

Презентация по выполнению индивидуального проекта №1

Основы информационной безопасности

Дворкина Е. В

16 марта 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Дворкина Ева Владимировна
- студентка группы НКАбд-01-22
- Российский университет дружбы народов
- <https://vk.com/yuri.kamori>

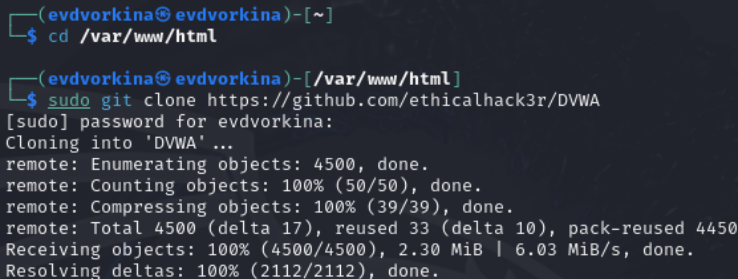


Приобретение практических навыков по установке DVWA.

Выполнение лабораторной работы

1.1

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub

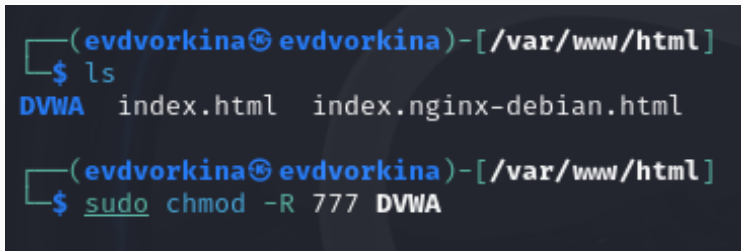
A terminal window with a dark background and light-colored text. The prompt is `(evdvorkina@evdvorkina)-[~]`. The first command is `$ cd /var/www/html`. The second prompt is `(evdvorkina@evdvorkina)-[/var/www/html]`, followed by the command `$ sudo git clone https://github.com/ethicalhack3r/DVWA`. The terminal shows the password prompt, the cloning progress, and the completion status.

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

(evdvorkina@evdvorkina)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for evdvorkina:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.30 MiB | 6.03 MiB/s, done.
Resolving deltas: 100% (2112/2112), done.
```

Рис. 1: Клонирование репозитория

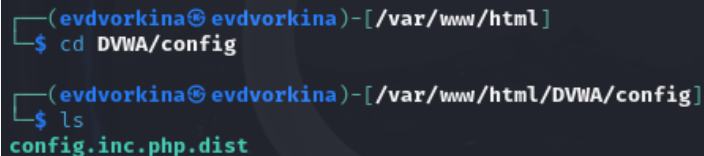
Повышаю права доступа к этой папке до 777

A terminal window with a dark background. The prompt is (evdvorkina@evdvorkina)-[/var/www/html]. The user enters 'ls' and the output is 'DVWA index.html index.nginx-debian.html'. Then the user enters 'sudo chmod -R 777 DVWA'.

```
(evdvorkina@evdvorkina)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html  
  
(evdvorkina@evdvorkina)-[/var/www/html]  
$ sudo chmod -R 777 DVWA
```

Рис. 2: Изменение прав доступа

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`

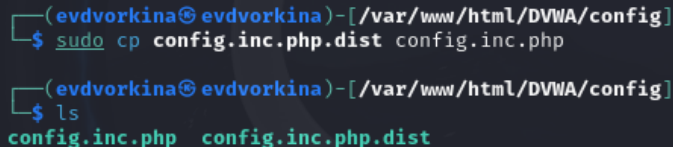
A terminal window with a dark background. The prompt is `(evdvorkina@evdvorkina)-[/var/www/html]`. The first command is `$ cd DVWA/config`. The prompt changes to `(evdvorkina@evdvorkina)-[/var/www/html/DVWA/config]`. The second command is `$ ls`, and the output is `config.inc.php.dist`.

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

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

Рис. 3: Перемещение по директориям

Создаем копию файла, используемого для настройки DVWA config.inc.php.dist с именем config.inc.php.

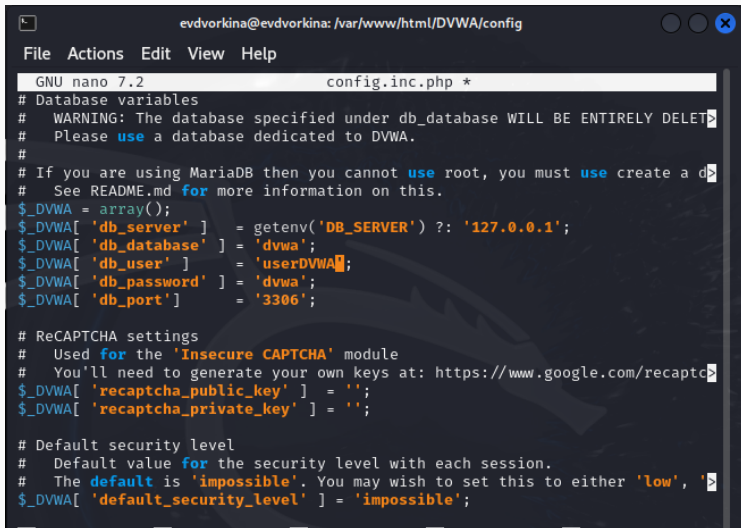
A terminal window with a dark background and light-colored text. The prompt is (evdvorkina@evdvorkina)-[/var/www/html/DVWA/config]. The first command is \$ sudo cp config.inc.php.dist config.inc.php. The second command is \$ ls. The output of the ls command is config.inc.php config.inc.php.dist.

