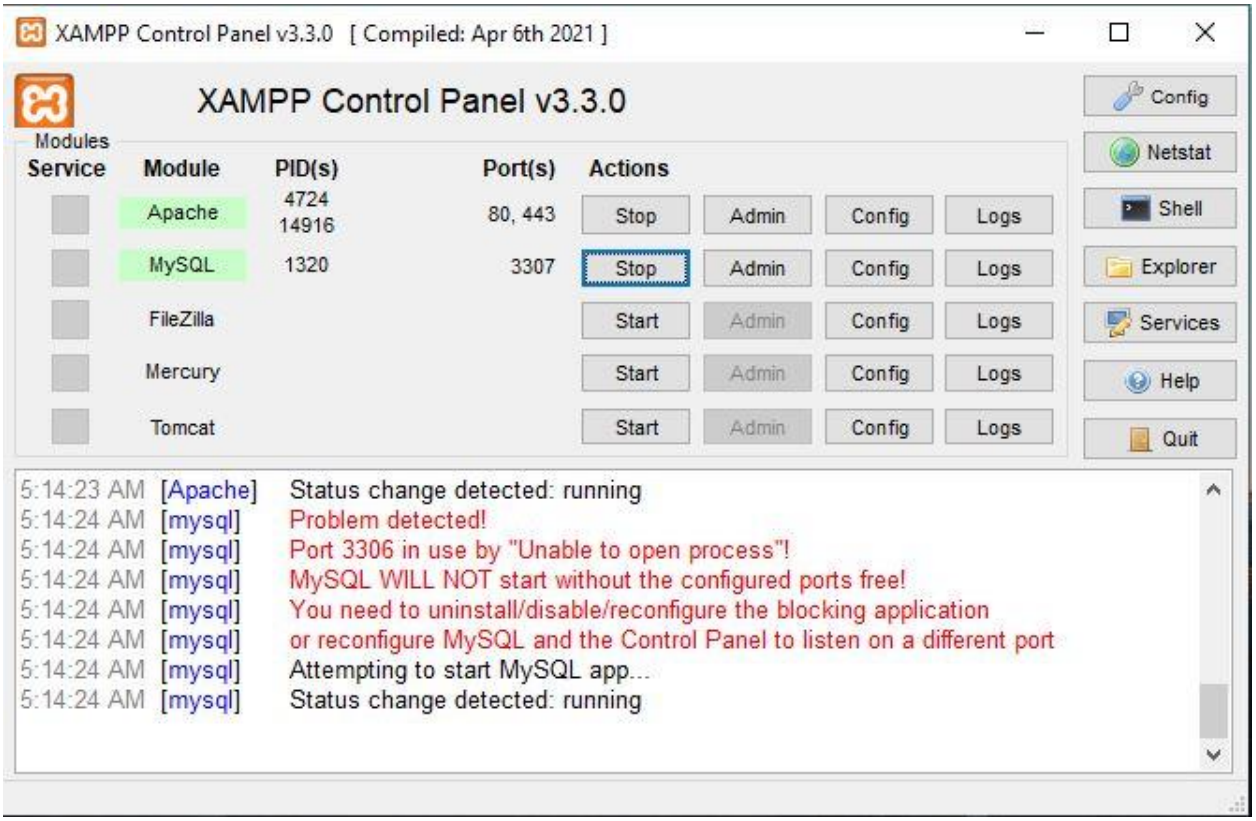
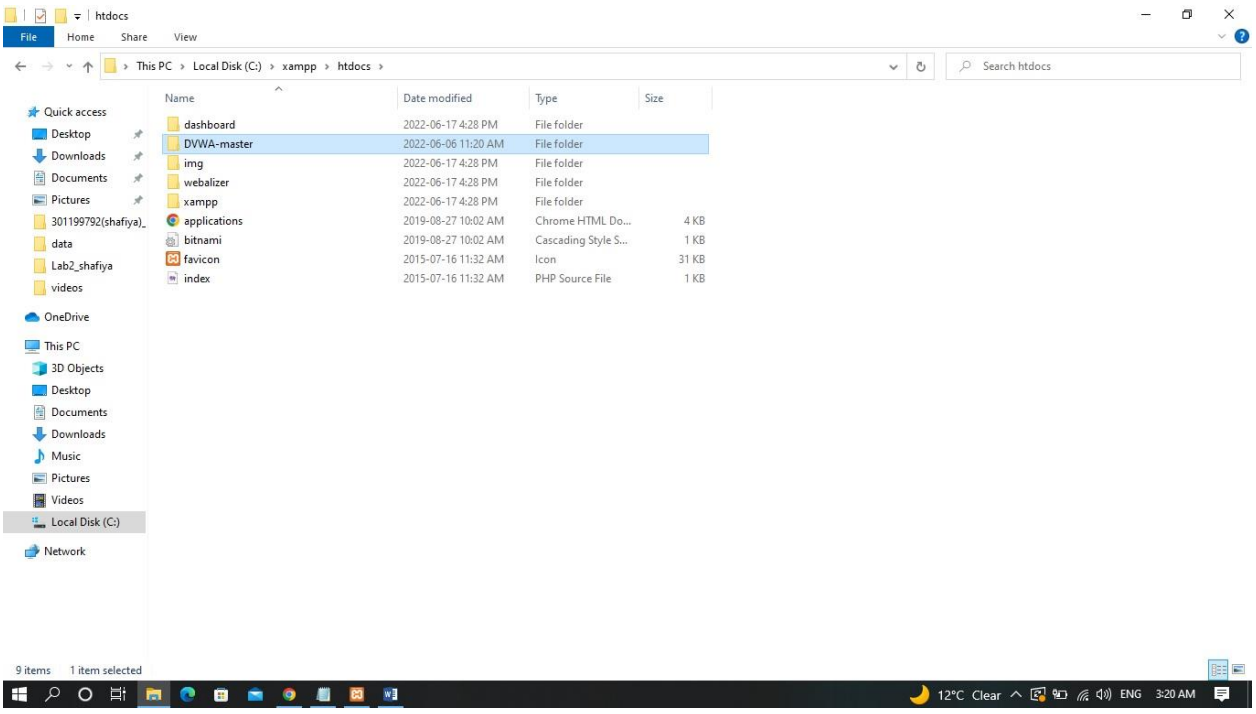
LabAssignment 6 (5 Contd..)

