

Отчёт по 2-ому этапу индивидуального проекта

Основы информационной безопасности

Бережной Иван Александрович

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
3.1	Основные особенности:	6
3.2	Как использовать:	6
3.3	Примеры уязвимостей:	7
4	Выполнение лабораторной работы	8
5	Выводы	12

Список иллюстраций

4.1	Клонирование репозитория	8
4.2	Изменения прав доступа	8
4.3	Копировани конфига	8
4.4	Редактирование конфига	9
4.5	Запуск mysql	9
4.6	Вход в бд	9
4.7	Создание пользователя бд	9
4.8	Привилегии пользователя	10
4.9	Переход к apache	10
4.10	Изменение php.ini	10
4.11	Запуск apache	10
4.12	Открытие DVWA	11
4.13	Вход	11

1 Цель работы

Попрактиковать навыки установки ПО на дистрибутив Linux - Kali.

2 Задание

Установить DVWA на ОС.

3 Теоретическое введение

DVWA (Damn Vulnerable Web Application) — это веб-приложение, специально созданное для тестирования на уязвимости и обучения основам веб-безопасности. Оно содержит множество уязвимостей, таких как SQL-инъекции, XSS, CSRF, файловые включения и другие, что позволяет безопасно практиковаться в их эксплуатации и устранении.

3.1 Основные особенности:

- **Цель:** Обучение и тестирование навыков пентеста.
- **Уязвимости:** Включает широкий спектр уязвимостей для изучения.
- **Уровни сложности:** Низкий, средний, высокий и невозможный (для разных уровней подготовки).
- **Простота установки:** Работает на локальном сервере (например, XAMPP, Docker).

3.2 Как использовать:

1. Установите DVWA на локальный сервер или используйте готовый образ Docker.
2. Войдите в систему (по умолчанию логин: admin, пароль: password).
3. Выберите уровень сложности и начинайте тестирование.

3.3 Примеры уязвимостей:

- **SQL Injection:** Внедрение SQL-кода для получения доступа к базе данных.
- **XSS (Cross-Site Scripting):** Внедрение вредоносных скриптов в веб-страницы.
- **CSRF (Cross-Site Request Forgery):** Подделка запросов от имени пользователя.

4 Выполнение лабораторной работы

Перейдём в каталог html и клонируем репозиторий git (рис. 4.1).

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

(iaberezhnoyj@iaberezhnoyj)-[/var/www/html]
$
sudo git clone https://github.com/digininja/DVWA.git
[sudo] пароль для iaberezhnoyj:
Клонирование в «DVWA» ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)
Получение объектов: 100% (5105/5105), 2.49 МиБ | 3.02 МиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.
```

Рис. 4.1: Клонирование репозитория

Изменим права доступа к папке установки и перейдём к файлу конфигурации (рис. 4.2).

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

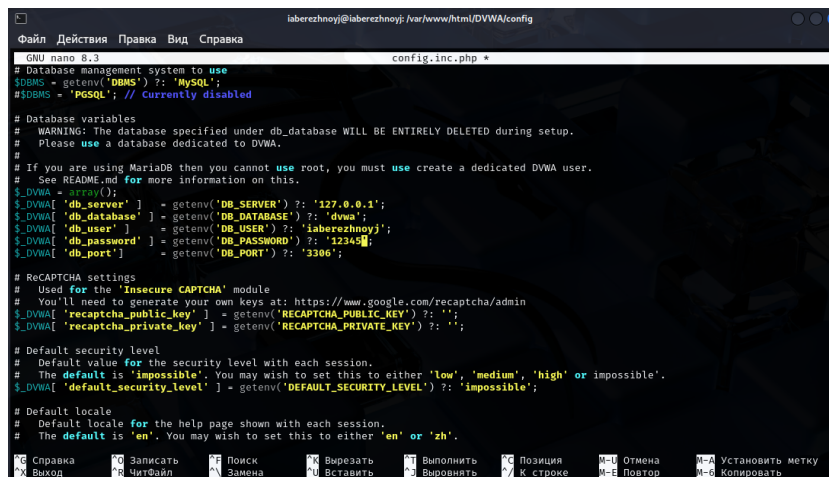
(iaberezhnoyj@iaberezhnoyj)-[/var/www/html]
$ cd DVWA/config
```

Рис. 4.2: Изменения прав доступа

Скопируем файл конфига и переименуем его (рис. 4.3). Откроем файл конфигурации и изменим имя пользователя и пароль (рис. 4.4).