```
(evdvorkina@evdvorkina)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

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

Рис. 4: Создание копии файла

Изменяю данные об имени пользователя и пароле



```
evdvorkina@evdvorkina: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php *
# 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' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'userDVWA';
$_DVWA[ 'db_password' ] = 'dvwa';
$_DVWA[ 'db_port' ] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium' or 'high'
$_DVWA[ 'default_security_level' ] = 'impossible';
```

Запускаю mysql

```
(evdvorkina@evdvorkina)-[~]  
$ sudo systemctl start mysql  
  
(evdvorkina@evdvorkina)-[~]  
$ systemctl status mysql  
● mariadb.service - MariaDB 10.11.6 database server  
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>  
   Active: active (running) since Sat 2024-03-16 00:20:47 MSK; 7s ago
```

Рис. 6: Запуск mysql

Авторизируюсь в базе данных от имени пользователя root. Создаем нового пользователя, используя учетные данные из файла config.inc.php

```
(evdvorkina@evdvorkina)-[~]  
$ sudo mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 10.11.6-MariaDB-2 Debian n/a  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
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 (0.010 sec)
```

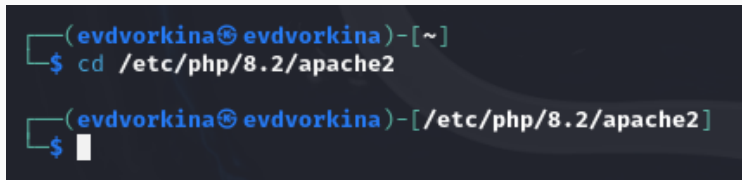
Рис. 7: Авторизация в базе данных

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';  
Query OK, 0 rows affected (0.006 sec)  
  
MariaDB [(none)]> exit  
Bye
```

Рис. 8: Изменение прав

Необходимо настроить сервер apache2, перехожу в соответствующую директорию

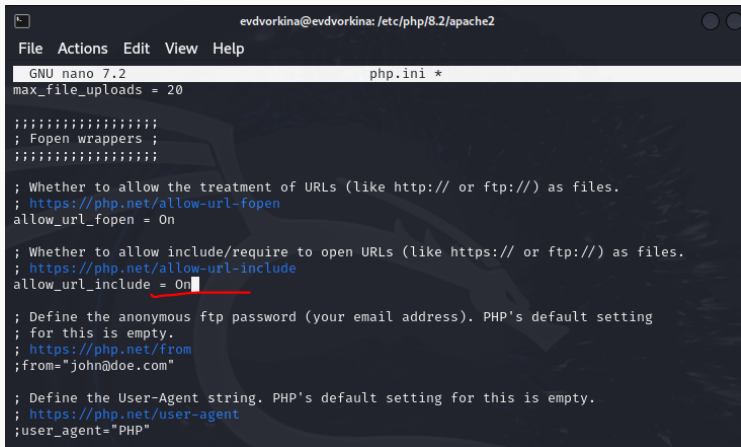
A terminal window with a dark background and light blue text. The prompt is '(evdvorkina@evdvorkina)-[~]'. The first command is '\$ cd /etc/php/8.2/apache2'. The second prompt is '(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]' followed by a '\$' and a cursor.

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

Рис. 9: Перемещение между директориями

3.2

В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `On`



