Wapiti 3 Cheatsheet (ingenieriainformatica.uniovi.es)

Website vulnerability scanner

https://wapiti.sourceforge.io/

GENERAL USAGE

```
wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}]
[-m MODULES_LIST] [--list-modules] [-l LEVEL] [-p PROXY_URL]
[--tor] [-a CREDENTIALS]
[--auth-type {basic,digest,kerberos,ntlm}] [-c COOKIE_FILE]
[--skip-crawl] [--resume-crawl] [--flush-attacks]
[--flush-session] [--store-session PATH] [-s URL] [-x URL]
[-r PARAMETER] [--skip PARAMETER] [-d DEPTH]
[--max-links-per-page MAX] [--max-files-per-dir MAX]
[--max-scan-time MINUTES] [--max-parameters MAX] [-S FORCE]
[-t SECONDS] [-H HEADER] [-A AGENT] [--verify-ssl {0,1}]
[--color] [-v LEVEL] [-f FORMAT] [-o OUPUT_PATH]
[--external-endpoint EXTERNAL_ENDPOINT_URL]
[--internal-endpoint INTERNAL_ENDPOINT_URL]
[--endpoint ENDPOINT_URL] [--no-bugreport] [--version]
```

EXAMPLES

wapiti http://<url> -n 10 -b folder -u -v 1 -f html -o /tmp/scan_report

wapiti http://<url>/path -u -n 5 -b domain -v 2 -o /tmp/outfile.html

wapiti http://<url>/path -u -n 5 -b domain -m "-all,sql,blindsql" -v 2 -o /tmp/outfile.html

OPTIONAL ARGUMENTS

-A AGENT, --user-agent AGENT: Set a custom user-agent to use for every requests

-a CREDENTIALS, --auth-cred CREDENTIALS: Set HTTP authentication credentials

--auth-type {basic,digest,kerberos,ntlm}: Set the authentication type to use

-c COOKIE_FILE, --cookie COOKIE_FILE: Set a JSON cookie file to use

--color: Colorize output

-d DEPTH, --depth DEPTH: Set how deep the scanner should explore the website

--endpoint ENDPOINT_URL: Url serving as endpoint for both attacker and target

--external-endpoint EXTERNAL_ENDPOINT_URL: Url serving as endpoint for target

-f FORMAT, --format FORMAT: Set output format. Supported: json, html (default), txt, openvas, vulneranet, xml

--flush-attacks: Flush attack history and vulnerabilities for the current session

--flush-session: Flush everything that was previously found for this target (crawled URLs, vulns, etc)

-H HEADER, --header HEADER: Set a custom header to use for every requests

-h, --help: Show this help message and exit

--internal-endpoint INTERNAL_ENDPOINT_URL: Url serving as endpoint for attacker

-l LEVEL, --level LEVEL: Set attack level

--list-modules: List Wapiti attack modules and exit

-m MODULES_LIST, --module MODULES_LIST: List of modules to load

--max-files-per-dir MAX: Set how many pages the scanner should explore per directory

--max-links-per-page MAX: Set how many (in-scope) links the scanner should extract for each page

--max-parameters MAX: URLs and forms having more than MAX input parameters will be erased before attack.

--max-scan-time MINUTES: Set how many minutes you want the scan to last (floats accepted)

--no-bugreport: Don't send automatic bug report when an attack module fails

-o OUPUT_PATH, --output OUPUT_PATH: Output file or folder

-p PROXY_URL, --proxy PROXY_URL: Set the HTTP(S) proxy to use. Supported: http(s) and socks proxies

-r PARAMETER, --remove PARAMETER: Remove this parameter from urls

--resume-crawl: Resume the scanning process (if stopped) even if some attacks were previously performed

-S FORCE, --scan-force FORCE: Easy way to reduce the number of scanned and attacked URLs.
Possible values: paranoid, sneaky, polite, normal, aggressive, insane

-s URL, --start URL: Adds an url to start scan with

--scope {page,folder,domain,url,punk}: Set scan scope

--skip PARAMETER: Skip attacking given parameter(s)

--skip-crawl: Don't resume the scanning process, attack URLs scanned during a previous session

--store-session PATH: Directory where to store attack history and session data.

-t SECONDS, --timeout SECONDS: Set timeout for requests

--tor: Use Tor listener (127.0.0.1:9050)

-u URL, --url URL: The base URL used to define the scan scope (default scope is folder)

-v LEVEL, --verbose LEVEL: Set verbosity level (0: quiet, 1: normal, 2: verbose)

--verify-ssl {0,1}: Set SSL check (default is no check)

--version: Show program's version number and exit

-x URL, --exclude URL: Adds an url to exclude from the scan

by José Manuel Redondo López