

Второй этап индивидуального проекта

Установка DVWA

Беличева Дарья Михайловна

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
3.1	Установка DVWA	7
3.2	Настройка DVWA	7
3.3	Настройка базы данных	9
3.4	Настройка сервера Apache	10
3.5	Открытие DVWA в веб-браузере	11
4	Выводы	14
	Список литературы	15

Список иллюстраций

3.1	Скачивание DVWA: клонирование репозитория	7
3.2	Каталог конфигурации	8
3.3	Редактирование файла конфигурации	9
3.4	Запуск службы mysql	9
3.5	Вход в базу данных, создание пользователя	10
3.6	Переход в нужную директорию	10
3.7	Редактирование файла php.ini	11
3.8	Запуск службы веб-сервера apache	11
3.9	Запуск приложения DVWA в веб-браузере	12
3.10	Создание базы данных	12
3.11	Вход в систему DVWA	13
3.12	Домашняя страница DVWA	13

1 Цель работы

Установить и настроить DVWA в гостевую систему к Kali Linux.

2 Теоретическое введение

Damn Vulnerable Web Application (DVWA) — это веб-приложение на PHP/MySQL, которое чертовски уязвимо. Его главная цель — помочь профессионалам по безопасности протестировать их навыки и инструменты в легальном окружении, помочь веб-разработчикам лучше понять процесс безопасности веб-приложений и помочь студентам и учителям в изучении безопасности веб-приложений в контролируемом окружении аудитории [1].

Цель DVWA попрактиковаться в некоторых самых распространённых веб-уязвимостях, с различными уровнями сложности, с простым прямолинейным интерфейсом. Обратите внимание, что имеются как задокументированные, так и незадокументированные уязвимости в этом программном обеспечении. Это сделано специально. Вам предлагается попробовать и обнаружить так много уязвимостей, как сможете.

Некоторые из уязвимостей веб-приложений, который содержит DVWA:

- Брут-форс: Брут-форс HTTP формы страницы входа; используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.
- Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.
- Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.

- Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб-приложение.
- SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение.
- Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб-сервер.
- Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб-приложение/базу данных. DVWA включает отражённую и хранимую XSS.
- Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

3 Выполнение лабораторной работы

3.1 Установка DVWA

Поскольку мы будем настраивать DVWA на нашем локальном хостинге, запустим терминал и перейдем в `/var/www/html` каталог. Это место, где хранятся файлы `localhost`. Далее мы клонируем репозиторий DVWA с GitHub в директорию `/html` (рис. 3.1).



```
(dmbelicheva@dmbelicheva)~  
$ cd /var/www/html  
  
(dmbelicheva@dmbelicheva)-[/var/www/html]  
$ sudo git clone https://github.com/ethicalhack3r/DVWA  
[sudo] password for dmbelicheva:  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 4784, done.  
remote: Counting objects: 100% (334/334), done.  
remote: Compressing objects: 100% (187/187), done.  
remote: Total 4784 (delta 185), reused 266 (delta 139), pack-reused 4450 (from 1)  
Receiving objects: 100% (4784/4784), 2.36 MiB | 600.00 KiB/s, done.  
Resolving deltas: 100% (2296/2296), done.  
  
(dmbelicheva@dmbelicheva)-[/var/www/html]  
$
```

Рис. 3.1: Скачивание DVWA: клонирование репозитория

3.2 Настройка DVWA

После успешного клонирования репозитория запустим команду `ls`, чтобы подтвердить, что DVWA был успешно клонирован. Теперь нам нужно назначить этой папке разрешения на чтение, запись и выполнение (777). Чтобы настроить DVWA, нам нужно будет перейти в каталог `/dvwa/config`. Запустим команду `ls`, чтобы просмотреть содержимое каталога конфигурации. Увидим

файл с именем `config.inc.php.dist`. Этот файл содержит конфигурации DVWA по умолчанию. Создадим копию этого файла с именем `config.inc.php`, который мы будем использовать для настройки DVWA (рис. 3.2).



