

Основы информационной безопасности

Индивидуальный проект. Этап №2. Установка DVWA

Нзита Диатезилуа Катенди

Содержание

Постановка задачи	4
Теоретические сведения	5
Выполнение лабораторной работы	7
Выводы	14
Список литературы	15

Список иллюстраций

1	Клонирование репозитория с DVWA	7
2	Запуск apache2	8
3	Проверка работы веб-сервера	9
4	Просмтр файла конфигураций	10
5	Просмотр стартового окна DVWA	11
6	Создание пользователя mariadb и базы данных	11
7	Проверка пользователя mariadb	12
8	Аутентификация	12
9	Запуск DVWA	13

Постановка задачи

Целью данной работы является установка DVWA на Kali Linux в виртуальную машину.

Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~@dvwa]. 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.

DVWA (Damn Vulnerable Web Application) — это приложение, предназначенное для практики работы с распространёнными веб-уязвимостями, предлагая пользователю интуитивно понятный интерфейс. Оно содержит как документированные, так и недокументированные уязвимости, позволяя исследовать безопасность веб-приложений на разных уровнях сложности.

Некоторые из уязвимостей, представленных в DVWA, включают:

- **Брутфорс:** Атака на формы входа, используемая для тестирования инструментов, позволяющих подбирать пароли, и демонстрации уязвимости слабых паролей.
- **Выполнение команд:** Позволяет злоумышленнику исполнять команды на уровне операционной системы.
- **Межсайтовая подделка запроса (CSRF):** Позволяет злоумышленнику изменять пароль администратора.
- **Внедрение файлов:** Злоумышленник может подключать удалённые или локальные файлы к веб-приложению.
- **SQL-внедрение:** Позволяет вставлять SQL-код в запросы через поля ввода,

включая слепое и основанное на ошибках внедрение.

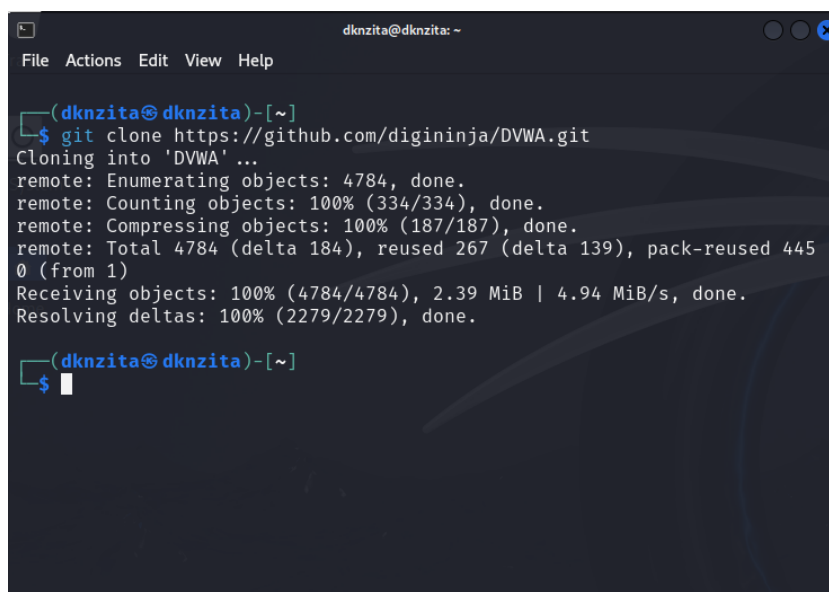
- **Небезопасная выгрузка файлов:** Позволяет загружать вредоносные файлы на сервер.
- **Межсайтовый скриптинг (XSS):** Злоумышленник может внедрять свои скрипты в веб-приложение или базу данных, включая отражённые и сохранённые XSS.
- **Пасхальные яйца:** Раскрытие путей к файлам, обход аутентификации и другие уязвимости.

DVWA предлагает четыре уровня безопасности, которые меняют уязвимость веб-приложений:

- **Невозможный:** Уровень безопасности, при котором приложение защищено от всех уязвимостей. Используется для сравнения уязвимого кода с безопасным.
- **Высокий:** Уровень сложности с элементами более сложных и альтернативных плохих практик, который снижает возможности эксплуатации.
- **Средний:** Уровень, показывающий примеры плохих практик безопасности, где разработчик пытался обеспечить безопасность, но не смог.
- **Низкий:** Полностью уязвимый уровень, предназначенный для демонстрации плохих практик программирования и обучения базовым методам эксплуатации.

