

**Индивидуальный проект. Отчёт о
выполнении №4
Информационная безопасность
Использование Nikto**

Выполнил: Мальков Роман Сергеевич,
НФИбд-02-21, 1032217048

Содержание

Цель работы	4
Использование Nikto	5
Заключение	9
Ссылки	10

Список иллюстраций

1	Проверка	5
2	сканирование DVWA	5
3	сканирование с указанием порта	6
4	сканирования с maxtime и Pause	6
5	сканирование с Tuning	7
6	сканирование с evasion	8
7	Сохраним отчет	8
8	Отчет	8

Цель работы

Рассмотреть и применить утилиту nikto для просмотра уязвимостей веб приложения DVWA.

Использование Nikto

Посмотрим версию nikto и проверим базы данных на ошибки.

```
(rsnaljkov@kali)-[~]
$ nikto -Version
Nikto 2.5.0 (LW 2.5)

(rsnaljkov@kali)-[~]
$ nikto -dbcheck
Syntax Check: /var/lib/nikto/databases/db_404_strings
39 entries
Syntax Check: /var/lib/nikto/databases/db_multiple_index
35 entries
Syntax Check: /var/lib/nikto/databases/db_outdated
1256 entries
Syntax Check: /var/lib/nikto/databases/db_domino
274 entries
Syntax Check: /var/lib/nikto/databases/db_dictionary
1825 entries
Syntax Check: /var/lib/nikto/databases/db_tests
```

Рис. 1: Проверка

Попробуем просканировать DVWA

```
(rsnaljkov@kali)-[~]
$ nikto -host 127.0.0.1
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-10-03 06:12:16 (GMT-4)

+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.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: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-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: 6215c2d80f8d9, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ///etc/passwd: 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
```

Рис. 2: сканирование DVWA

Также дополнительно можно указать порт

```
(rsmaljkov@kali)-[~]
$ nikto -host 127.0.0.1 -port 80
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-10-03 06:16:40 (GMT-4)

+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.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: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-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: 6215c2d80f8d9, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /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-544
```

Рис. 3: сканирование с указанием порта

Укажем параметр maxtime, отвечающий за длительность работы сканирования, а также параметр Pause, отвечающий за паузу между выполнением запросов

```
(rsmaljkov@kali)-[~]
$ nikto -host 127.0.0.1 -maxtime 5 -Pause 2
-***** Pausing 2 second(s) per request
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-10-03 06:33:33 (GMT-4)

+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.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: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ ERROR: Host maximum execution time of 5 seconds reached
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:       2024-10-03 06:33:41 (GMT-4) (8 seconds)

+ 1 host(s) tested

(rsmaljkov@kali)-[~]
$
```

Рис. 4: сканирования с maxtime и Pause

При помощи параметра Tuning можно выбрать тип теста приложения:

- 0 - File Upload
- 1 - Interesting File / Seen in Logs
- 2 - Misconfiguration / Default File

- 3 - Information Disclosure
- 4 - (XSS/Script/HTML) Injection
- 5 - Remote file retrieval Inside web root
- 6 - Denial of service
- 7 - Remote file retrieval / Server wide
- 8 - Command exec / Remote shell
- 9 - SQL Injection
- a - Authentication Bypass
- b - Software Indetification
- c - Remote source Inclusion
- x - Reverse tuning options

```

(rsmal)kov@kali:~$ nikto --host 127.0.0.1 -Tuning 1
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-10-03 06:39:21 (GMT+4)

+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.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: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
  
```

Рис. 5: сканирование с Tuning

Для того чтобы обойти систему обнаружения вторжения, можно воспользоваться параметром evasion:

- 1 - Random URI encoding
- 2 - Directory self reference (/./)
- 3 - Premature URL ending
- 4 - Prepend long random string
- 5 - Fake parameter
- 6 - TAB as request spacer
- 7 - Change case of URL
- 8 - Use Windows directory separator

```

(rsmaljkov@kali)-[~]
$ nikto --host 127.0.0.1 -evasion 7
+ Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Using Encoding: Change the case of the URI
+ Start Time: 2024-10-03 06:42:35 (GMT+4)

+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.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 ty

```

Рис. 6: сканирование с evasion

Сохраним отчет в определенном формате используя параметры о и Format

```

(rsmaljkov@kali)-[~]
$ nikto --host 127.0.0.1 -evasion 4 -tuning 9 -o /home/nikto -Format htm

```

Рис. 7: Сохраним отчет

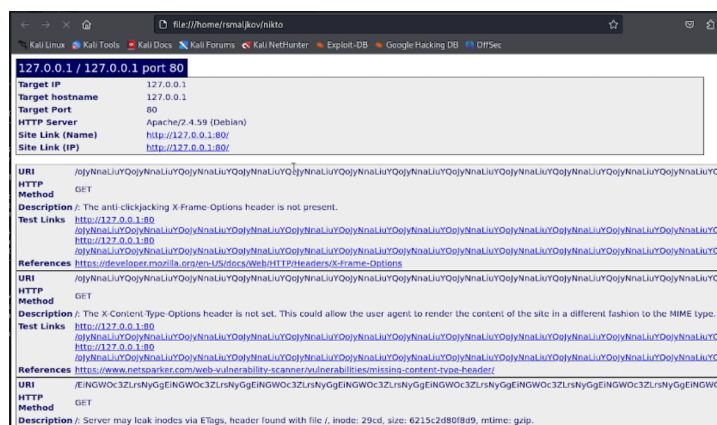


Рис. 8: Отчет

Заключение

Были получены базовые навыки работы с утилитой `nikto`.

Ссылки

“Nikto vulnerability scanner: Complete guide”: <https://www.hackercoolmagazine.com/nikto-vulnerability-scanner-complete-guide/>