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

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

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

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

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

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

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

Рис. 3.2: Каталог конфигурации

Теперь откроем `config.inc.php` файл с помощью `nano` редактора, чтобы произвести необходимые настройки. Прокрутим вниз до того места, где находятся такие параметры, как `db_database`, `db_user`, `db_password` и т.д. Отредактируем эти значения (рис. 3.3).


```
File Actions Edit View Help
GNU nano 8.1 config.inc.php *
<?php
# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$dbms = 'MySQL';
# $dbms = 'PGSQL'; // 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 = array();
$DVWA['db_server'] = getenv('DB_SERVER') ? '127.0.0.1';
$DVWA['db_database'] = 'dvwa';
$DVWA['db_user'] = 'dmbelicheva';
$DVWA['db_password'] = 'qwerty';
$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/admin
$DVWA['recaptcha_public_key'] = '';
$DVWA['recaptcha_private_key'] = '';
```

Рис. 3.3: Редактирование файла конфигурации

3.3 Настройка базы данных

По умолчанию Kali Linux поставляется с системой управления реляционными базами данных MariaDB. Следовательно, не нужно устанавливать никаких пакетов. Сначала запустим службу mysql.

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

(dmbelicheva@dmbelicheva)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 00:16:42 MSK; 14s ago
   Invocation: 85e22b14f2c547c490a39fa2d5e38e02
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 13997 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql
   Process: 14007 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITI
   Process: 14009 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || V
   Process: 14100 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITI
   Process: 14102 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 14069 (mariabdb)
   Status: "Taking your SQL requests now ..."
   Tasks: 15 (limit: 30404)
   Memory: 24.1M (max: 24.1M)
```

Рис. 3.4: Запуск службы mysql

Войдем в базу данных. Создадим нового пользователя, используя учетные данные, которые мы установили в config.inc.php файле в каталоге DVWA.

```
(dmbelicheva@dmbelicheva)-[/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: 11.4.2-MariaDB-4 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)]> creat user 'dmbelicheva'@'127.0.0.1' identified by 'qwerty'
→ create user 'dmbelicheva'@'127.0.0.1' identified by 'qwerty';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right
se near 'creat user 'dmbelicheva'@'127.0.0.1' identified by 'qwerty'

create user 'dmb...' at line 1
MariaDB [(none)]> create user 'dmbelicheva'@'127.0.0.1' identified by 'qwerty';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'dmbelicheva'@'127.0.0.1' identified by 'qwerty';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]>
```

Рис. 3.5: Вход в базу данных, создание пользователя

3.4 Настройка сервера Apache

Веб-сервер Apache по умолчанию установлен в Kali Linux. Следовательно, нам не нужно устанавливать никаких дополнительных пакетов.

Чтобы приступить к настройке Apache2, запустим терминал и перейдем в /etc/php/7.4/apache2 каталог. При выполнении команды ls увидим файл с именем php.ini.

```
(dmbelicheva@dmbelicheva)-[/var/www/html/DVWA/config]
$ cd /etc/php/7.4/apache2
cd: no such file or directory: /etc/php/7.4/apache2

(dmbelicheva@dmbelicheva)-[/var/www/html/DVWA/config]
$ ls /etc/php
8.2

(dmbelicheva@dmbelicheva)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2

(dmbelicheva@dmbelicheva)-[/etc/php/8.2/apache2]
$ ls
conf.d  php.ini

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

Рис. 3.6: Переход в нужную директорию

Откроем файл на редактирование. Прокрутим и найдем строки allow_url_fopen и allow_url_include, убедитесь, что для обеих установлено значение On.

```

; 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