```
evdvorkina@evdvorkina: /etc/php/8.2/apache2
File Actions Edit View Help
GNU nano 7.2 php.ini *
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 files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; 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.
; https://php.net/user-agent
user_agent="PHP"
```

Запускаем службу веб-сервера apache и проверяем, запущена ли служба

```
(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(evdvorkina@evdvorkina)-[/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; preset: disabled)
   Active: active (running) since Sat 2024-03-16 00:31:47 MSK; 11s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 11911 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 11927 (apache2)
    Tasks: 6 (limit: 4611)
   Memory: 23.8M (peak: 24.1M)
      CPU: 101ms
   CGroup: /system.slice/apache2.service
           └─11927 /usr/sbin/apache2 -k start
             └─11930 /usr/sbin/apache2 -k start
               └─11931 /usr/sbin/apache2 -k start
                 └─11932 /usr/sbin/apache2 -k start
                   └─11933 /usr/sbin/apache2 -k start
                     └─11934 /usr/sbin/apache2 -k start

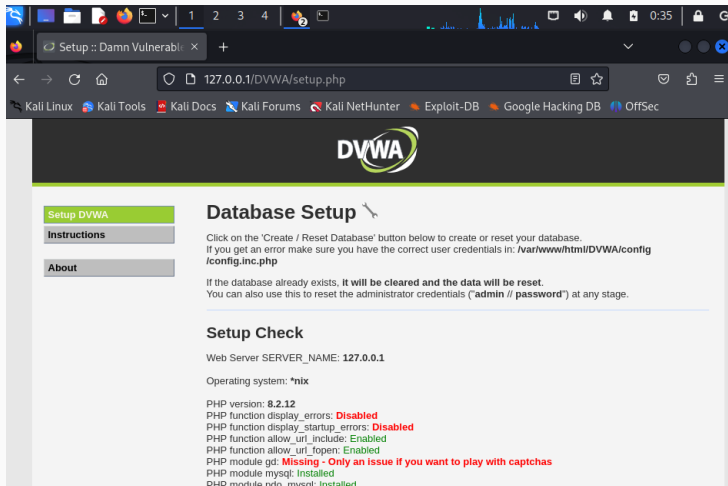
Mar 16 00:31:47 evdvorkina systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 16 00:31:47 evdvorkina systemd[1]: Started apache2.service - The Apache HTTP Server.

(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$
```

Рис. 11: Запуск apache

4.1

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA



Прокручиваем страницу вниз и нажимаем на кнопку create\reset database

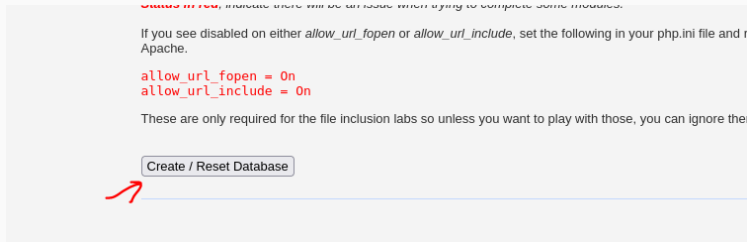


Рис. 13: “Создание базы данных”

Авторизуюсь с помощью предложенных по умолчанию данных



Username

admin

Password

••••••••|

Login

Оказываюсь на домашней странице веб-приложения, на этом установка окончена

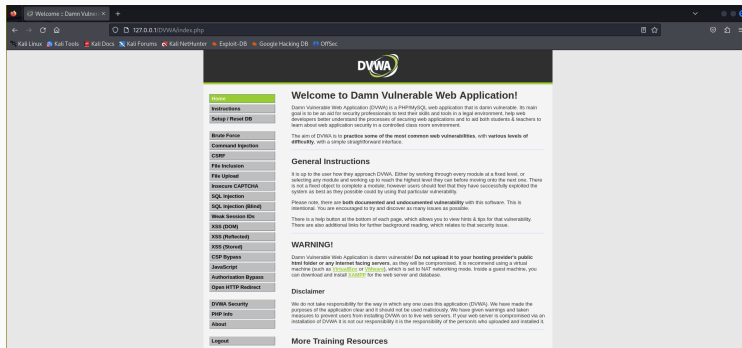


Рис. 15: Домашняя страница DVWA

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

Спасибо за внимание