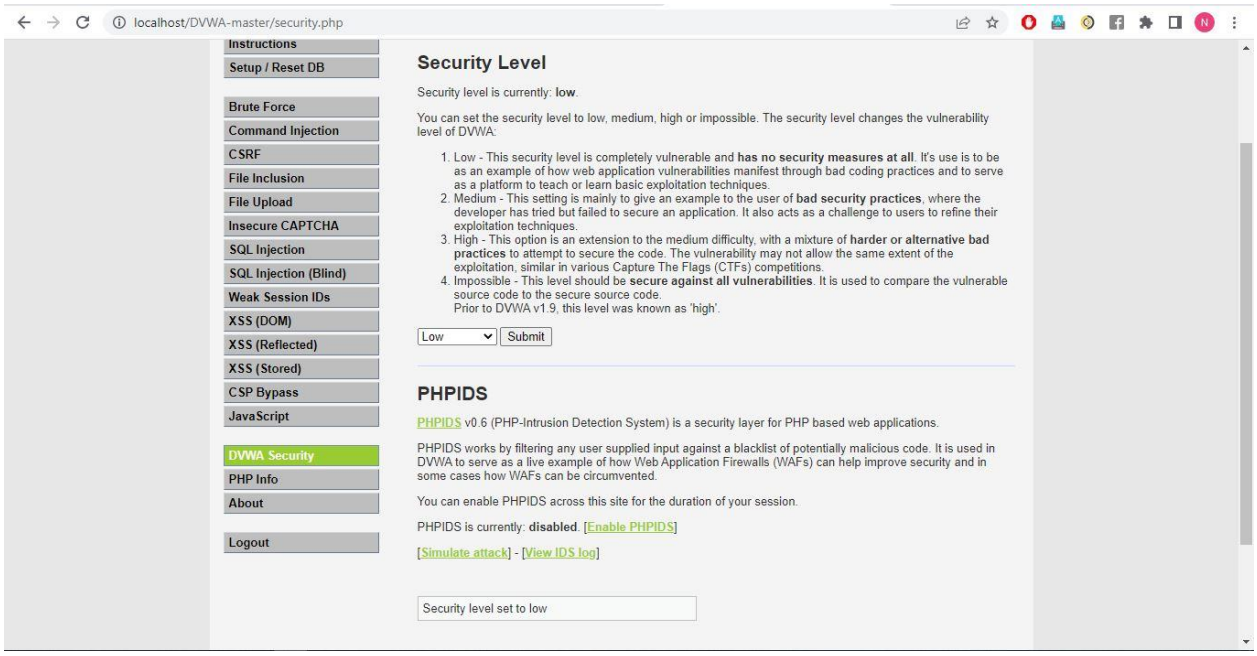
Pre-requisite step

0) Setup XAMPP+DVWA (as before) (Take snapshot)

