

Индивидуальный проект. Этап №4

Использование nikto

Камкина А. Л.

Информация

Докладчик

- Камкина Арина Леонидовна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- 1032216456@pfur.ru
- <https://alkamkina.github.io/ru/>



Вводная часть

Цели и задачи

Цель работы:

На практике попробовать использовать сканер безопасности веб-сервера nikto.

Задачи:

- Создать файл-отчёт уязвимостей веб-сервера
- Проанализировать отчёт

Инструмент: VirtualBox

Выполнение лабораторной работы

Nikto установлен

```
(alkamkina@alkamkina)-[~]
$ nikto
- Nikto v2.5.0

+ ERROR: No host (-host) specified

Options:
  -ask+           Whether to ask about submitting updates
                   yes   Ask about each (default)
                   no   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)
  -Cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+        Use this config file
  -Display+       Turn on/off display outputs:
                   1     Show redirects
                   2     Show cookies received
                   3     Show all 200/OK responses
                   4     Show URLs which require authentication
                   D     Debug output
                   E     Display all HTTP errors
                   P     Print progress to STDOUT
                   S     Scrub output of IPs and hostnames
                   V     Verbose output
  -dbcheck        Check database and other key files for syntax errors
  -evasion+       Encoding technique:
                   1     Random URI encoding (non-UTF8)
                   2     Directory self-reference (../)
                   3     Premature URL ending
                   4     Prepend long random string
                   5     Fake parameter
                   6     TAB as request spacer
                   7     Change the case of the URL
                   8     Use Windows directory separator (\)
                   A     Use a carriage return (0x0d) as a request spacer
                   B     Use binary value 0x0b as a request spacer
  -followredirects Follow 3xx redirects to new location
  -Format+        Save file (-o) format:
                   csv   Comma-separated-value
                   json  JSON Format
                   htm   HTML Format
                   nbe   Nessus NBE format
                   sql   Generic SQL (see docs for schema)
                   txt   Plain text
                   xml   XML Format
                   (if not specified the format will be taken from the file extens
ion passed to -output)
  -Help           This help information
  -host+          Target host/URL
  -id+            Host authentication to use, format is id:pass or id:pass:realm
  -ipv4           IPv4 Only
  -ipv6           IPv6 Only
```

