Experiment-3

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

Date: 28/08/24

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

```
cd /var/www/html
$ ls
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for kali: kali
cloning into 'DVWA'. . . .
```

```
remote : Enumerating
Receiving objects : 100% (459314593), 2.34
$ ls
$ sudo mv DVWA dvwa
$ sudo chmod -R 777 dvwa
$ cd dvwa
$ ls
$ cd config
$ ls
Config .inc . php .dist
$ sudo cp config.inc.php.dist config.inc.php
$ ls
Config .inc . php Config.inc.php .dist
$ sudo nano config.inc.php
Note : change username as admin and password as
Password ctrl + x → y → Hit Enter
$ cat config.inc.php
$ sudo service mysql start
Sudo mysql -u Root -p
Enter password :' password'
Welcome to the MariaDB monitor
mariaDB [(none)] > Create database dvwa;
> Create user admin@127.0.0.1 identified by 'password';
> grant all on dvwa * to admin@127.0.0.1;
> exit
> cd /etc
> ls
> cd php
```

```
>ls
>cd 8.2
>ls
>cd apache 2
>ls
>Sudo nano php.ini
```

Press ctrl+w type fopen change url_include as 'on"

ctrl+x+y → to move out of Screen.

>Sudo Service apache 2 start

Go to the browser and type http://127.0.0.1/dvwa/

login page

→Enter username and password

admin password

→click on create/reset database again enter username and password.

→Go to DVWA Security and set low, submit

click on SQL injection in user Id type %

or '1'='1'

and click submit

Id: % or '1'='1'

First name = admin

Surname = admin

ID: % or '1'='1'

Firstname: Garden

Surname Brown