Experiment-3

Examination of a Website to Test the Vulnerability of Attacks – DVWA Setup & SQLi

Date: 19-8-24

AIM

Examination of a website to test the vulnerability of attacks – DVWA setup & SQLi.

PROCEDURE

Step-1: Login the kali linux. Open browser and search for DVWA—a vulnerable website.

Step-2: Install DVWA in Kali using Terminal

Step-3: Copy config.inc.php.dist and in new file change the login credentials.

Step-4: start mysql service and login to it.

Step-5: Create a database, user and add permissions to that user and exit from the database.

Step-6: Start apache service and open browser and search for http://localhost/DVWAor http://127.0.0.1/DVWA/login.php

Step-7: login to DVWA. Goto DVWA Security click on impossible and change it to LOW.

Step-8: Attack the system using SQLinjection

SOURCECODE

1. open cmd in Kali
→ $ cd ..
→ $ cd ..
→ $ ls
2. Go to var directory

→ $ cd var
→ $ ls
3. list all the files go to www file
→ $ cd www
→ $ ls
4. list all the files and goto html file
→ $ cd html
→ $ ls
5. Go to chrome and search dvwa, click on first link and copy the code link in github and paste.
→ $ sudo git clone https://github.com/digininja/DVWA.git
6. password for cloning is "kali"
→ $ ls
7. create dvwa8
→ $ sudo mv DVWA dvwa8
→ $ ls
8. change directory to dvwa8
→ $ cd dvwa8
→ $ ls
9. It lists all the files go to config.
→ $ cd config
→ $ ls
config.inc.php.dist
10. Now change the inc file to php file.
→ $ sudo cp config.inc.php.dist config.inc.php
→ $ ls
config.inc.php config.inc.php.dist

11) Open the config.inc.php file
→ $ sudo nano config.inc.php
12) Now change the db_database = 'dvwa8', db_user='admin',
db_password = 'password'
13) Hold ctrl and press X, Y then Enter.
14) To display the changes made in php file type
→ $ cat config.inc.php
15) Rember server number '127.0.0.1', username & password
→ $ sudo service mysql start
→ $ sudo mysql -u root -p
16) Enter password as "kali"
17) In database type - show database;
18) For creating database type - create database dvwa8;
19) Again check the created database type - show database;
→ Grant permission type - grant all on dvwa8.* to admin@127.0.0.1;
20) for exit type - exit;
→ $ cd /etc
→ $ ls
→ $ cd php
→ $ cd 8.2
→ $ cd apache2
→ $ ls
conf.d php.ini
→ $ sudo nano php.ini
Enter password : kali
21) Press ctrl+W, type fopen and press enter.
In ; fopen wrappers ;
;;;;;;;;;;;;;;;

OUTPUT

22) check allow_url_fopen = On and allow_url_include=On should be On. if it is in Off change to On.

23) Press ctrl+X and ctrl+Y

→ $ sudo service apache2 start

e $ sudo nano php.ini

Open browser and type https://127.0.0.1/dvwa/login.php type username as admin and password as password and click on login. Click on create/reset database again do login.

24) Click on DVWA Security, goto click on impossible and change it to low and submit.

25) Click on SQL injection, in user ID enter 1 and submit it displays the information in database.

Note: If any error occur while granting permission in database just type command -

create user 'admin'@127.0.0.1' identified by 'password';

Experiment-4

Examination of a Website to test the Vulnerability of Attacks

Date: 27-8-24

AIM

Examination of a website to test the vulnerability of attacks- XSS & CSRF & Command Line injection attack.

PROCEDURE:

Use previous experiment to setup DVWA

Step-1: If the DVWA website setup is done run apache and my sql service in the terminal and open a browser to access the website.

Step-2: Change the level of DVWA security.

Step-3: Click Command Injection and use IP address to test.

Step-4: Click and test XSS Reflection.

Step-5: Click and test CSRF Attack

SOURCE CODE:

- Follow the same steps to setup DVWA
- Setup the DVWA security to Low.
- Click on Command Injection and enter IP address

- Enter multiple commands using pipe or 127.0.0.1;ls, 127.0.0.1;ls../, 127.0.0.1;cat../view_source.php, 127.0.0.1&&net user
- While using 127.0.0.1&net user command, open cmd in the windows system and use the command ping 0.0.0.0&&net user.
- Now use the command ping 0.0.0.0&net user - replace & with &&
- for XSS Reflection → click on XSS(Reflected) → enter any name in the text box and click on submit it displays the name.
- for CSRF attack
- Click on CSRF, enter pa username & password same used for DVWA login. Click on login.