

Индивидуальный проект - этап 4

Петров Артем Евгеньевич¹

15 декабря, 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

Введение

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.

Введение

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

Сканирование веб-сервера

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

Сканирование

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@aspetrov) ~
$ nikto -h http://localhost
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:    2025-12-16 10:21:21 (GMT-5)

+ 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: 29kf, size: 62d6610811c8b, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: Server may leak inodes via Etags, header found with file /, inode: 29kf, size: 62d6610811c8b, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /server-status: Status levels Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed hosts. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-561
+ 7858 requests; 0 errors(0) and 5 items(s) reported on remote host
+ End Time:       2025-12-16 10:21:31 (GMT-5) (10 seconds)

+ 1 host(s) tested
```

Рис. 1: Тестирование localhost

Сканирование localhost/dvwa/

```
[user@aspetrov:~] $ nikto -h http://localhost/dvwa/
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:    2025-12-16 10:20:32 (GMT-5)

+ 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/
+ No CGI Directories found (use '-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:    2025-12-16 10:28:41 (GMT-5) (9 seconds)

+ 1 host(s) tested
```

Рис. 2: Тестирование localhost/dvwa/

Выводы по проделанной работе

Вывод

Мы изучили возможности сканера nikto.