Презентация по этапу №4

Использование nikto

Галацан Николай

Российский университет дружбы народов, Москва, Россия

Докладчик

- Галацан Николай
- · 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов



Научиться использовать инструмент для сканирования на уязвимости nikto.

```
ngalacan@ngalacan: ~
File Actions Edit View Help
$ nikto -h
Option host requires an argument
       -ask+
                           Whether to ask about submitting updates
                               ves Ask about each (default)
                                     Don't ask, don't send
                               auto Don't ask, just send
       -check6
                           Check if IPv6 is working (connects to ipv6.google.com
or value set in nikto.conf)
                           Scan these CGI dirs: "none", "all", or values like "/c
                           Use this config file
                           Turn on/off display outputs:
       -Display+
                                     Show redirects
                                     Show cookies received
                                     Show all 200/OK responses
                                     Show URLs which require authentication
                                     Debug output
                                     Display all HTTP errors
                                     Print progress to STDOUT
                                     Scrub output of IPs and hostnames
                                     Verbose output
       -dbcheck
                          Check database and other key files for syntax errors
                          Encoding technique:
                                     Random URI encoding (non-UTF8)
                                     Directory self-reference (/./)
                                     Premature URL ending
                                     Prepend long random string
                                     Fake parameter
                                     TAB as request spacer
                                     Change the case of the URL
                                     Use Windows directory separator (\)
                                     Use a carriage return (0×0d) as a request sp
```

Рис. 1: Справка

```
_$ nikto -h gazel.me
- Nikto v2.5.0
+ Multiple TPs found: 85.119.149.161. 2a00:ab00:1103:7:23::1
+ Target IP:
                      85.119.149.161
+ Target Hostname:
                     gazel.me
+ Target Port:
+ Start Time:
                      2024-03-22 19:55:51 (GMT3)
+ Server: nginx/1.20.2
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mo
zilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: PHP/5.5.38.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://dev
eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type. See: h
ttps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten
t-type-header/
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://deve
loper.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Web Server returns a valid response with junk HTTP methods which may cause fa
lse positives.
+ /?mod=<script>alert(document.cookie)</script>Gop=browse: Sage 1.0b3 is vulnerabl
e to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?nam
0-CVE-2003-1242
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-r
estricting-access-to-iconsreadme/
+ 8770 requests: 1 error(s) and 9 item(s) reported on remote host
                      2024-03-22 19:58:11 (GMT3) (140 seconds)
+ Fnd Time:
+ 1 host(s) tested
```

```
-$ nikto -h 127.0.0.1
  Nikto v2.5.0
 Target TP:
                     127.0.0.1
+ Target Hostname:
                     127.0.0.1
+ Target Port:
+ Start Time:
                      2024-03-22 19:53:24 (GMT3)
+ Server: Apache/2.4.58 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://dev
eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type. See: h
ttps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten
t-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size
: 6124d1e7a22be, mtime: gzip, See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=C
VE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ ///etc/hosts: The server install allows reading of any system file by adding an
extra '/' to the URL
+ /server-status: This reveals Apache information. Comment out appropriate line in
the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /wn-content/themes/twentveleven/images/headers/server.php?filesrc=/etc/hosts: A
PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentveleven/images/headers/server.php?filesrc=/etc
/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoo
r file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A P
```

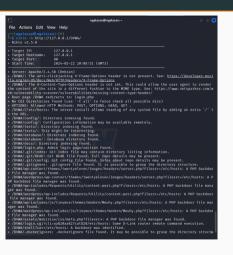


Рис. 4: Сканирование DVWA

Приобретены навыки использования nikto для сканирования веб-серверов на уязвимости. Сканер nikto позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения.