

Презентация по индивидуальной проекте: Этап 2

Основы информационной безопасности

Нджову Н.

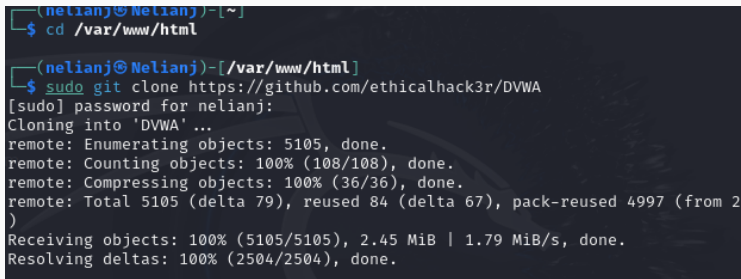
18 марта 2025

Российский университет дружбы народов, Москва, Россия

Приобретение практических навыков по установке DVWA.

1. Установите DVWA на дистрибутив Kali Linux

Поскольку я буду настраивать DVWA на моем локальном хостинге, я открываю терминал и перехожу в каталог `/var/www/html`. Затем я клонирую репозиторий DVWA на github в каталог `/html`, используя команду `git clone`(рис.1).

A screenshot of a terminal window with a dark background. The prompt is `(nelianj@Nelianj)-[~]`. The first command is `$ cd /var/www/html`. The second command is `$ sudo git clone https://github.com/ethicalhack3r/DVWA`. The terminal shows the password prompt `[sudo] password for nelianj:` and the cloning progress: `Cloning into 'DVWA'...`, `remote: Enumerating objects: 5105, done.`, `remote: Counting objects: 100% (108/108), done.`, `remote: Compressing objects: 100% (36/36), done.`, `remote: Total 5105 (delta 79), reused 84 (delta 67), pack-reused 4997 (from 2)`, `Receiving objects: 100% (5105/5105), 2.45 MiB | 1.79 MiB/s, done.`, and `Resolving deltas: 100% (2504/2504), done.`

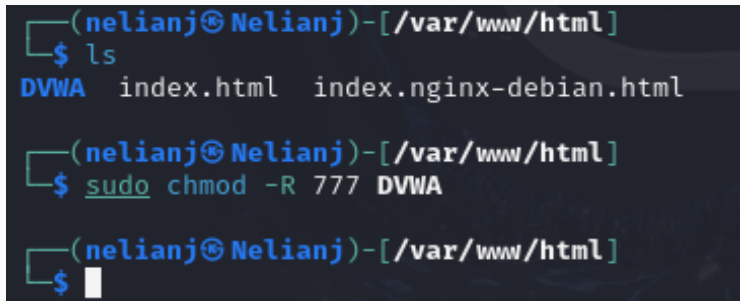
```
(nelianj@Nelianj)-[~]
$ cd /var/www/html

(nelianj@Nelianj)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for nelianj:
Cloning into 'DVWA'...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (108/108), done.
remote: Compressing objects: 100% (36/36), done.
remote: Total 5105 (delta 79), reused 84 (delta 67), pack-reused 4997 (from 2)
Receiving objects: 100% (5105/5105), 2.45 MiB | 1.79 MiB/s, done.
Resolving deltas: 100% (2504/2504), done.
```

Рис. 1: Клонирование репозитория

Выполнение лабораторной работы

После этого, я запускаю команду `ls`, чтобы подтвердить, что DVWA был успешно клонирован. После подтверждения я меняю права доступа к файлу DVWA(рис.2)



```
(nelianj@Nelianj)-[/var/www/html]
$ ls
DVWA  index.html  index.nginx-debian.html

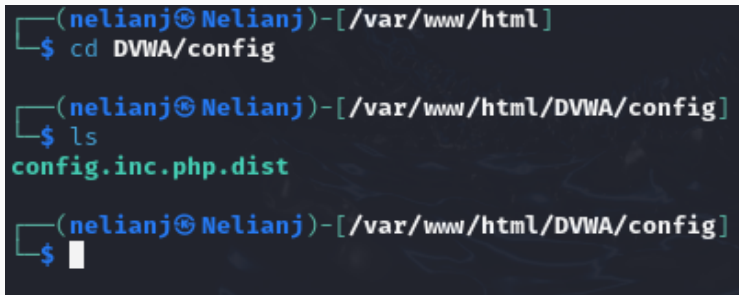
(nelianj@Nelianj)-[/var/www/html]
$ sudo chmod -R 777 DVWA

(nelianj@Nelianj)-[/var/www/html]
$
```

Рис. 2: Изменение прав доступа

Выполнение лабораторной работы

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`, затем проверю содержимое каталога(рис.3)

A terminal window with a dark background and light-colored text. The prompt is `(nelianj@Nelianj)-[/var/www/html]`. The first command is `$ cd DVWA/config`. The second prompt is `(nelianj@Nelianj)-[/var/www/html/DVWA/config]`, and the command `$ ls` is entered, resulting in the output `config.inc.php.dist`. The third prompt is `(nelianj@Nelianj)-[/var/www/html/DVWA/config]`, and the command `$` is entered, followed by a white cursor block.

```
(nelianj@Nelianj)-[/var/www/html]
$ cd DVWA/config

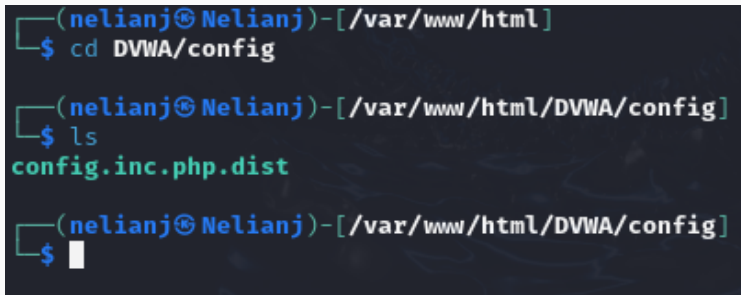
(nelianj@Nelianj)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist

(nelianj@Nelianj)-[/var/www/html/DVWA/config]
$
```

Рис. 3: Перемещение по директориям

Выполнение лабораторной работы

Я делаю копию файла `config.inc.php.dist`, называю его `config.inc.php`. Я использую новый файл для настройки DVWA. Файл `config.inc.php.dist` не изменяем его, чтобы у нас будет запасной вариант, если что-то пойдет не так (рис.4)

A terminal window with a dark background and light blue/green text. The prompt is `(nelianj@Nelianj)-[/var/www/html]`. The first command is `$ cd DVWA/config`. The second prompt is `(nelianj@Nelianj)-[/var/www/html/DVWA/config]`, and the command is `$ ls`. The output is `config.inc.php.dist`. The third prompt is `(nelianj@Nelianj)-[/var/www/html/DVWA/config]` with a cursor on the line.

```
(nelianj@Nelianj)-[ /var/www/html ]
$ cd DVWA/config

(nelianj@Nelianj)-[ /var/www/html/DVWA/config ]
$ ls
config.inc.php.dist

(nelianj@Nelianj)-[ /var/www/html/DVWA/config ]
$
```

Рис. 4: Создание копии файла

Теперь я открываю файл config.inc.php с помощью редактора nano, чтобы выполнить необходимые настройки(рис.5)

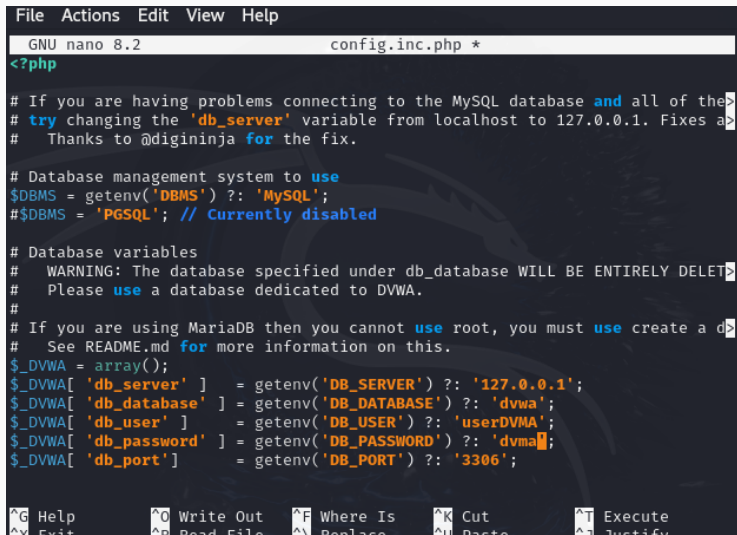
A terminal window with a dark background. The prompt is (nelianj@Nelianj)-[/var/www/html/DVWA/config]. The user enters the command \$ sudo nano config.inc.php. The prompt changes to (nelianj@Nelianj)-[/var/www/html/DVWA/config] and the user's input \$ is followed by a white cursor block.

```
(nelianj@Nelianj)-[/var/www/html/DVWA/config]  
$ sudo nano config.inc.php  
  
(nelianj@Nelianj)-[/var/www/html/DVWA/config]  
$
```

Рис. 5: Открытие файла в редакторе

Выполнение лабораторной работы

Я изменяю данные об имени пользователя и пароле(рис.6)



```
File Actions Edit View Help
GNU nano 8.2 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
# $DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a database
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_database'] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA['db_user'] = getenv('DB_USER') ?: 'userDVMA';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'dvma';
$_DVWA['db_port'] = getenv('DB_PORT') ?: '3306';

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute
^X Exit      ^P Read File  ^\ Replace    ^U Paste      ^_ Justify
```

Выполнение лабораторной работы

По умолчанию Kali Linux поставляется с установленной Система управления реляционными базами данных MariaDB. Поэтому мне не нужно устанавливать никаких пакетов, я просто запускаю службу mysql командой `sudo systemctl start mysql`(рис.7)

```
(nelianj@Nelianj)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql
[sudo] password for nelianj:

(nelianj@Nelianj)-[/var/www/html/DVWA/config]
$ systemctl start mysql

(nelianj@Nelianj)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Thu 2025-03-06 22:42:33 MSK; 1min 33s ago
   Invocation: 8bc6bb7c727648fd9960bcf7493b8cc7
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/
   Process: 15527 ExecStartPre=/usr/bin/install -m 755 -o mysql -u root -d
```

Рис. 7: Запуск mysql

Выполнение лабораторной работы

Я вхожу в базу данных, используя команду `sudo mysql -u root -p`. В этом случае я использую `root`, так как это имя суперпользователя, установленное в моей системе. Затем я создаю нового пользователя, используя учетные данные, которые я установил в файле `config.inc.php`(рис.8)

```
(nelianj@nelianj)-[~]  
$ sudo mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 32  
Server version: 11.4.3-MariaDB-1 Debian n/a  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Support MariaDB developers by giving a star at https://github.com/MariaDB/server  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement  
.  
  
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "dvwa";  
Query OK, 0 rows affected (0.009 sec)
```

Рис. 8: Авторизация в базе данных

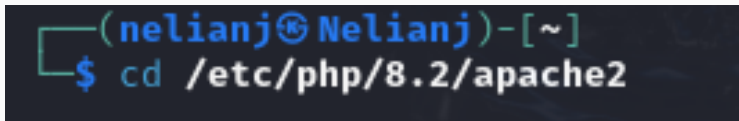
Теперь я предоставляю этому пользователю полные привилегии над базой данных dvwa(рис.9)

A screenshot of a terminal window with a dark background. The text shows a MySQL command being executed: 'grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';'. The response from the database is 'Query OK, 0 rows affected (0.008 sec)'. Then, the user types 'exit' and the terminal displays 'Bye'. At the bottom, the terminal shows the user's shell prompt as '(nelianj@Nelianj)-[~]' with a blue cursor, and a shell prompt '\$' with a white cursor below it.

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';  
Query OK, 0 rows affected (0.008 sec)  
  
MariaDB [(none)]> exit  
Bye  
  
(nelianj@Nelianj)-[~]  
$
```

Рис. 9: Изменение прав

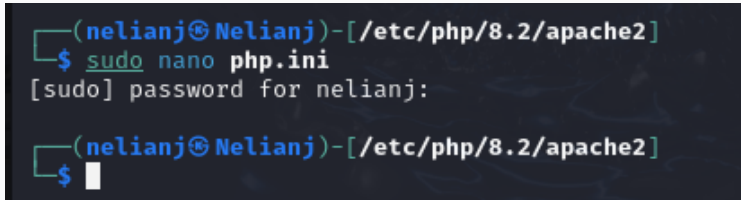
Необходимо настроить сервер apache2, перехожу в соответствующую директорию(рис.10)

A terminal window with a dark background. The prompt is '(nelianj@Nelianj)-[~]' in blue. Below it, the command '\$ cd /etc/php/8.2/apache2' is entered in white text.

