-枚举安装插件 ...

ruby ./wpscan.rb --url www.example.com --enumerate p

-枚举安装主题 ...

ruby ./wpscan.rb --url www.example.com --enumerate t

-列举用户...

ruby ./wpscan.rb --url www.example.com --enumerate u

-枚举安装timthumbs ...

ruby ./wpscan.rb --url www.example.com --enumerate tt

-使用HTTP代理 ...

ruby ./wpscan.rb --url www.example.com --proxy 127.0.0.1:8118

-使用SOCKS5代理 ... (cURL >= v7.21.7 needed)

ruby ./wpscan.rb --url www.example.com --proxy socks5://127.0.0.1:9000

-使用自定义内容目录 ...

ruby ./wpscan.rb -u www.example.com --wp-content-dir custom-content

-自定义插件目录...

ruby ./wpscan.rb -u www.example.com --wp-plugins-dir wp-content/custom-plugins

-更新数据库 ...

ruby ./wpscan.rb --update

-调试输出 ...

ruby ./wpscan.rb --url www.example.com --debug-output 2>debug.log

See README for further information.