

# Индивидуальный проект - этап 4

---

Сморчков Дмитрий<sup>1</sup>

9 ноября, 2024, Москва, Россия

<sup>1</sup>Российский 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@dsmorchkov)-[~]
$ nikto -h http://localhost

- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-11-09 15:36:16 (GMTJ)

+ 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: 621d5e43cc127, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ /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: 2024-11-09 15:36:37 (GMTJ) (21 seconds)

+ 1 host(s) tested
```

Figure 1: Тестирование localhost



# Сканирование localhost/dvwa/

```
(user@dsamorkov) ~  
$ nikto -h http://localhost/DVWA  
  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: localhost  
+ Target Port: 80  
+ Start Time: 2024-11-09 15:37:41 (GMT3)  
  
+ Server: Apache/2.4.59 (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/  
+ Root page /DVWA redirects to: login.php  
+ No CGI Directories found (use "-C all" to force check all possible dirs)  
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .  
+ /DVWA/config/: Directory indexing found.  
+ /DVWA/config/: Configuration information may be available remotely.  
+ /DVWA/tests/: Directory indexing found.  
+ /DVWA/tests/: This might be interesting.  
+ /DVWA/database/: Directory indexing found.  
+ /DVWA/database/: Database directory found.  
+ /DVWA/docs/: Directory indexing found.  
+ /DVWA/login.php: Admin login page/section found.  
+ /DVWA/.git/index: Git Index file may contain directory listing information.  
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.  
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.  
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.  
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.  
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host  
+ End Time: 2024-11-09 15:38:03 (GMT3) (22 seconds)  
  
+ 1 host(s) tested
```

Figure 2: Тестирование localhost/dvwa/

## **Выводы по проделанной работе**

---

Мы изучили возможности сканера nikto.