

Основы информационной безопасности

Индивидуальный проект. Этап № 2. Установка DVWA

Демидова Екатерина Алексеевна

Содержание

1	Постановка задачи	4
2	Теоретические сведения	5
3	Выполнение лабораторной работы	7
4	Выводы	13
	Список литературы	14

Список иллюстраций

3.1	Клонирование репозитория с DVWA	7
3.2	Запуск apache2	7
3.3	Проверка работы веб-сервера	8
3.4	Просмтр файла конфигураций	9
3.5	Просмотр стартового окна DVWA	10
3.6	Создание пользователя mariadb и базы данных	10
3.7	Проверка пользователя mariadb	11
3.8	Аутентификация	11
3.9	Запуск DVWA	12

1 Постановка задачи

Целью данной работы является установка DVWA на Kali Linux.

2 Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~ 1]. Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. обстановка помещения.

Цель DVWA – отработать некоторые из наиболее распространенных веб-уязвимостей различного уровня сложности с помощью простого и понятного интерфейса. В этом программном обеспечении существуют как задокументированные, так и недокументированные уязвимости.

Некоторые из уязвимостей веб приложений, который содержит DVWA:

- Брутфорс: Брутфорс 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 внедре-

ние.

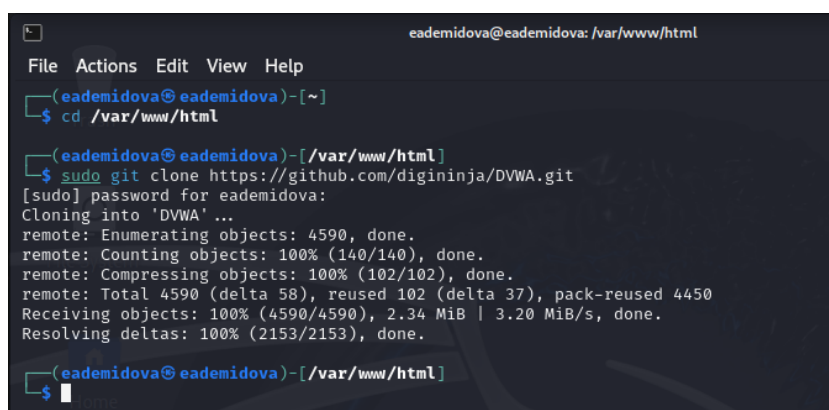
- Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер.
- Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS.
- Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

- Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.
- Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу.
- Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

3 Выполнение лабораторной работы

Скопируем в каталог /etc/www/html файлы веб-приложения DVWA с гита(рис. 3.1)



```
eademidova@eademidova: /var/www/html
File Actions Edit View Help
(eademidova@eademidova)-[~]
$ cd /var/www/html
(eademidova@eademidova)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for eademidova:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4590, done.
remote: Counting objects: 100% (140/140), done.
remote: Compressing objects: 100% (102/102), done.
remote: Total 4590 (delta 58), reused 102 (delta 37), pack-reused 4450
Receiving objects: 100% (4590/4590), 2.34 MiB | 3.20 MiB/s, done.
Resolving deltas: 100% (2153/2153), done.
(eademidova@eademidova)-[/var/www/html]
$
```

Рис. 3.1: Клонирование репозитория с DVWA

Затем запускаем веб сервер(рис. 3.2, 3.3).



```
(eademidova@eademidova)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html
(eademidova@eademidova)-[/var/www/html]
$ sudo service apache2 start
```