Проверка установки nikto

Запуск анализа

```
(alkamkina@alkamkina)-[~]
$ nikto -h http://localhost/DVWA/ -o report.html -Format htm
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-04 18:55:24 (GMT3)

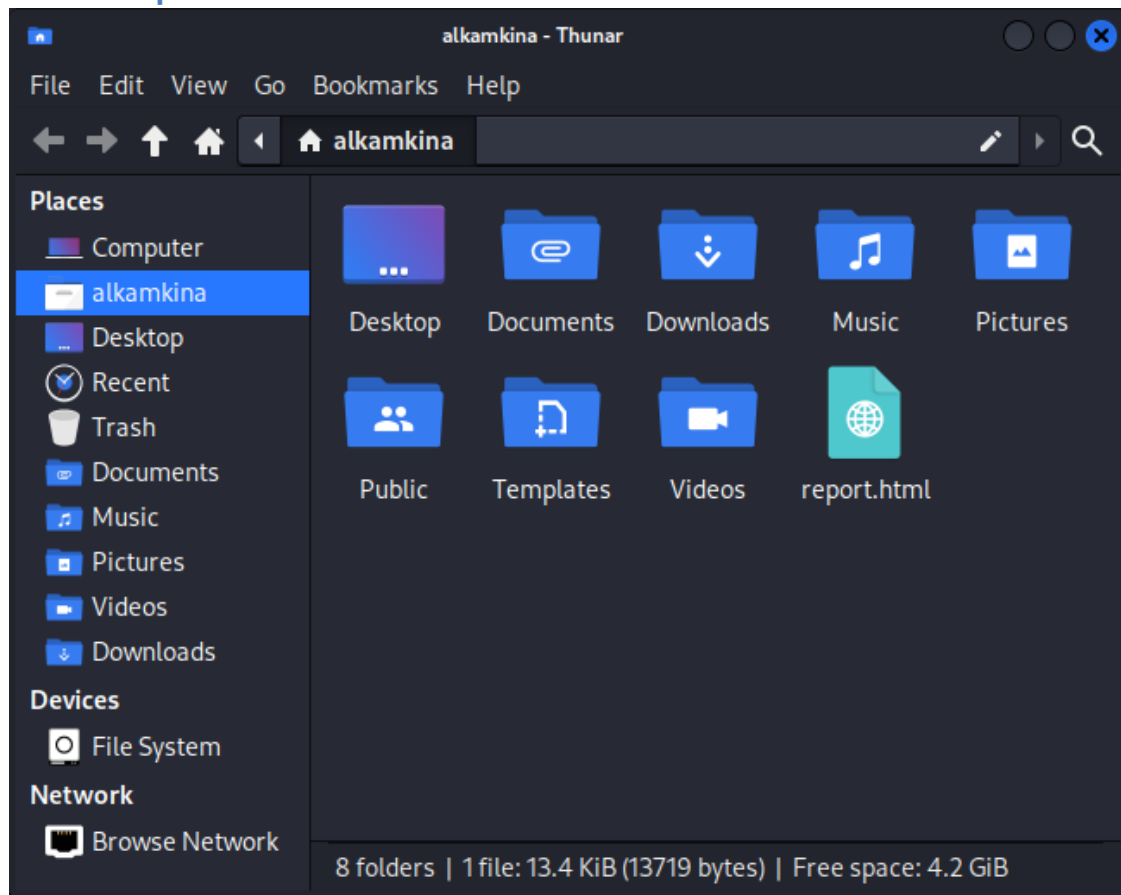
+ Server: Apache/2.4.62 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DVWA/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/tests/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/login.php: Admin login page/section found.
+ /DVWA/.git/index: Git Index file may contain directory listing information.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time: 2024-10-04 18:55:41 (GMT3) (17 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.62) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n
```

Запуск анализа

Файл сохранен



Расположение файла

Анализ уязвимостей

HTTP Method	GET
Description	/DVWA/login.php: Admin login page/section found.
Test Links	http://localhost:80/DVWA/login.php http://127.0.0.1:80/DVWA/login.php
References	
URI	/DVWA/.git/index
HTTP Method	GET
Description	/DVWA/.git/index: Git Index file may contain directory listing information.
Test Links	http://localhost:80/DVWA/.git/index http://127.0.0.1:80/DVWA/.git/index
References	
URI	/DVWA/.git/HEAD
HTTP Method	GET
Description	/DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
Test Links	http://localhost:80/DVWA/.git/HEAD http://127.0.0.1:80/DVWA/.git/HEAD
References	
URI	/DVWA/.git/config
HTTP Method	GET
Description	/DVWA/.git/config: Git config file found. Infos about repo details may be present.
Test Links	http://localhost:80/DVWA/.git/config http://127.0.0.1:80/DVWA/.git/config
References	
URI	/DVWA/.gitignore
HTTP Method	GET
Description	/DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
Test Links	http://localhost:80/DVWA/.gitignore http://127.0.0.1:80/DVWA/.gitignore
References	
URI	/DVWA/.dockerignore
HTTP Method	GET
Description	/DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
Test Links	http://localhost:80/DVWA/.dockerignore http://127.0.0.1:80/DVWA/.dockerignore
References	
Host Summary	
Start Time	2024-10-04 18:55:24
End Time	2024-10-04 18:55:41
Elapsed Time	17 seconds
Statistics	7850 requests, 0 errors, 16 findings
Scan Summary	
Software Details	Nikto 2.5.0
CLI Options	-h http://localhost/DVWA/ -o report.html -Format htm
Hosts Tested	1
Start Time	Fri Oct 4 18:55:24 2024
End Time	Fri Oct 4 18:55:41 2024
Elapsed Time	17 seconds

© 2008 Chris Sullo

Анализ уязвимостей

Заключение

Вывод

На практике посмотрели уязвимости веб-сервера.