```
(nelianj@Nelianj)-[~]  
$ cd /etc/php/8.2/apache2
```

Рис. 10: Перемещение между директориями

В моем текущем каталоге я открываю файл `php.ini` с помощью текстового редактора(`nano`), чтобы редактировать его(рис.11)

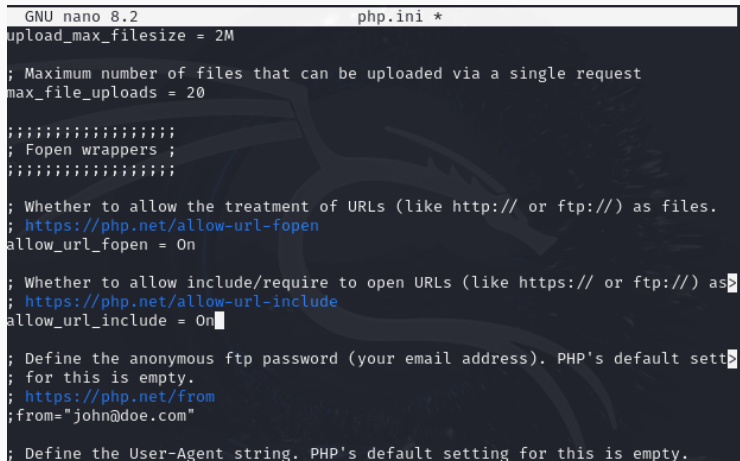
A terminal window with a dark background and light blue/green text. The prompt is `(nelianj@Nelianj)-[/etc/php/8.2/apache2]`. The user enters `$ sudo nano php.ini`. The system responds with `[sudo] password for nelianj:`. The prompt returns to `(nelianj@Nelianj)-[/etc/php/8.2/apache2]`, and the user enters a password, represented by a white rectangle.

```
(nelianj@Nelianj)-[/etc/php/8.2/apache2]
$ sudo nano php.ini
[sudo] password for nelianj:
(nelianj@Nelianj)-[/etc/php/8.2/apache2]
$ 
```

Рис. 11: Открытие файла в текстовом редакторе

Выполнение лабораторной работы

Я прокручиваю страницу вниз, ищу строки `allow_url_fopen` и `allow_url_include` и убеждаюсь, что обе они включены(рис.12)



```
GNU nano 8.2          php.ini *
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default sett
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
```

Выполнение лабораторной работы

Я запускаю службу веб-сервера apache и проверяю, запущена ли служба (рис.13)

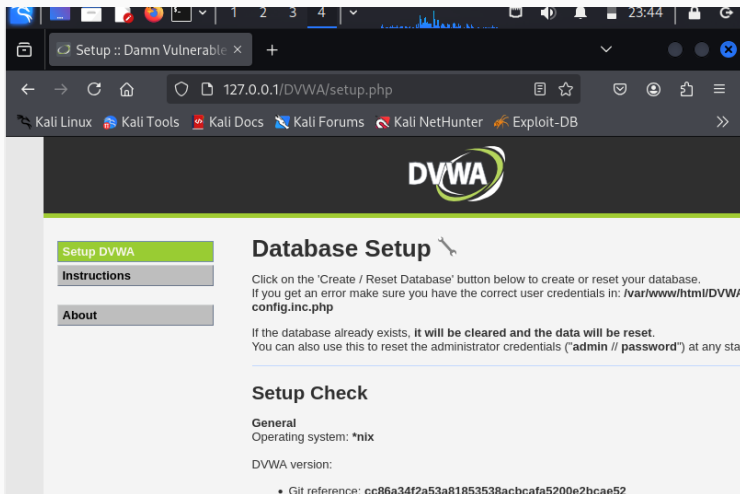
```
(nelianj@Nelianj)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pres>
   Active: active (running) since Thu 2025-03-06 23:28:38 MSK; 52s ago
 Invocation: fece6b54d5cb41ba894493bf8f40a5bc
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 38292 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
  Main PID: 38316 (apache2)
     Tasks: 6 (limit: 2219)
    Memory: 20.2M (peak: 20.5M)
       CPU: 62ms
    CGroup: /system.slice/apache2.service
            └─38316 /usr/sbin/apache2 -k start
              └─38319 /usr/sbin/apache2 -k start
                └─38320 /usr/sbin/apache2 -k start
                  └─38321 /usr/sbin/apache2 -k start
                    └─38322 /usr/sbin/apache2 -k start
                      └─38323 /usr/sbin/apache2 -k start