```

Рис. 3.7: Редактирование файла php.ini

Перейдем к запуску службы веб-сервера apache. Можно проверить, запущена ли служба, выполнив команду status.

```

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

(dmbelicheva@dmbelicheva)-[/etc/php/8.2/apache2]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 00:47:17 MSK; 9s ago
 Invocation: 8192ce95b4214c8fb8c43afcc3902089
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 29116 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 29140 (apache2)
    Tasks: 6 (limit: 4606)
   Memory: 19.7M (peak: 20M)
      CPU: 161ms
   CGroup: /system.slice/apache2.service
           └─29140 /usr/sbin/apache2 -k start
             └─29143 /usr/sbin/apache2 -k start
               └─29144 /usr/sbin/apache2 -k start
                 └─29145 /usr/sbin/apache2 -k start
                   └─29146 /usr/sbin/apache2 -k start
                     └─29147 /usr/sbin/apache2 -k start

Sep 21 00:47:17 dmbelicheva systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Sep 21 00:47:17 dmbelicheva apachectl[29139]: AH00558: apache2: Could not reliably determine t
Sep 21 00:47:17 dmbelicheva systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)

```

Рис. 3.8: Запуск службы веб-сервера apache

3.5 Открытие DVWA в веб-браузере

На данный момент мы настроили DVWA, базу данных и веб-сервер Apache.

Теперь мы можем приступить к запуску приложения DVWA. Запустим свой веб-браузер и введем URL-адрес.

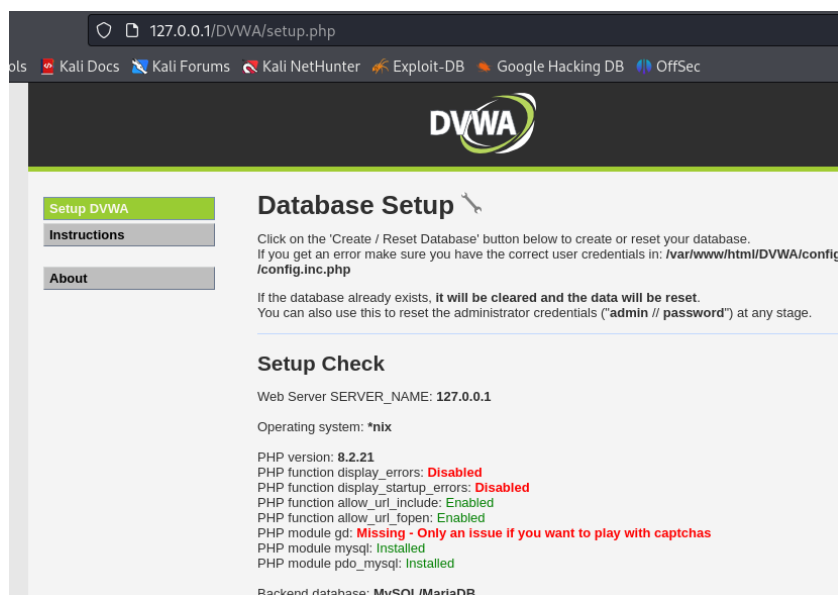


Рис. 3.9: Запуск приложения DVWA в веб-браузере

Нажмем кнопку Создать / Сбросить базу данных в конце страницы. Это создаст и настроит базу данных DVWA. Через несколько секунд мы будем перенаправлены на страницу входа в DVWA.

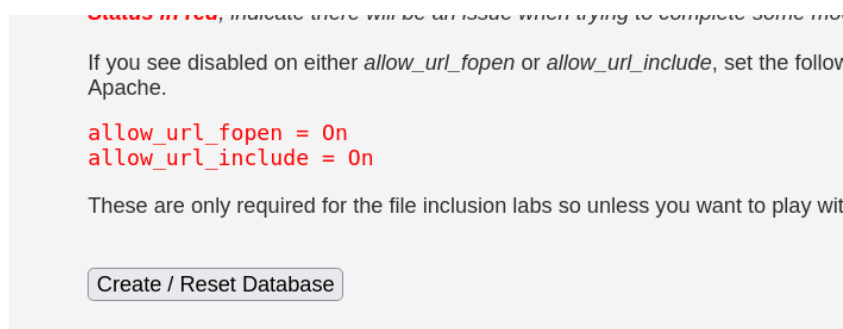


Рис. 3.10: Создание базы данных

Используем приведенные ниже учетные данные по умолчанию для входа в систему.