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

Рис. 4.3: Копирование конфига



```
GNU nano 8.3 config.inc.php
# Database management system to use
$DBMS = getenv('DBMS') ? 'MySQL';
# $DBMS = 'MySQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$DVWA[ 'db_server' ] = getenv('DB_SERVER') ? '127.0.0.1';
$DVWA[ 'db_database' ] = getenv('DB_DATABASE') ? 'dvwa';
$DVWA[ 'db_user' ] = getenv('DB_USER') ? 'iaberezhnoyj';
$DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ? '12345';
$DVWA[ 'db_port' ] = getenv('DB_PORT') ? '3306';

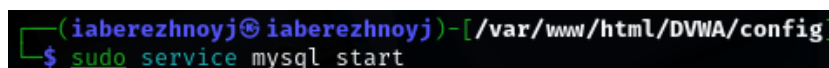
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$DVWA[ 'recaptcha_public_key' ] = getenv('RECAPTCHA_PUBLIC_KEY') ? '':
$DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ? '':

# 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', 'high' or 'impossible'.
$DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ? 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
```

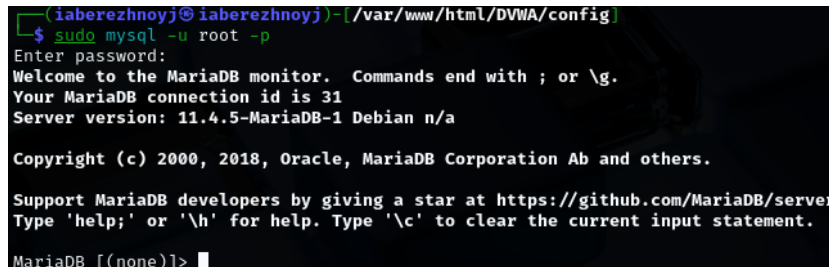
Рис. 4.4: Редактирование конфига

Поскольку mysql уже установлен, запустим его (рис. 4.5) и войдём в базу данных (рис. 4.6).



```
(iaberezhnoyj@iaberezhnoyj)-[/var/www/html/DVWA/config]
$ sudo service mysql start
```

Рис. 4.5: Запуск mysql



```
(iaberezhnoyj@iaberezhnoyj)-[/var/www/html/DVWA/config]
$ 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: 11.4.5-MariaDB-1 Debian n/a

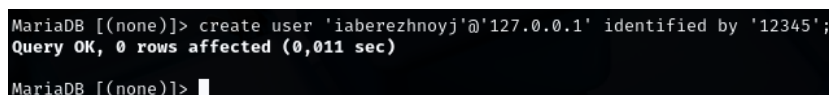
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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)]>
```

Рис. 4.6: Вход в бд

Создадим пользователя базы данных, указав имя и пароль такие же, как в файле конфигурации (рис. 4.7), а также предоставим этому пользователю все привилегии (рис. 4.8).



```
MariaDB [(none)]> create user 'iaberezhnoyj'@'127.0.0.1' identified by '12345';
Query OK, 0 rows affected (0,011 sec)

MariaDB [(none)]>
```

Рис. 4.7: Создание пользователя бд

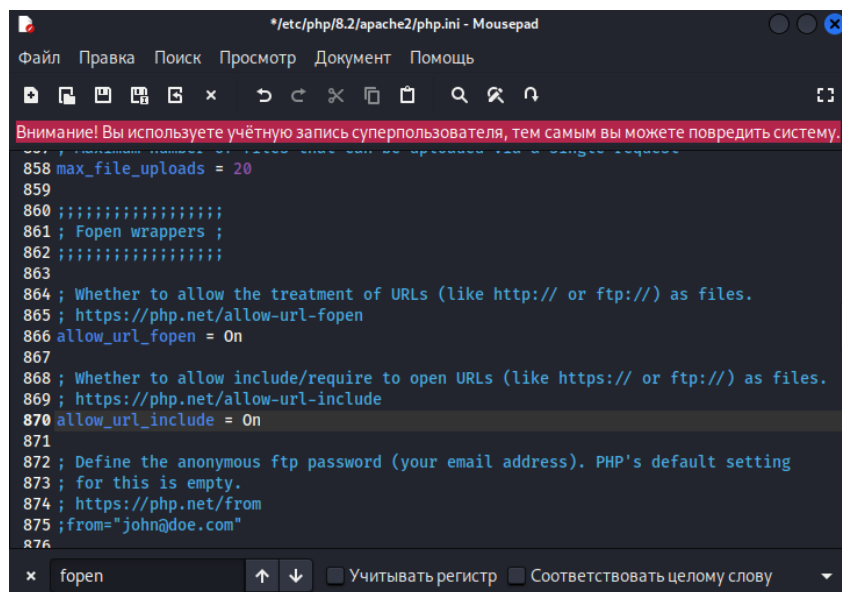
```
MariaDB [(none)]> grant all privileges on dvwa.* to 'iaberezhnoyj'@'127.0.0.1' identified by '12345';
Query OK, 0 rows affected (0,010 sec)
```

Рис. 4.8: Привилегии пользователя

Перейдём в каталог apache (рис. 4.9) и откроем файл php.ini, чтобы включить параметр allow_url_include (рис. 4.10).

