

# Проект этап 4

---

Malkov Roman Sergeevich

24.09.2024

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

# Использование Nikto

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

# Использование Nikto

```
(ramaljkov@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

# Использование Nikto

```
(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/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-3748
```

Рис. 3: сканирование с указанием порта

# Использование Nikto

```
(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

# Использование Nikto

```
(rsmaljkov@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

# Использование Nikto

```
(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 URL  
+ 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



A terminal window with a dark background. The prompt is '(rsmaljkov@kali)-[~]'. The command entered is 'nikto --host 127.0.0.1 -evasion 4 -tuning 9 -o /home/nikto -Format htm'.

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

**Рис. 7:** Сохраним отчет

# Использование Nikto

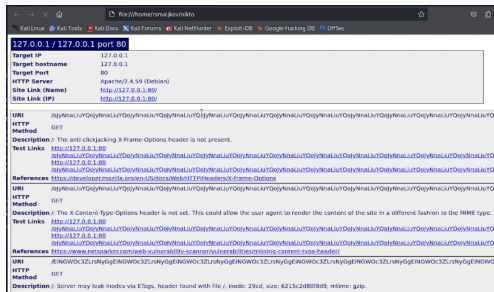


Рис. 8: Отчет

Были получены базовые навыки работы с утилитой nikto.