

Презентация о выполнении индивидуальнй проект Этап 2

Информационная безопасность

Акандзо Жордани Лади Гаэл.

21 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Акондзо Жордани Лади Гаэл.
- студент 4-го курса группы НКНбд-01-21
- 1032215649
- Российский университет дружбы народов
- GitHub

Вводная часть

Цель работы

Научиться основным способам тестирования веб приложений

Задание

- Найти максимальное количество уязвимостей различных типов.
- Реализовать успешную эксплуатацию каждой уязвимости.

Выполнение лабораторной работы

Установка необходимых зависимостей

- DVWA требует наличия некоторых зависимостей для работы, таких как Apache, MariaDB (или MySQL), PHP и несколько модулей PHP.

```
(jordani@kali)-[~]
$ sudo apt install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php -y
[sudo] password for jordani:
Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
apache2 is already the newest version (2.4.62-1).
apache2 set to manually installed.
mariadb-server is already the newest version (1:11.4.3-1).
mariadb-server set to manually installed.
php is already the newest version (2:8.2+93+nm1).
php set to manually installed.
php8.2-mysql is already the newest version (8.2.23-1).
php8.2-mysql set to manually installed.
libapache2-mod-php is already the newest version (2:8.2+93+nm1).
libapache2-mod-php set to manually installed.
The following packages were automatically installed and are no longer required:
 fonts-liberation2      libpostproc57
 ibverbs-providers      libproxy1-plugin-gsettings
 libassuan0              libproxy1-plugin-networkmanager
 libavfilter9            libproxy1-plugin-webkit
 libboost-iostreams1.83.0 libpython3.11-dev
 libboost-thread1.83.0  librados2
 libcephfs2              librdmacm1t64
 libdisplay-info1        libusbmuxd6
 libgeos3.12.2           openjdk-17-jre
 libgfat0                openjdk-17-jre-headless
 libgfrpc0               python3-lib2to3
 libgfxdr0               python3.11
 libglusterfs0           python3.11-dev
 libibverbs1             python3.11-minimal
 libimobiledevice6       rwho
 libjsoncpp25            rwhod
 libplacebo338           samba-vfs-modules
 libplist3
Use 'sudo apt autoremove' to remove them.

Installing:
 php-gd
```

Запуск служб Apache и MariaDB

- Убедился, что службы Apache и MariaDB запущены.

```
(jordani@kali)-[~]  
$ sudo systemctl start apache2  
  
(jordani@kali)-[~]  
$ sudo systemctl start mariadb  
  
(jordani@kali)-[~]  
$
```

- Чтобы эти службы запускались автоматически при старте системы, выполнил следующие команды.

```
jordani@kali: ~  
  
(jordani@kali)-[~]  
$ sudo systemctl enable mariadb
```

Настройка MariaDB

- Подключусь к MariaDB для создания базы данных и пользователя для DVWA. Потом в командной строке MariaDB выполнил следующие команды.

A screenshot of a terminal window titled 'jordani@kali: ~'. The user is in a shell prompt '(jordani@kali)-[~]'. They run the command '\$ sudo mysql -u root -p'. The terminal shows the MariaDB monitor interface with the following text: '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', and 'Type \'help;\' or \'\\h\' for help. Type \'\\c\' to clear the current input statement.' The user then enters three SQL commands in the MariaDB prompt: 'create database dvwa;', 'create user dvwa@localhost identified by \'Jordanigael7\';', and 'grant all on dvwa.* to dvwa@localhost;'. Each command is followed by a confirmation message: 'Query OK, 1 row affected (0.001 sec)', 'Query OK, 0 rows affected (0.315 sec)', and 'Query OK, 0 rows affected (0.004 sec)' respectively.

```
(jordani@kali)-[~]
$ 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 database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'Jordanigael7';
Query OK, 0 rows affected (0.315 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.004 sec)
```

Загрузка и настройка DVWA

- Скачайл последнюю версию DVWA из репозитория GitHub.

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

(jordani@kali)-[/var/www/html]
$ sudo 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 185), reused 266 (delta 139), pack-reused 4450 (from 1)
Receiving objects: 100% (4784/4784), 2.36 MiB | 602.00 KiB/s, done.
Resolving deltas: 100% (2296/2296), done.

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

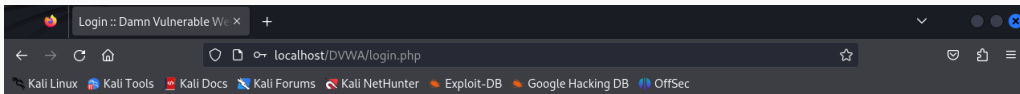
- Потом создал файл конфигурации для DVWA .

Завершение установки DVWA

- Потос открыл браузер и перешёл по адресу: `http://localhost/DVWA/setup.php`. Следовал инструкциям на странице для завершения установки. По окончании установки, вошёл в DVWA, используя следующие данные для входа:

Логин: `admin`

Пароль: `password`



Username

Password

- Проверка настроек базы данных (Setup Check).

Setup :: Damn Vulnerable < +

localhost/DVWA/setup.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

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)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: localhost

Operating system: *nix

PHP version: 8.2.23
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

Выводы

На этом этапе я научился устанавливать и настраивать DVWA на Kali Linux. Я освоил конфигурацию баз данных, работу с Apache и MariaDB, а также внес необходимые изменения в настройки PHP для тестирования уязвимостей. Изучение разных уровней безопасности в DVWA позволило понять, как плохие практики разработки делают приложения уязвимыми для атак.