

Отчет по второму этапу индивидуального проекта

Дисциплина: Основы информационной безопасности

Иванов Сергей Владимирович, НПИбд-01-23

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Выводы	12

Список иллюстраций

3.1	Клонирование репозитория	6
3.2	Повышение прав доступа	6
3.3	Переход по каталогу и проверка	7
3.4	Открытие файла в редакторе	7
3.5	Редактирование файла	7
3.6	Запуск mysql	8
3.7	Авторизация в базе данных	8
3.8	Предоставление привелегий	8
3.9	Перемещение по директориям	9
3.10	Редактирование файла	9
3.11	Запуск и проверка статуса	9
3.12	Запуск веб-приложения	10
3.13	Создание базы	10
3.14	Авторизация	11
3.15	Завершение установки	11

1 Цель работы

Установить и настроить DVWA на Kali Linux.

2 Задание

1. Установить DVWA в гостевую систему к Kali Linux.

3 Выполнение лабораторной работы

Переходим в директорию `var/www/html`. Затем клонируем нужный репозиторий GitHub. (рис. 1).

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

(svivanov@svivanov)-[/var/www/html]
$ git clone https://github.com/digininja/DVWA.git
fatal: не удалось создать рабочий каталог «DVWA»: Отказано в доступе

(svivanov@svivanov)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] пароль для svivanov:
Клонирование в «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)
Получение объектов: 100% (5105/5105), 2.49 МБ | 3.95 МБ/с, готово.
Определение изменений: 100% (2489/2489), готово.

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

Рис. 3.1: Клонирование репозитория

Проверяю директорию и повышаю права доступа до 777. (рис. 2)

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

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

Рис. 3.2: Повышение прав доступа

Перехожу в каталог `DVWA/config` и проверяю содержимое. (рис. 3)

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

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

Рис. 3.3: Переход по каталогу и проверка

Далее открываю файл конфигурации в текстовом редакторе. (рис. 4)

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

(svivanov@svivanov)-[/var/www/html/DVWA/config]
$ █
```

Рис. 3.4: Открытие файла в редакторе

Редактирую данные о логине и пароле. (рис. 5)

```
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated
# 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') ? 'svivanovDVWA';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ? 'palann78';
$_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.
```

Рис. 3.5: Редактирование файла

Запускаю службу mysql и проверяю статус. (рис. 6)

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

(svivanov@svivanov)-[/var/www/html/DVWA/config]
$ status mysql
Команда «status» не найдена. Возможно, вы имели в виду:
  command 'statfs' from deb gocryptfs
  command 'states' from deb enscript
Try: sudo apt install <deb name>

(svivanov@svivanov)-[/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; preset: disab>
   Active: active (running) since Thu 2025-03-06 14:17:43 MSK; 34s ago
```

Рис. 3.6: Запуск mysql

Авторизуюсь в бвзе данных от имени пользователя root. Создаем в ней нового пользователя. (рис. 7)

```
(svivanov@svivanov)-[/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: 11.4.3-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 'dwva'
→
→ ;
Query OK, 0 rows affected (0,003 sec)
```

Рис. 3.7: Авторизация в базе данных

Предоставляю пользователю привелегии для работы с этой базой данных. (рис. 8)

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified
by 'dwva';
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> exit
```

Рис. 3.8: Предоставление привелегий

Необходимо настроить сервер apache2. Перехожу в нужную директорию и открываю файл. (рис. 9)


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

(svivanov@svivanov)-[/etc/php/8.2/apache2]
$ sudo nano php.ini
```

Рис. 3.9: Перемещение по директориям

Редактирую 2 параметра. (рис. 10)

```
; 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.

^G Справка      ^O Записать    ^F Поиск       ^K Вырезать    ^T Выполнить   ^C Позиция
^X Выход        ^R ЧитФайл    ^\ Замена     ^U Вставить    ^J Выводить    ^_ К строке
```

Рис. 3.10: Редактирование файла

Запускаю веб-сервер apache2 и проверяю его статус. (рис. 11)

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

(svivanov@svivanov)-[/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: disab>
   Active: active (running) since Thu 2025-03-06 14:27:33 MSK; 26s ago
   Invocation: 598be9bc6a88426aba94f54640840cdc
```

Рис. 3.11: Запуск и проверка статуса

Открываю браузер и запускаю веб-приложение, введя 127.0.0.1/DVWA . (рис. 12)

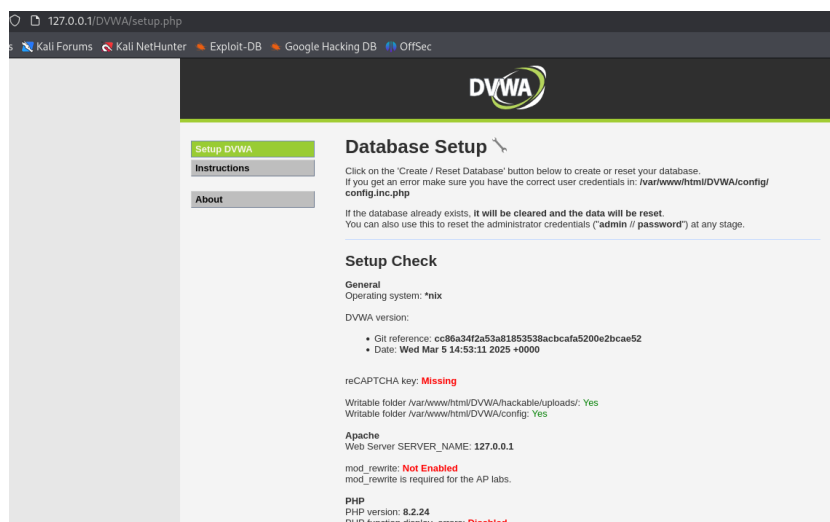


Рис. 3.12: Запуск веб-приложения

Прокручиваю страницу вниз и нажимаю кнопку create/reset database. (рис. 13)

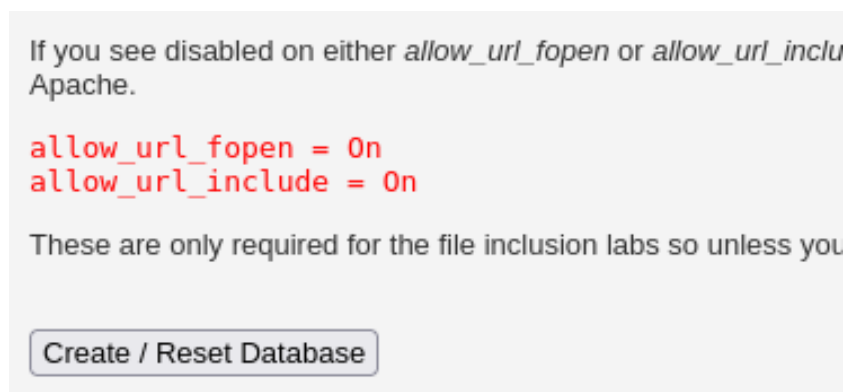



Рис. 3.13: Создание базы

Авторизуюсь с помощью предложенных данных по умолчанию. (рис. 14)




Username

Password

Login

Рис. 3.14: Авторизация

Мы оказались на домашней странице веб-приложения. Установка завершена.
(рис. 15)



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities, with various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)

Рис. 3.15: Завершение установки

4 Выводы

Приобретены навыки по установке веб-приложения DVWA на гостевую систему Kali Linux.