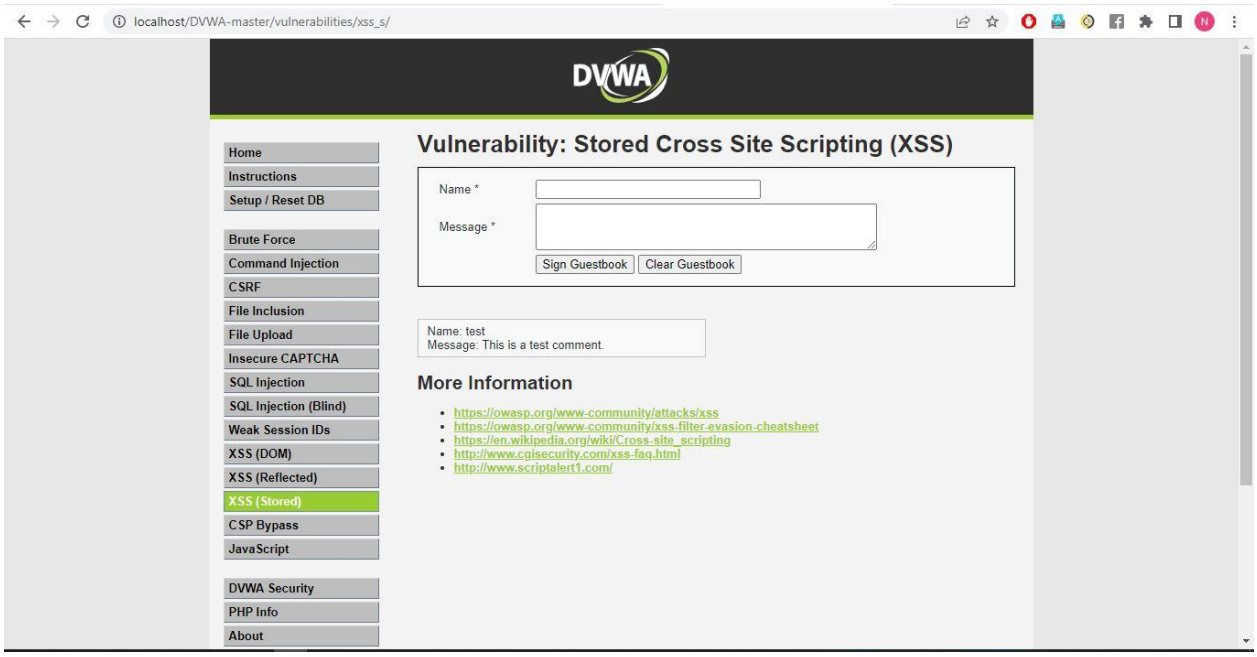




1) **Login** DVWA and Set Security Low (Take snapshot)



2) Goto 'XSS Stored' (Take snapshot)

