

# **Отчет по индивидуальному проекту.**

## **Этап 4**

*дисциплина: Информационная безопасность*

Морозова Ульяна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>3</b>	<b>Выводы</b>	<b>7</b>

## Список иллюстраций

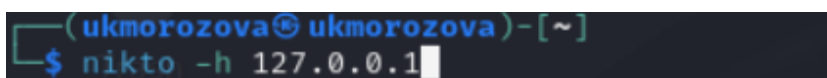
2.1	Запуск nikto . . . . .	5
2.2	Вывод команды nikto . . . . .	5
2.3	Вывод команды nikto 2 . . . . .	6

# 1 Цель работы

Использование nikto для обнаружения уязвимости веб-приложения DVWA.

## 2 Выполнение лабораторной работы

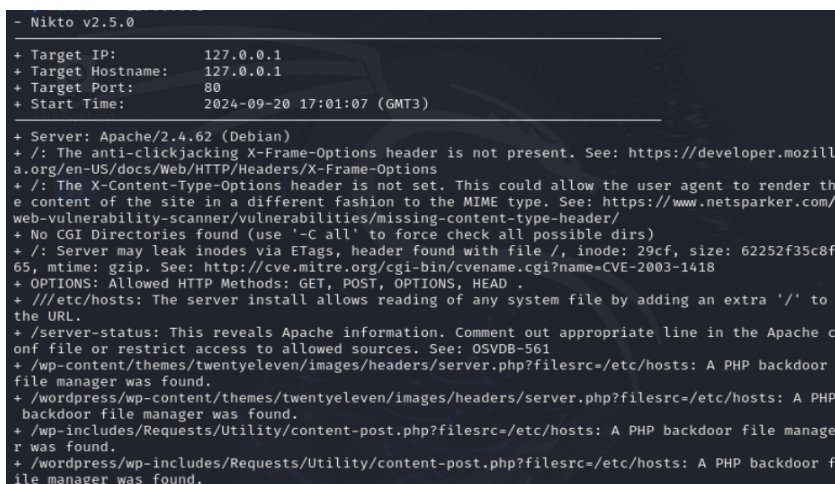
В консоли вводим команду `bash nikto -h 127.0.0.1` где 127.0.0.1 - это IP адрес нашего хоста (рис. 2.1).



```
(ukmorozova@ukmorozova)-[~]  
$ nikto -h 127.0.0.1
```

Рис. 2.1: Запуск nikto

Запуск команды выводит список уязвимостей нашего веб-приложения DVWA (рис. 2.2 - рис. 2.3).



```
- Nikto v2.5.0  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 80  
+ Start Time: 2024-09-20 17:01:07 (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: 62252f35c8f65, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .  
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.  
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache config file or restrict access to allowed sources. See: OSVDB-561  
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
```

Рис. 2.2: Вывод команды nikto

```

+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat=/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-09-20 17:01:18 (GMT3) (11 seconds)

+ 1 host(s) tested

*****
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 submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? █

```

Рис. 2.3: Вывод команды nikto 2

## 3 Выводы

Мы использовали nikto для проверки уязвимостей веб-приложения DVWA.