

Индивидуальный проект - этап 4

Ларина Наталья¹

14 марта, 2025, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение сканера уязвимостей nikto.

Процесс выполнения лабораторной работы

Nikto — это популярный сканер веб-серверов с открытым исходным кодом, который проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности.

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе.

Сканирование веб-сервера

```
perl nikto.pl -h <URL>
```

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию.

Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

```
perl nikto.pl -h http://localhost/dvwa/
```

Сканирование localhost

```
(user@ndlarina)~$ nikto -h http://localhost
- Nikto v2.5.0

+ Target IP:      127.0.0.1      255 (Preferred)
+ Target Hostname: localhost    255 (Default)
+ Target Port:    80            255 (Default)
+ Start Time:     2025-03-14 08:25:03 (GMT-4) 255 (Default)

+ Server: Apache/2.4.62 (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: 29cf, size: 62d6610811c8b, mtime: gzip. See: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:      2025-03-14 08:25:12 (GMT-4) (9 seconds)

+ 1 host(s) tested
```

WARNING!
Nikto Vulnerability Web Application is open source. Do not blame or deny Internet hosting services, or they will blame you.

More Training Resources
Nikto aims to assist the most concerning web application security of others issues with their experience. Nikto is made with a lot of experience, and they wish to make it easy for you to use.

Рис. 1: Тестирование localhost

Сканирование localhost/dvwa/

```
(user@ndlarina)-[~]
$ nikto -h http://localhost/dvwa/

Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2025-03-14 08:24:38 (GMT-4)

+ 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/mis-sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ 7849 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2025-03-14 08:24:48 (GMT-4) (10 seconds)

+ 1 host(s) tested
```

Рис. 2: Тестирование localhost/dvwa/

Выводы по проделанной работе

Мы изучили возможности сканера nikto.