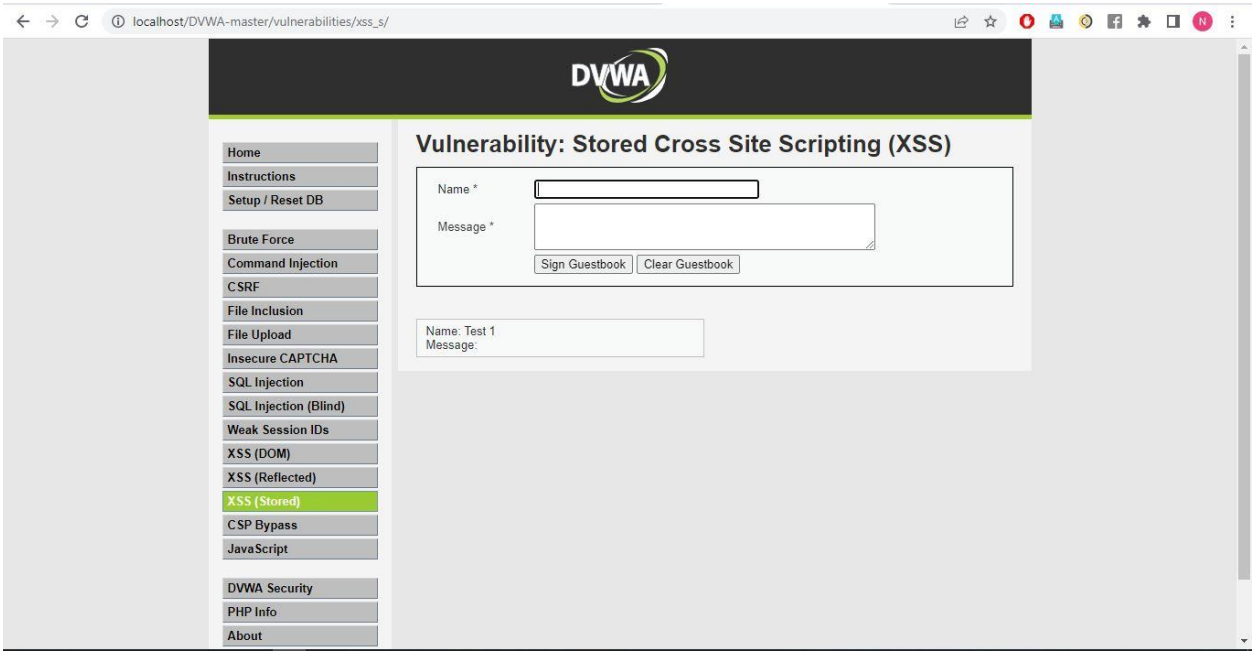


A) Basic XSS Test

1. Name: Test 1

2. Message: <script>alert("This is a XSS Exploit Test")</script>

3. Click Sign Guestbook

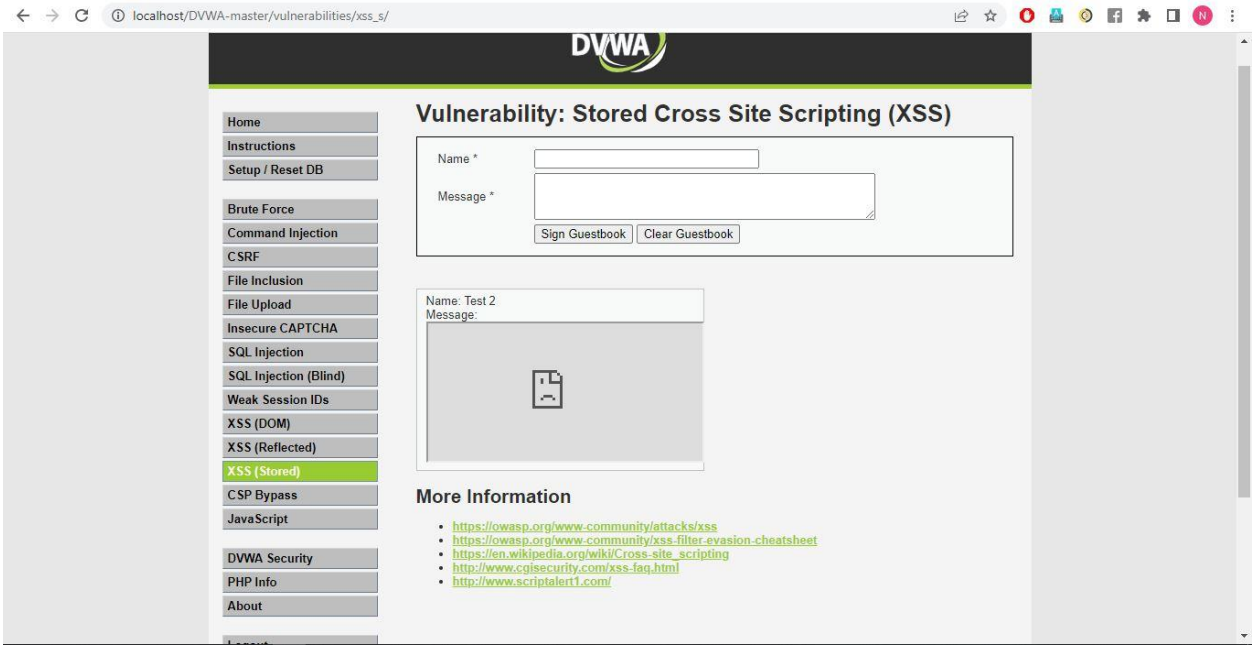


B) XSS Test 2 (Take snapshot)

