

# **Индивидуальный проект 4**

Генералов Даниил, 1032212280

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>9</b>

# Список иллюстраций

2.1	nikto . . . . .	6
2.2	nikto . . . . .	7
2.3	nikto . . . . .	7

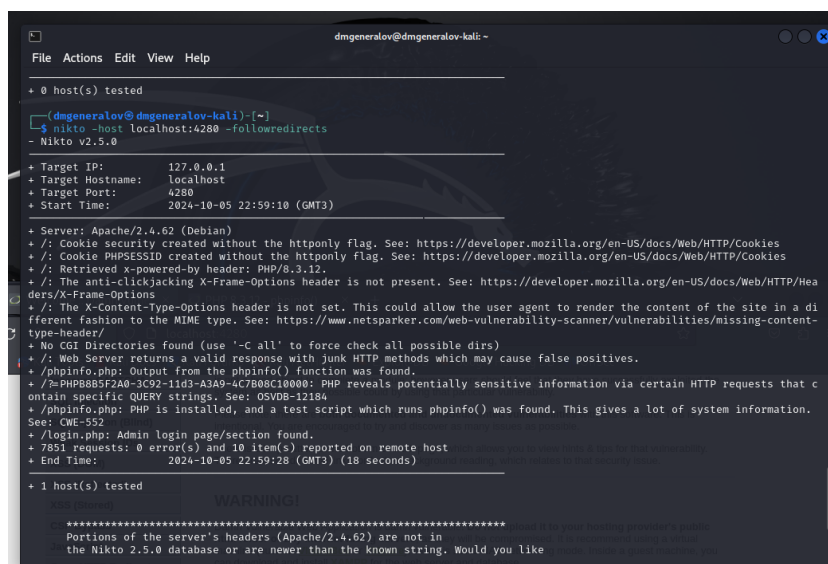
## **Список таблиц**

# 1 Цель работы

В этом этапе индивидуального проекта требуется использовать сканер уязвимостей nikto, чтобы найти какие-то уязвимости в DVWA.

## 2 Выполнение лабораторной работы

Сканер nikto уже идет в стандартной установке Kali Linux. Мы просто запускаем его, направляя его на адрес, где развернут DVWA, и получаем список потенциальных проблем (рис. 2.1).

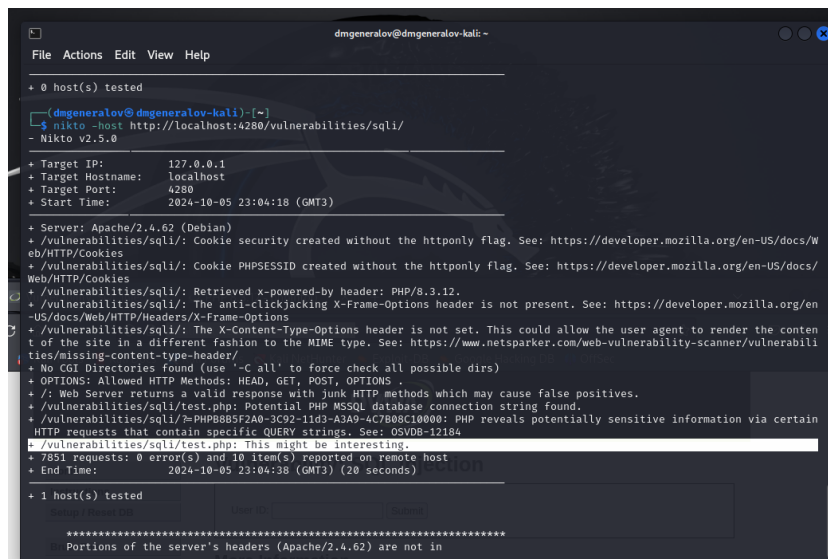


```
dmgeneralov@dmgeneralov-kali: ~  
File Actions Edit View Help  
+ 0 host(s) tested  
  
[dmgeneralov@dmgeneralov-kali:~]  
$ nikto -host localhost:4280 -followredirects  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: localhost  
+ Target Port: 4280  
+ Start Time: 2024-10-05 22:59:10 (GMT3)  
  
+ Server: Apache/2.4.62 (Debian)  
+ /: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /: Retrieved x-powered-by header: PHP/8.3.12.  
+ /: 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)  
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.  
+ /phpinfo.php: Output from the phpinfo() function was found.  
+ /?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184  
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CVE-552  
+ /login.php: Admin login page/section found.  
+ 7851 requests: 0 error(s) and 10 item(s) reported on remote host  
+ End Time: 2024-10-05 22:59:28 (GMT3) (18 seconds)  
  
+ 1 host(s) tested  
  
WARNING!  
*****  
Portions of the server's headers (Apache/2.4.62) are not in the Nikto 2.5.0 database or are newer than the known string. Would you like to update the database?  
*****
```

Рис. 2.1: nikto

К сожалению, большинство из этих проблем не слишком интересные, например тот факт что сервер раскрывает версию PHP на которой он работает.

Более интересный вывод можно получить, направив его на какую-то страницу, которая демонстрирует уязвимость. Например, на странице с SQL-инъекцией, он обнаружил, что может быть что-то интересное в скрипте, который используется для выдачи данных для формы (рис. 2.2).



Также можно найти уязвимость, связанную с подключением файлов: скрипт `include.php` может вернуть содержимое файлов в файловой системе (вроде `/etc/passwd`) и на HTTP-сайтах (рис. 2.3).

Рис. 2.3: nikto

Nikto не имеет автоматического рекурсивного сканирования, поэтому можно использовать другую программу, чтобы сгенерировать список всех страниц на

сайте, а затем направить Nikto на каждую страницу и проверить ее; или в ручном режиме пробовать интересные страниуы.



## 3 Выводы

Мы успешно использовали Nikto, чтобы найти какие-то уязвимости в DVWA, определить их тип и получить ссылки на источники, где есть информация о том, как их можно исправить.