Oups! No translations found for your language... Using english.

Please send your translations for improvements.

===============================================================

Wapiti-2.3.0 (wapiti.sourceforge.net)

Wapiti-2.3.0 - Web application vulnerability scanner

格式: python wapiti.py http://server.com/base/url/ [options]

支持的选项:

-s <url>

--start <url>

要指定要开始的网址。这个选项可以被称为几次。

Wapiti会浏览这些链接，即使指定的链接不在范围内找到更多的网址。

-x <url>

--exclude <url>

排除一个URL从扫描（如：注销URL）。这个选项可以被称为几次来指定几个网址。 通配符（\*）可以使用URL基本正则表达式。

例子: -x http://server/base/?page=\*&module=test

or -x http://server/base/admin/\* to exclude a directory.

-p <url\_proxy>

--proxy <url\_proxy>

指定代理。目前支持HTTP和HTTPS代理。

这个选项可以被调用两次指定的HTTP和HTTPS代理。

例子: -p http://proxy:port/

-c <cookie\_file>

--cookie <cookie\_file>

输入要用于扫描的饼干。Cookie文件必须以JSON格式。

Cookies can be grabbed using the cookie.py and getcookie.py utilities (net directory).

-t <timeout>

--timeout <timeout>

要设置超时时间（在秒的最大时间等待服务器发送响应）。

-a <login%password>

--auth <login%password>

对于HTTP身份验证凭据集。

--auth-method <method>

如果服务器需要身份验证，则设置使用该身份验证方法的身份验证方法。

目前支持的方法是（一些需要额外的模块来安装）：

+ basic

+ digest

+ kerberos

+ ntlm

-r <parameter\_name>

--remove <parameter\_name>

从网址删除参数（名称和值）。

-n <limit>

--nice <limit>

定义一个限制的网址以相同的模式浏览（即相同参数的最大值的最大值）。

使用此选项在扫描过程中防止无休止的循环。限制必须大于0。

-m <module\_options>

--module <module\_options>

设置模块（HTTP方法为每个模块）用于攻击。

模块名称前缀加停用相关模块。

只浏览目标（不发送任何有效载荷），使每个模块-“-all”。

如果你不指定HTTP GET和POST方法，将使用。

例子: -m "-all,xss:get,exec:post"

-u

--color

使用颜色突出显示输出中的漏洞和异常。

-v <level>

--verbose <level>

设置的详细程度。

0: quiet (default), 1: print each URL, 2: print every attack.

-b <scope>

--scope <scope>

设置扫描的范围：

+ page: 仅分析给定作为根网址的页面。

+ folder: 分析所有的URL传递到马鹿的根URL下（默认）。

+ domain: 分析所有的链接，在同一个域的URL传递到马鹿页。

-f <type\_file>

--format <type\_file>

为报表设置格式类型。

json: JSON格式的报告

html: HTML格式的报告（默认）

openvas: 在OpenVAS XML格式的报告

txt: 在普通文本报告（UTF-8）

vulneranet: VulneraNET在报告中（基于XML）格式

xml: XML格式报告

-o <output>

--output <output\_file>

设置报表文件的名称

如果选定的报告格式为“HTML”，此参数将作为目录名称。

-i <file>

--continue <file>

此参数表示瓦皮蒂恢复以前的扫描保存在指定的XML状态文件。

文件名称是可选的，如果没有指定，Wapiti作为默认的文件从“扫描”文件夹。

-k <file>

--attack <file>

此参数表示瓦皮蒂没有扫描网站的再次攻击，从指定的文件中加载扫描状态。

文件名称是可选的，如果没有指定，默认的文件从Wapiti以“扫描”的文件夹。

--verify-ssl <0|1>

此参数表示是否马鹿必须检查SSL证书。

默认是验证证书

-h

--help

打印此使用消息