Выполнение лабораторной работы

Скопируем в каталог /etc/www/html файла веб приложения DVWA с Гита (рис. @fig:001)



```

(dknzita@dknzita)-[~]
$ git clone https://github.com/digininja/DVWA.git
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 184), reused 267 (delta 139), pack-reused 445
0 (from 1)
Receiving objects: 100% (4784/4784), 2.39 MiB | 4.94 MiB/s, done.
Resolving deltas: 100% (2279/2279), done.

(dknzita@dknzita)-[~]
$
```

Рис. 1: Клонирование репозитория с DVWA

Затем запускаем веб сервер(рис. @fig:002, @fig:003).

```
(dknzita@dknzita)-[~]
$ sudo mv DVWA /var/www/html
[sudo] password for dknzita:

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

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

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

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

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

(dknzita@dknzita)-[/var/www/html]
$ sudo service apache2 start

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

Рис. 2: Запуск apache2

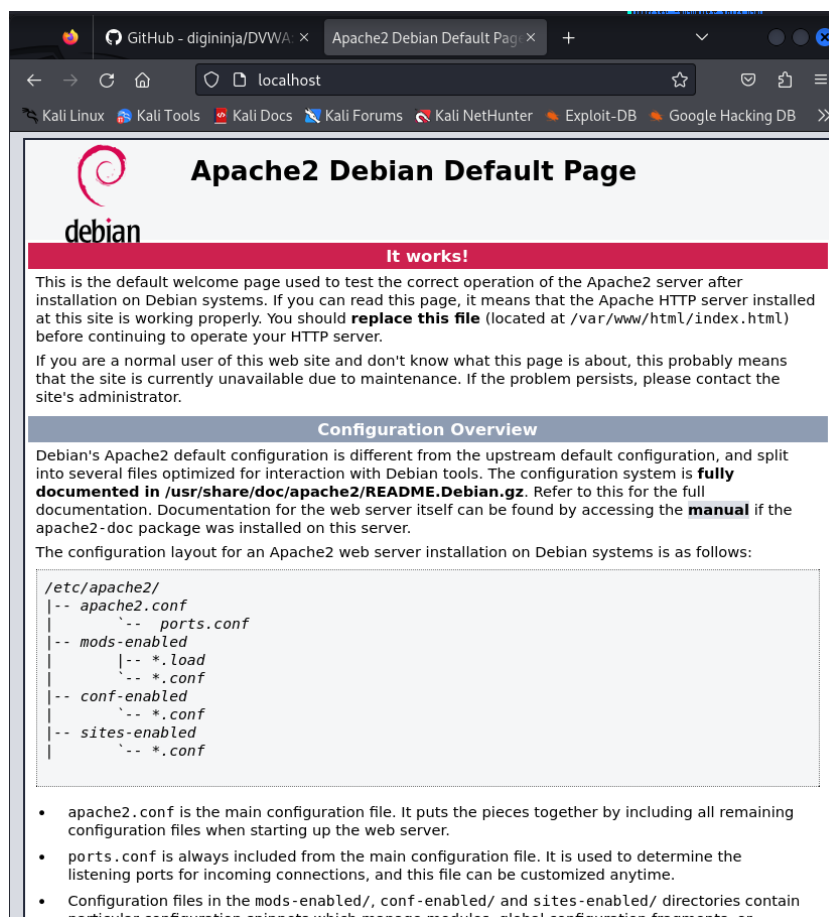


Рис. 3: Проверка работы веб-сервера

Затем скопируем файл конфигураций DVWA, чтобы затем можно было его безопасно изменять. Мы воспользуемся именем пользователя и паролем по умолчанию(рис. @fig:004, @fig:005).

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

(dknzita@dknzita)-[/var/www/html/DVWA]
$ ls
CHANGELOG.md  README.md      database      logout.php
COPYING.txt   README.pt.md   docs          php.ini
Dockerfile    README.tr.md   dvwa         phpinfo.php
README.ar.md  README.vi.md   external     robots.txt
README.es.md  README.zh.md   favicon.ico  security.php
README.fa.md  SECURITY.md    hackable     security.txt
README.fr.md  about.php      index.php    setup.php
README.id.md  compose.yml    instructions.php tests
README.ko.md  config        login.php    vulnerabilities

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

(dknzita@dknzita)-[/var/www/html/DVWA]
$ cp config/config.inc.php config/config.inc.php
cp: cannot stat 'config/config.inc.php': No such file or directory

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

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

Рис. 4: Просмотр файла конфигураций

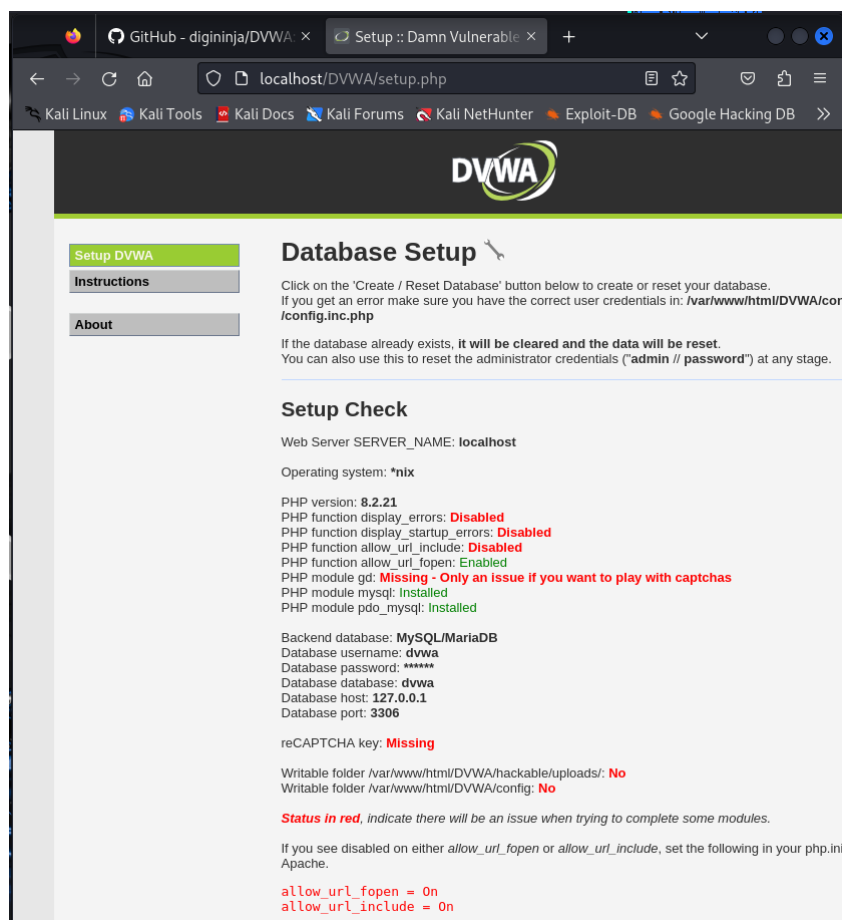


Рис. 5: Просмотр стартового окна DVWA

Запустим сервер mariadb и создадим на нем пользователя и пароль совпадают с данными в файле конфигураций dvwa)(рис. @fig:006, @fig:007).



Рис. 6: Создание пользователя mariadb и базы данных