Имя пользователя: admin

Пароль: пароль

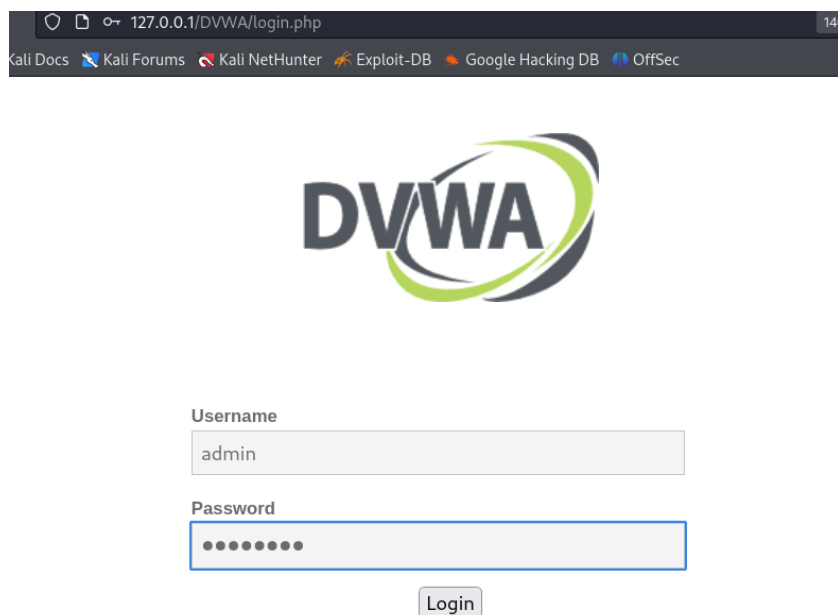


Рис. 3.11: Вход в систему DVWA

После успешного входа в систему увидим домашнюю страницу DVWA. В левой части увидим все доступные уязвимые страницы, которые можно использовать для практики.

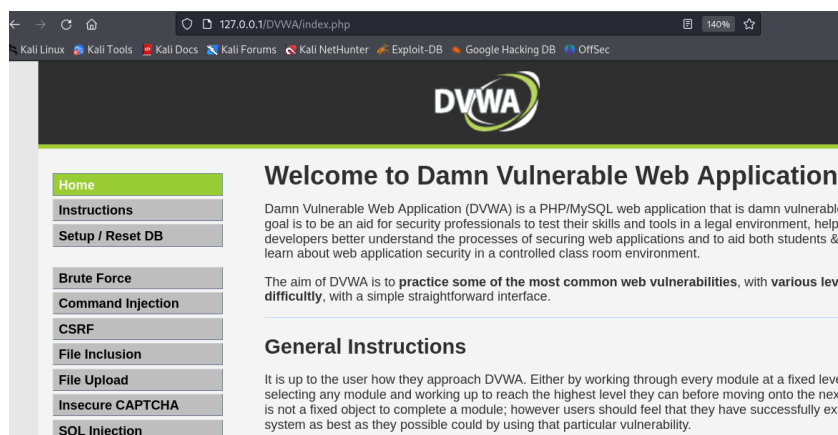


Рис. 3.12: Домашняя страница DVWA

4 Выводы

В результате выполнения данного этапа проекта я установила и настроила DVWA в гостевую систему к Kali Linux.

Список литературы

1. Damn Vulnerable Web Application (DVWA) [Электронный ресурс]. 2024. URL: <https://kali.tools/?p=1820>.