Mar 06 23:28:38 Nelianj systemd[1]: Starting apache2.service - The Apache HT>
Mar 06 23:28:38 Nelianj systemd[1]: Started apache2.service - The Apache HT>
```

Рис. 13: Запуск apache

Выполнение лабораторной работы

Я настроила DVWA, Apache и базу данных, поэтому открываю браузер и запускаю веб-приложение, введя 127.0.0/DVWA(рис.14)



Я прокручиваю страницу вниз и нажимаю на кнопку create reset database(рис.15)

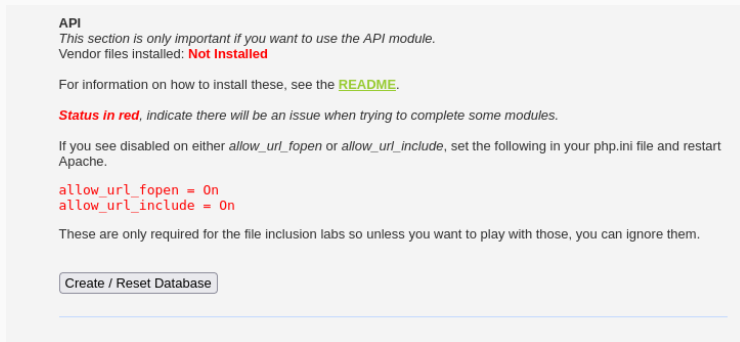
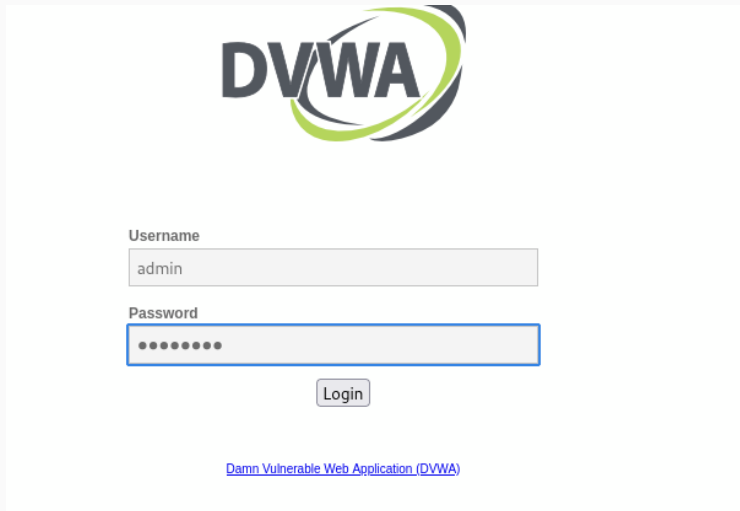


Рис. 15: Создание базы данных

Я авторизуюсь с помощью предложенных по умолчанию данных(рис.16)



The image shows the login interface of the Damn Vulnerable Web Application (DVWA). At the top center is the DVWA logo, which consists of the letters 'DVWA' in a bold, dark grey font, with a stylized green and grey swoosh graphic to the right. Below the logo, there are two input fields. The first is labeled 'Username' and contains the text 'admin'. The second is labeled 'Password' and contains ten black dots, indicating a masked password. Below these fields is a 'Login' button. At the bottom of the page, there is a blue hyperlink that reads 'Damn Vulnerable Web Application (DVWA)'.

Username

admin

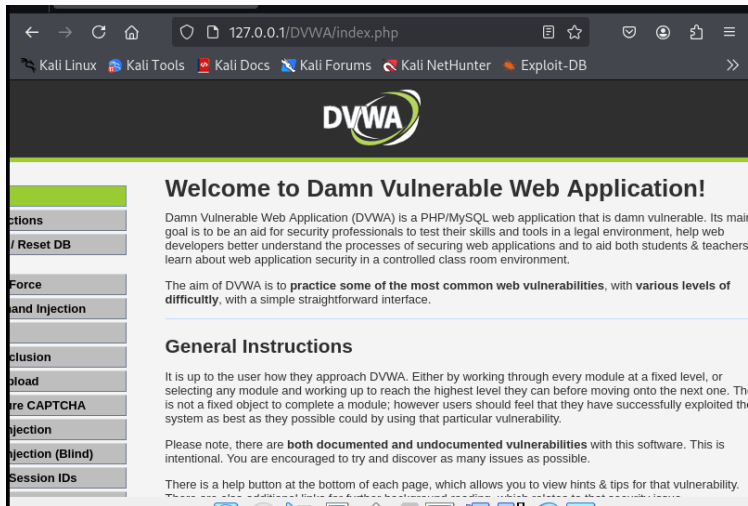
Password

••••••••••

Login

[Damn Vulnerable Web Application \(DVWA\)](#)

Я оказываюсь на домашней странице веб-приложения, на этом установка окончена(рис.17)



Выполнив эту работу, я приобрела практических навыков по установке уязвимого веб-приложения DVWA.