Рис. 3.2: Запуск apache2

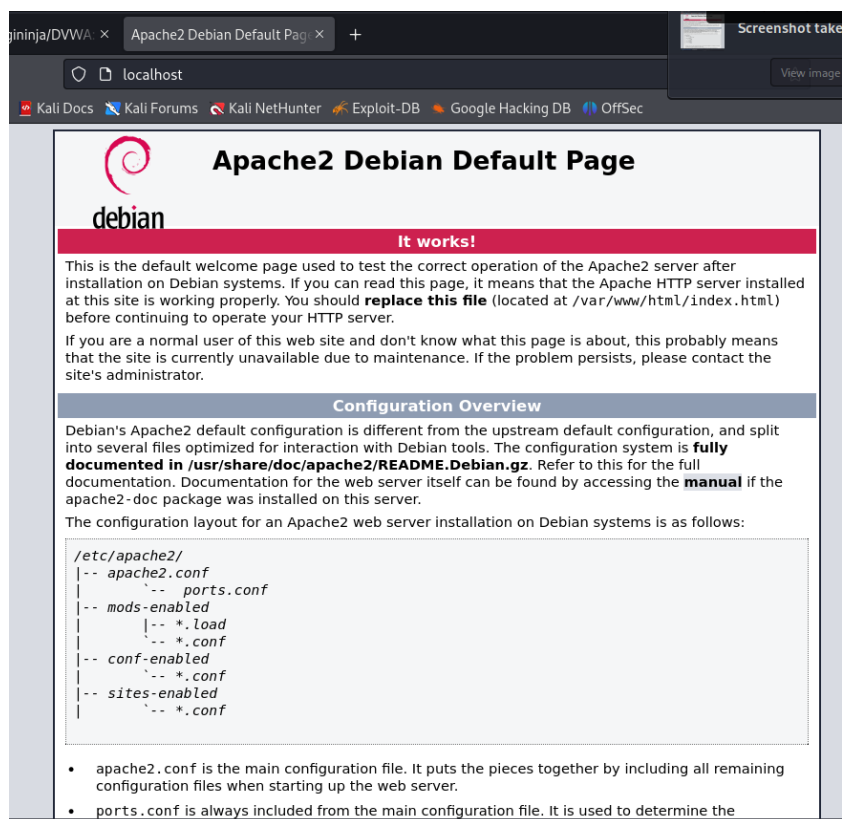


Рис. 3.3: Проверка работы веб-сервера

Затем скопируем файл конфигураций DVWA, чтобы затем можно было его безопасно изменять. Мы воспользуемся именем пользователя и паролем по умолчанию(рис. 3.4, 3.5).


```
eademidova@eademidova: /var/www/html/DVWA
File Actions Edit View Help
(eademidova@eademidova)-[/var/www/html]
$ cd DVWA
(eademidova@eademidova)-[/var/www/html/DVWA]
$ sudo cp config/config.inc.php.dist config/config.inc.php
(eademidova@eademidova)-[/var/www/html/DVWA]
$ ls
CHANGELOG.md  README.fa.md  README.pt.md  compose.yml  external  login.php  security.php
COPYING.txt   README.fr.md  README.tr.md  config       favicon.ico  logout.php  security.txt
Dockerfile    README.id.md  README.zh.md  database     hackable    php.ini     setup.php
README.ar.md  README.ko.md  SECURITY.md   docs         index.php   phpinfo.php tests
README.es.md  README.md     about.php    dvwa         instructions.php  robots.txt  vulnerabilities

(eademidova@eademidova)-[/var/www/html/DVWA]
$ cat config/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' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_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' ] = '';

# 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' ] = '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'.
$_DVWA[ 'default_locale' ] = 'en';
```

Рис. 3.4: Просмотр файла конфигураций

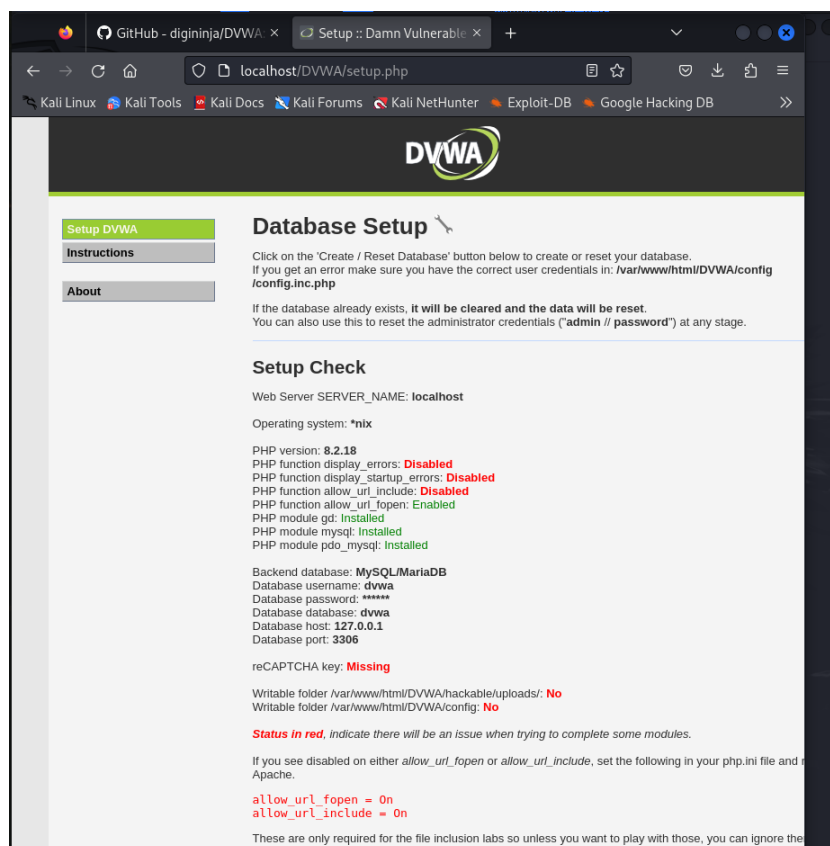


Рис. 3.5: Просмотр стартового окна DVWA

Запустим сервер mariadb и создадим на нем пользователя(имя и пароль совпадают с данными в файле конфигурации dvwa)(рис. 3.6, 3.7).