0. Name: Test 2

1. Message: <iframe src="http://www.cnn.com"></iframe>

2. Click Sign Guestbook

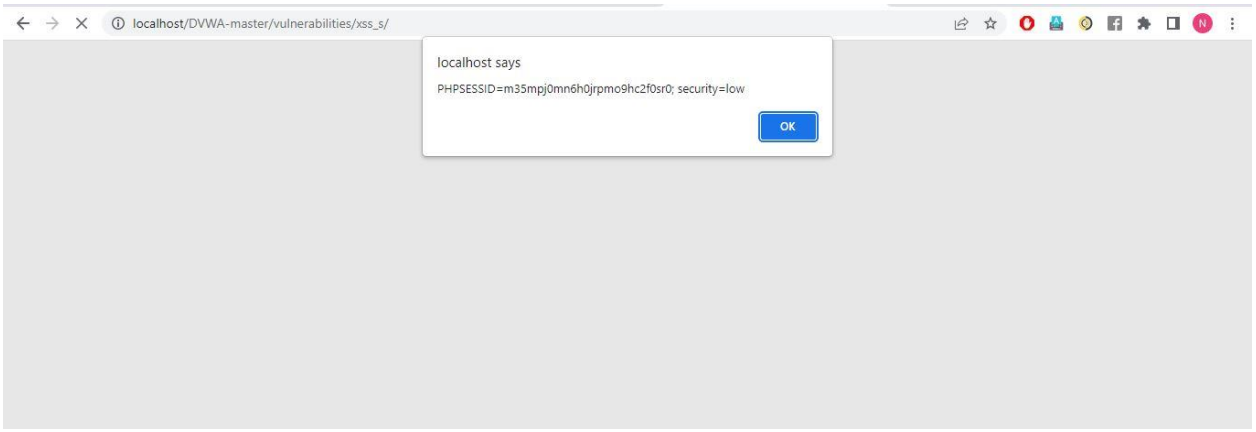


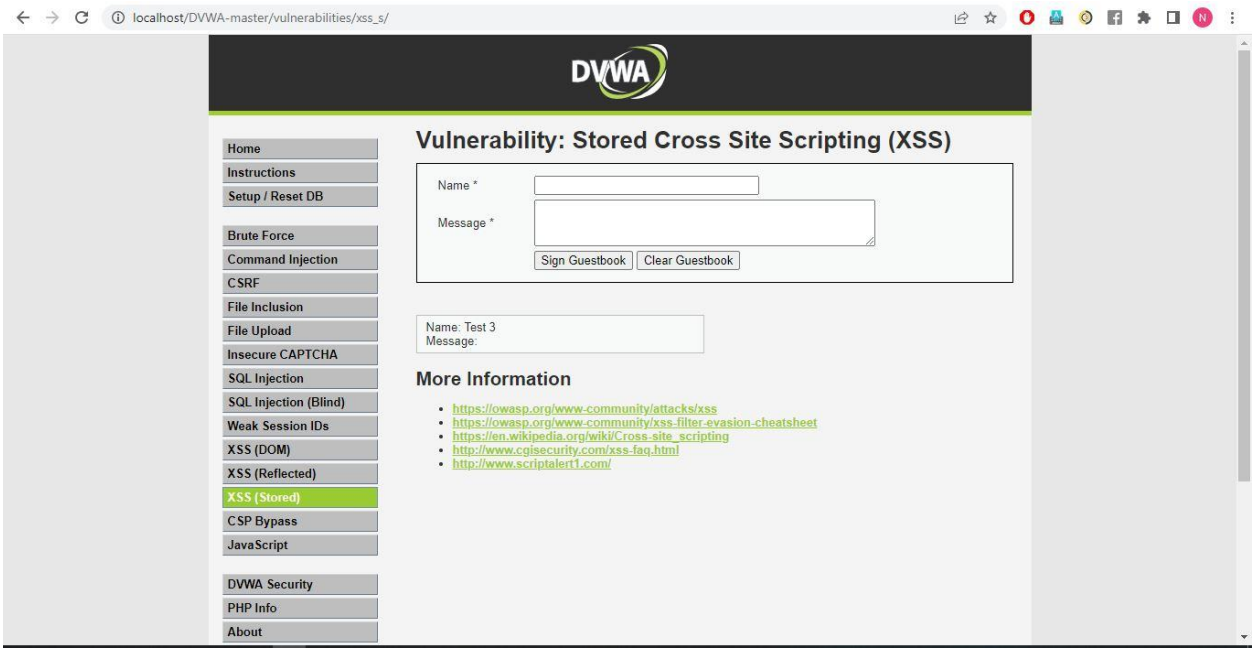
C) XSS Test 3 (Take snapshot)

