

# Индивидуальный проект - этап 4

## Использование nikto

Овезов Мерген

### Содержание

#### 1 Цель работы

Освоить работу с инструментом Nikto для выявления уязвимостей веб-приложений и веб-серверов, провести сканирование DVWA и проанализировать результаты.

#### 2 Исходные условия

Целевая система: DVWA (Damn Vulnerable Web Application)

Уровень безопасности: Low

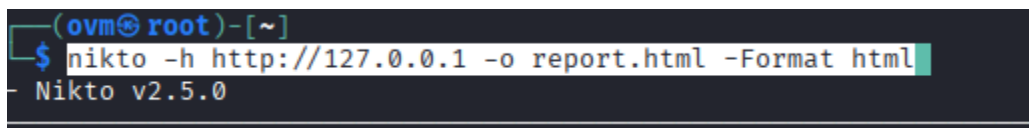
Метод авторизации: HTTP POST Form

Инструмент: Nikto v2.5.0

#### 3 Выполнение работы

Запустить DVWA и убедиться в доступности веб-приложения.

Составить команду nikto:



```
(ovm@ root) - [~]  
$ nikto -h http://127.0.0.1 -o report.html -Format html  
- Nikto v2.5.0
```

Figure 1: запуск команды nikto

Дождаться завершения сканирования и зафиксировать найденные уязвимости.

```

(ovm@root)-[~]
$ nikto -h http://127.0.0.1 -o report.html -Format html
Nikto v2.5.0

- Target IP: 127.0.0.1
- Target Hostname: 127.0.0.1
- Target Port: 80
- Start Time: 2025-09-13 19:49:42 (GMT3)

- Server: Apache/2.4.65 (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/
- /: Directory indexing found.
- No CGI Directories found (use '-C all' to force check all possible dirs)
- OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
- /.: Directory indexing found.
- /.: Appending './' to a directory allows indexing.
- //: Directory indexing found.
- ///: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page
- /%2e/: Directory indexing found.
- /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
- ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
- ///: Directory indexing found.
- /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
- /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
- /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
- //////////////////////////////////////
- //////////////////////////////////////: Directory indexing found.
- //////////////////////////////////////
- //////////////////////////////////////: Abyss 1.03 reveals directory listing when multiple '/'s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
- /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was

```

Figure 2: найденные уязвимости:

Nikto выполнил 8074 запроса, найдено 26 потенциальных уязвимостей

### 3 Вывод

Nikto выявил критические уязвимости, позволяющие удалённый доступ и выполнение команд. Для повышения безопасности необходимо удалить вредоносные файлы, обновить ПО и ограничить доступ к служебным ресурсам.