Рис. 3.6: Создание пользователя mariadb и базы данных

```
(eademidova@eadeidova)-[~]
$ mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.11.8-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)]> use dvwa;
Database changed
MariaDB [dvwa]>
```

Рис. 3.7: Проверка пользователя mariadb

Затем на стартовом окне DVWA нажмем кнопку Create/Reset Database, и нас перекинет на страницу ввода данных учетной записи. После ввода увидим рабочую область DVWA(рис. 3.8, 3.9).

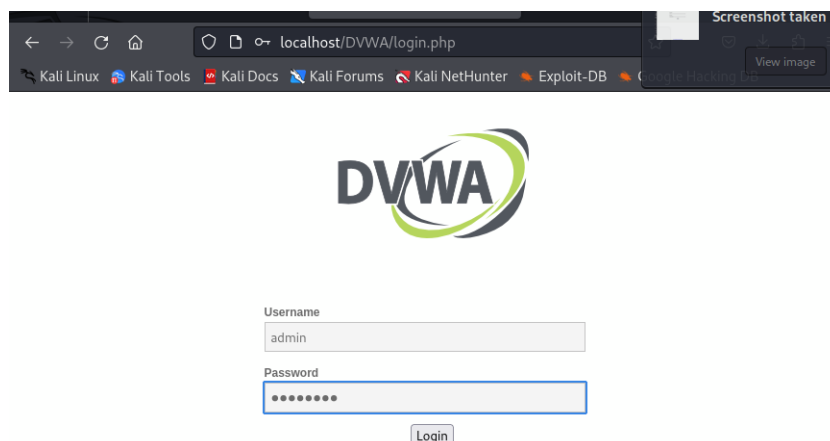


Рис. 3.8: Аутентификация

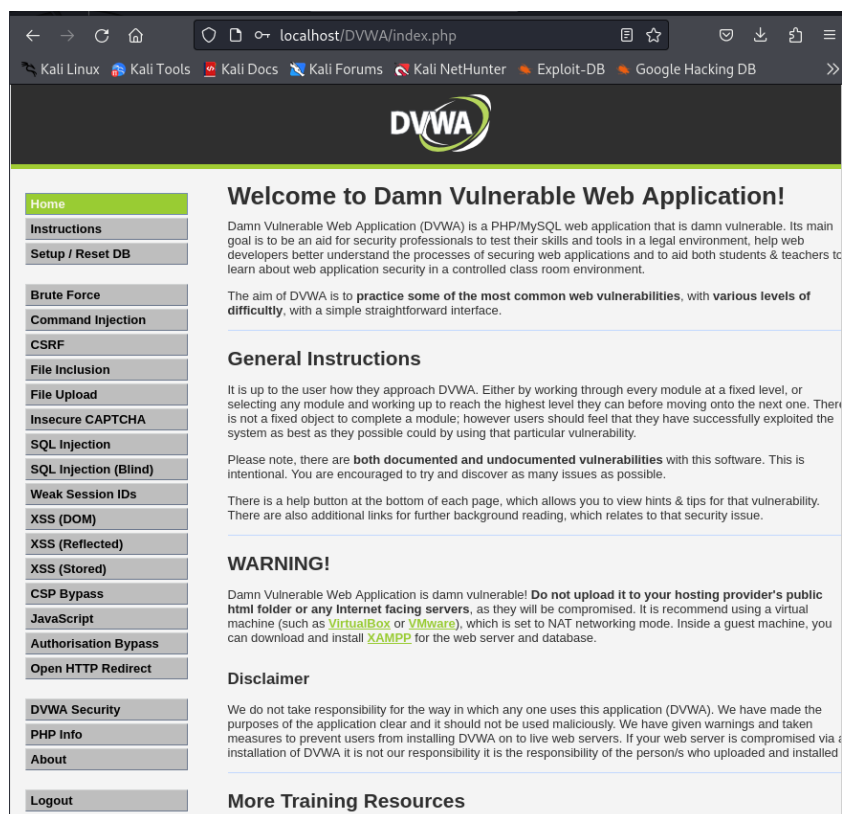


Рис. 3.9: Запуск DVWA

4 Выводы

В результате выполнения работы был установлен DVWA на Kali Linux.

Список литературы

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: <https://github.com/digininja/DVWA>.