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

Рис. 4.9: Переход к apache



```
*etc/php/8.2/apache2/php.ini - Mousepad
Файл  Правка  Поиск  Просмотр  Документ  Помощь
Внимание! Вы используете учётную запись суперпользователя, тем самым вы можете повредить систему.
858 max_file_uploads = 20
859
860 ;;;;;;;;;;;;;;;;;
861 ; Fopen wrappers ;
862 ;;;;;;;;;;;;;;;;;
863
864 ; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
865 ; https://php.net/allow-url-fopen
866 allow_url_fopen = On
867
868 ; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
869 ; https://php.net/allow-url-include
870 allow_url_include = On
871
872 ; Define the anonymous ftp password (your email address). PHP's default setting
873 ; for this is empty.
874 ; https://php.net/from
875 ;from="john@doe.com"
876
x  fopen  ↑ ↓  ☐ Учитывать регистр  ☐ Соответствовать целому слову
```

Рис. 4.10: Изменение php.ini

Запустим apache (рис. 4.11).

```
(iaberezhnoyj@iaberezhnoyj)-[/etc/php/8.2/apache2]
$ sudo service apache2 start
```

Рис. 4.11: Запуск apache

Теперь можем перейти в браузер и открыть DVWA по адресу 127.0.0.1/DVWA/setup.php (рис. 4.12)

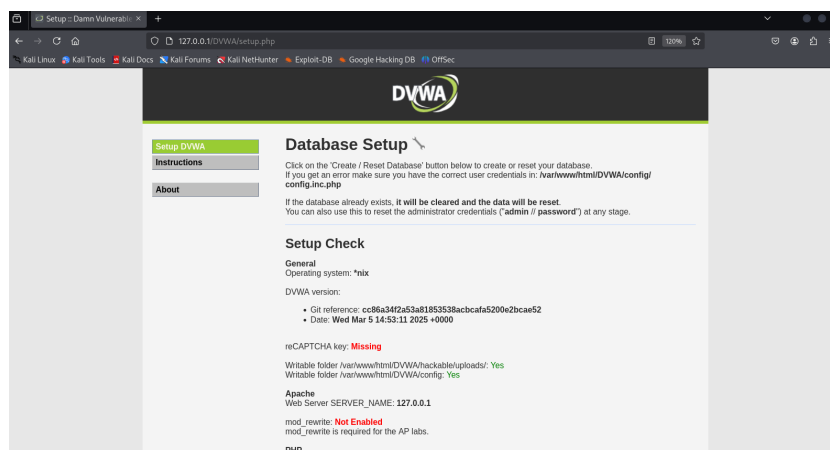


Рис. 4.12: Открытие DVWA

Внизу нажмём Create Database, введём “admin” и “password” в соответствующих строках. Увидим следующую страницу (рис. 4.13)

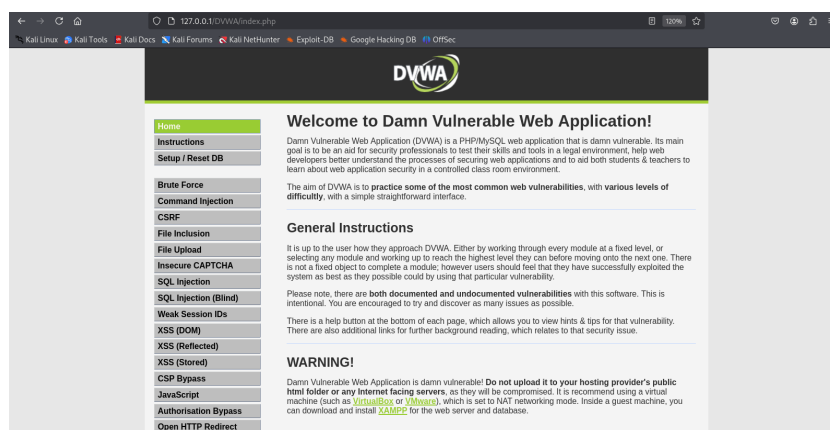


Рис. 4.13: Вход

5 Выводы

В ходе выполнения этапа проекта мы потренировались устанавливать ПО на виртуальную машину, а конкретно на дистрибутив Linux - Kali.