

Отчет по четвертому этапу индивидуального проекта

Дисциплина: Основы информационной безопасности

Иванов Сергей Владимирович, НПИбд-01-23

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Выводы	9

Список иллюстраций

3.1	Запуск DVWA	6
3.2	Выбор уровня безопасности	7
3.3	Запуск nikto	7
3.4	Сканирование	8
3.5	Сканирование	8

1 Цель работы

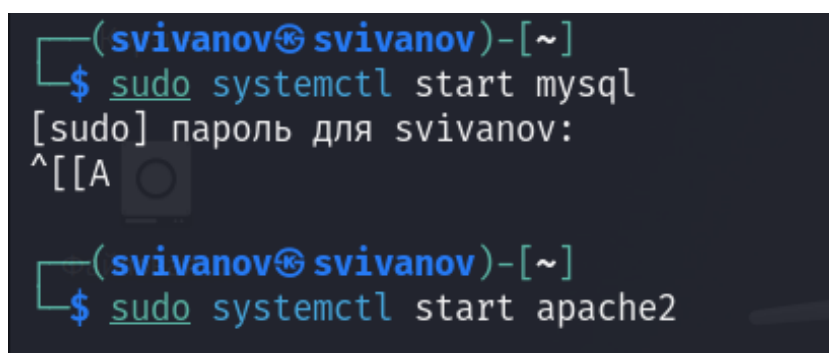
Просканировать веб-приложение используя сканер nikto.

2 Задание

1. Использовать nikto

3 Выполнение лабораторной работы

Для начала запустим веб приложение DVWA. Для этого необходимо запустить mysql и apache2. (рис. 1).



```
(svivanov@svivanov)-[~]  
$ sudo systemctl start mysql  
[sudo] пароль для svivanov:  
^[A  
  
(svivanov@svivanov)-[~]  
$ sudo systemctl start apache2
```

Рис. 3.1: Запуск DVWA

Захожу на сайт DVWA и перехожу во вкладку DWVA Security. Выбираю низкий уровень безопасности. (рис. 2)

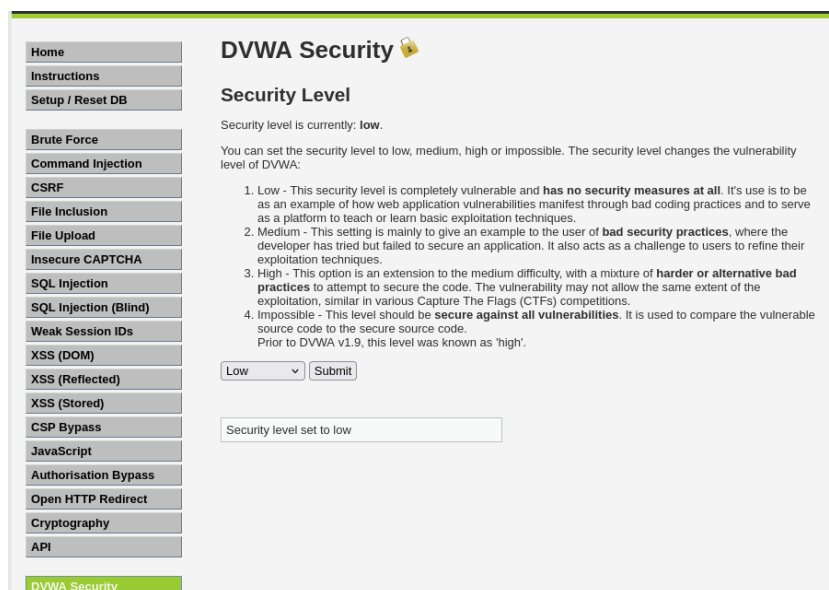


Рис. 3.2: Выбор уровня безопасности

Запускаю сканер nikto. (рис. 3)

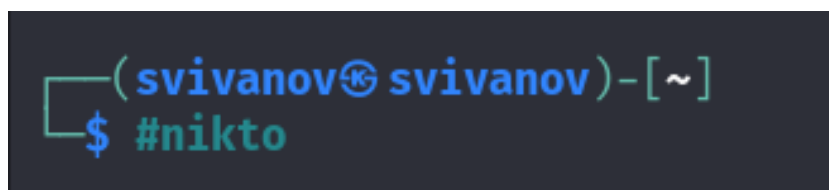


Рис. 3.3: Запуск nikto

Запускаю сканирование веб приложения вводя URL адрес. (рис. 4)

```

(svivanov@svivanov)-[~]
$ nikto -h http://127.0.0.1/DWVA/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-10 13:44:58 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /DWVA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DWVA/: 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)
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /DWVA///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /DWVA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /DWVA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /DWVA/shell?cat+/etc/hosts: A backdoor was identified.
+ 8073 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2025-04-10 13:45:17 (GMT3) (19 seconds)

```

Рис. 3.4: Сканирование

Запускаю сканирование вводя номер порта и адрес порта. (рис. 5)

```

(svivanov@svivanov)-[~]
$ nikto -h 127.0.0.1 -p 80
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-10 13:46:35 (GMT3)

+ 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: 62fac5ae956b8, mime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418

```

Рис. 3.5: Сканирование

4 Выводы

Получены практические навыки по использованию `nikto` для сканирования веб приложений.