0. Name: Test 3

1. Message: <script>alert(document.cookie)</script>

2. Click Sign Guestbook

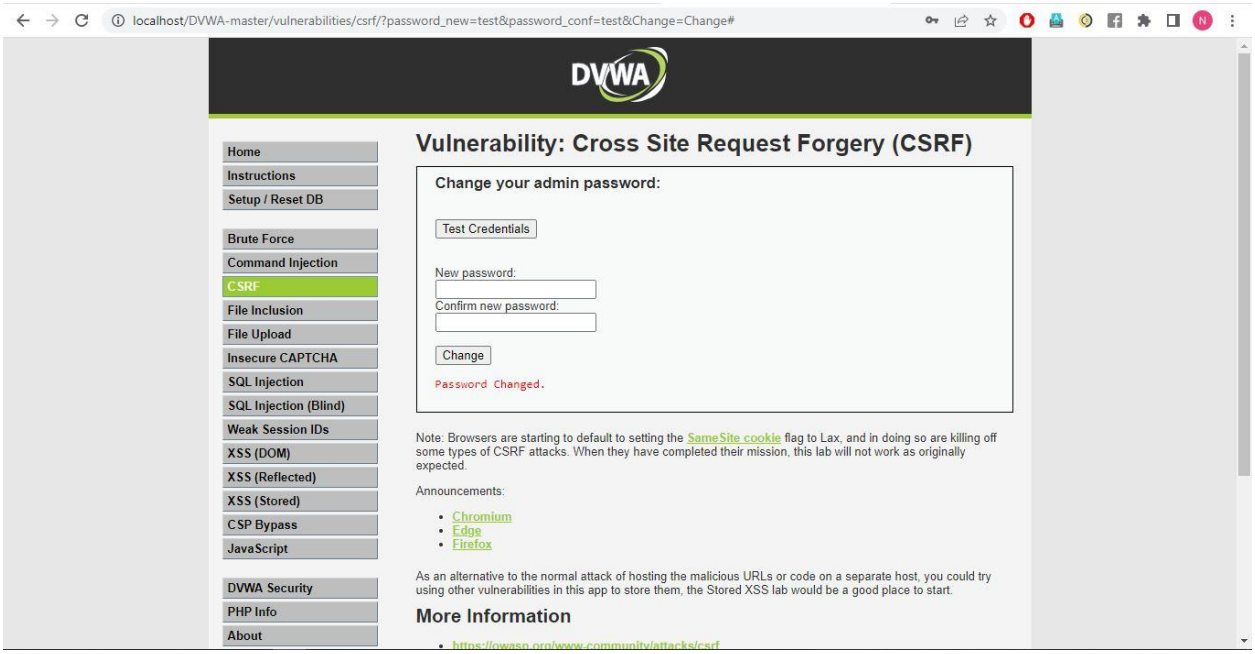




CSRF

Step 1: In the DVWA navigation menu, **click** the **CSRF button.**
Step 2: As a valid user of the Web application, type boxes on the following data into the CSRF page and click Change to change the admin password. (Take snapshot)

New password: **test**
Confirm new password: **test**



Once the code form is submitted, the CSRF page displays a confirmation message indicating that the password has changed, and the URL of the CSRF page now includes a query string (http://172.30.0.11/dvwa/vulnerabilities/csrf/?password_new=test&password_conf=test Change=Change#) that forces the password change.

File Inclusion

Step 1: In the DVWA navigation menu, **click** the **File Inclusion button.**

Step 2: (Take snapshot) In the URL, **highlight include.php and Type file1.php,** so that the complete URL reads:

http://172.30.0.11/dvwa/vulnerabilities/fi/?page=file1.php, and **press Enter** to submit the script.