Experiment-4

Examination of a Website to test the Vulnerability of Attacks

Date: 4/9/24

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 run IP address to test.

Step-4: Click and test XSS Reflection.

Step-5: Click and test CSRF Attack

SOURCECODE

→ start the process from here then go to the before page

```
$ cd/var/www/html
$ ls
$ sudo git clone https://github.com/digininja/DVWA.git
        Password : Kali
```

```
$ls
$ sudo mv DVWA dvwa
$ sudo chmod -R 777 dvwa
$cd dvwa
$ls
$ cd Config
$ ls
$ cd config
$ ls
Config.inc.php.dist
$sudo ep config.inc.php.dist Config.inc.php
$ls
$ sudo nano config.inc.php
    change username - Admin
                Password - password
$ cat config.inc.php
$ sudo Service my.sql start
$ sudo mysql -u root -p
            enter : password
 welcome to the MariaDB monitor
> create database dvwa;
 Create user admin@127.0.0.4 identified by 'password';
>grant all on dvwa.* to admin@127.0.0.1;
>exit
 > cd /etc/php/8.2/apache2
```

```
>ls
>sudo apache2
>ls
>sudo nano php.ini
```

Press c̄trl+w

type fopen

change_url_include='on' c̄trl+x+y → move out of screen.

```
$sudo service apache2 start
```

→goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php

username: admin password: password

→ click create database

we get http://127.0.0.1/DVWA/index.php

→ Go to DVWA security

→click on impossible and set as low and click Submit.

→ Enter IP address

$ multiple commands using pipe or ;

```
$ 127.0.0.1
$ 127.0.0.1 ;ls
$ 127.0.0.1; ls. ../
$ 127.0.0.1 ; cat ../view_source.php
```

→127.0.0.1 && net user

→open command prompt in the windows system and use the command ping 0.0.0.0& net user.

OUTPUT

→Now use the Command ping 0.0.0.0 & Rnet user replace & with & &

→click xss Reflection

Enter any name in the text box and click submit

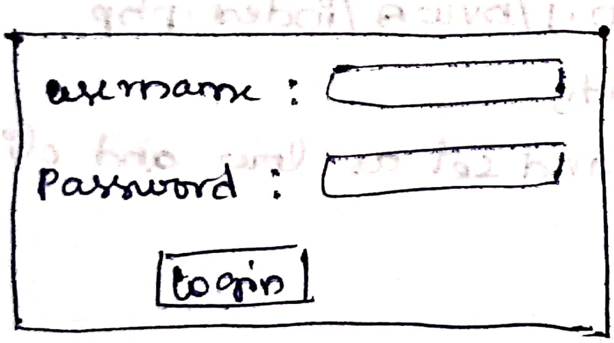
→It displays as

Now instead of any text let's try some Script text.

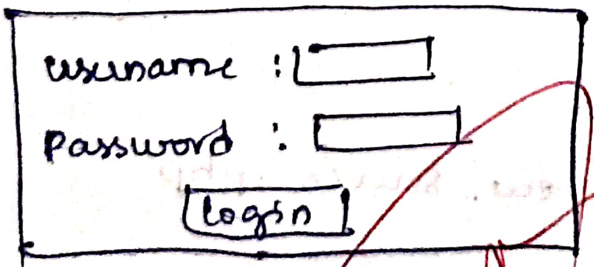
Ex: <Script> alert ('Hello world') </script>

→It displays ~~an~~ alert as shown below.

→ click ok.



Valid password


username :
Password :
login