dotdotpwn Cheatsheet (ingenieriainformatica.uniovi.es)

Automated scanning tool for File Inclusion vulnerabilities in URL paths

https://github.com/wireghoul/dotdotpwn

GENERAL USAGE

```
./dotdotpwn.pl -m <module> -h <host> [OPTIONS]
```

NOTES

May give false positives if navigation to an URL returns a default web page instead of an error, manual check of allegedly VULNERABLE! URLs must be done to be sure about its results

```
8etc%uEFC8issue <- VULNERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uEFC8??%uEFC8??%uEFC8??%uEFC8??%uEFC
8??%uEFC8etc%uEFC8passwd <- VULNERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uEFC8??%uEFC8??%uEFC8??%uEFC8??%uEFC
8??%uEFC8etc%uEFC8issue <- VULNERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uF025etc%uF025passwd <- VULNERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uF025etc%uF025issue <- VULNERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uF025??%uF025etc%uF025passwd <- VULN
ERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uF025??%uF025etc%uF025issue <- VULNE
RABLE!
[*] Testing Path: http://192.168.14.2:80/??%uF025??%uF025??%uF025etc%uF025passwd
<- VULNERABLE!
[*] Testing Path: http://192.168.14.2:80/??%uF025??%uF025??%uF025etc%uF025issue
<- VULNERABLE!
```

OPTIONS

-b: Break after the first vulnerability is found	**-o**: Operating System type if known ("windows", "unix" or "generic")
-C: Continue if no data was received from host	**-p**: Filename with the payload to be sent and the part to be fuzzed marked with the TRAVERSAL keyword
-d: Depth of traversals (e.g. deepness 3 equals to ../../../; default: 6)	**-P**: Password (default: 'dot@dot.pwn')
-E: Add @Extra_files in TraversalEngine.pm (e.g. web.config, httpd.conf, etc.)	**-q**: Quiet mode (doesn't print each attempt)
-e: File extension appended at the end of each fuzz string (e.g. ".php", ".jpg", ".inc")	**-r**: Report filename (default: 'HOST_MM-DD-YYYY_HOUR-MIN.txt')
-f: Specific filename (e.g. /etc/motd; default: according to OS detected, defaults in TraversalEngine.pm)	**-s**: Service version detection (banner grabber)
-h: Hostname	**-S**: Use SSL for HTTP and Payload module (not needed for http-url, use a https:// url instead)
-k: Text pattern to match in the response (http-url & payload modules - e.g. "root:" if trying /etc/passwd)	**-t**: Time in milliseconds between each test (default: 300 (.3 second))
-M: HTTP Method to use when using the 'http' module [GET | POST | HEAD | COPY | MOVE] (default: GET)	**-u**: URL with the part to be fuzzed marked as TRAVERSAL (e.g. http://foo:8080/id.php?x=TRAVERSAL&y=31337)
-m: Module [http | http-url | ftp | tftp | payload | stdout]	**-U**: Username (default: 'anonymous')
-O: Operating System detection for intelligent fuzzing (nmap)	**-x**: Port to connect (default: HTTP=80; FTP=21; TFTP=69)
EXAMPLES	**-X**: Use the Bisection Algorithm to detect the exact deepness once a vulnerability has been found
dotdotpwn -m http -h 192.168.14.2	

by José Manuel Redondo López