```
(dknzita@dknzita)-[~]
$ mysql -u dvwa -pDia123
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 35
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)]> use dvwa;
Database changed
MariaDB [dvwa]>
```

Рис. 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. @fig:008, @fig:009).

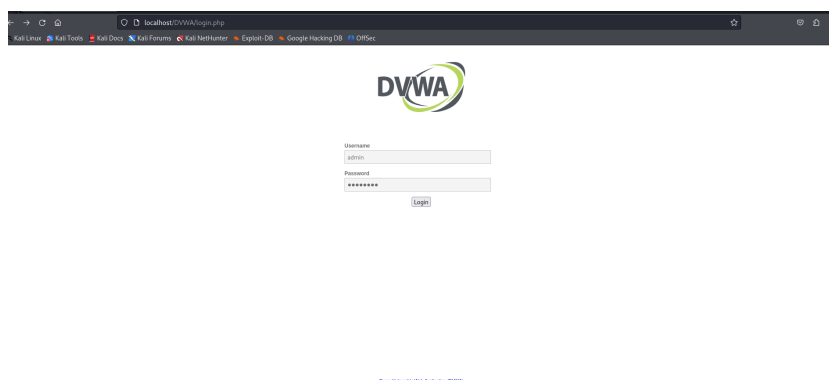


Рис. 8: Аутентификация

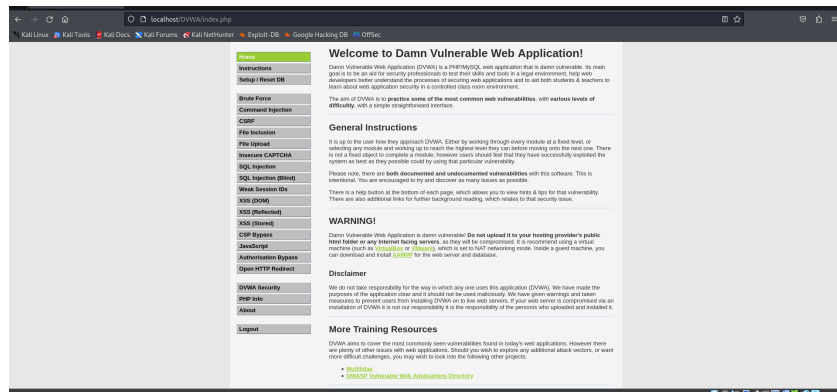


Рис. 9: Запуск DVWA

Выводы

В результате выполнения работы был установлен DVWA на Kali Linux.

Список литературы

.....