Practical - 7

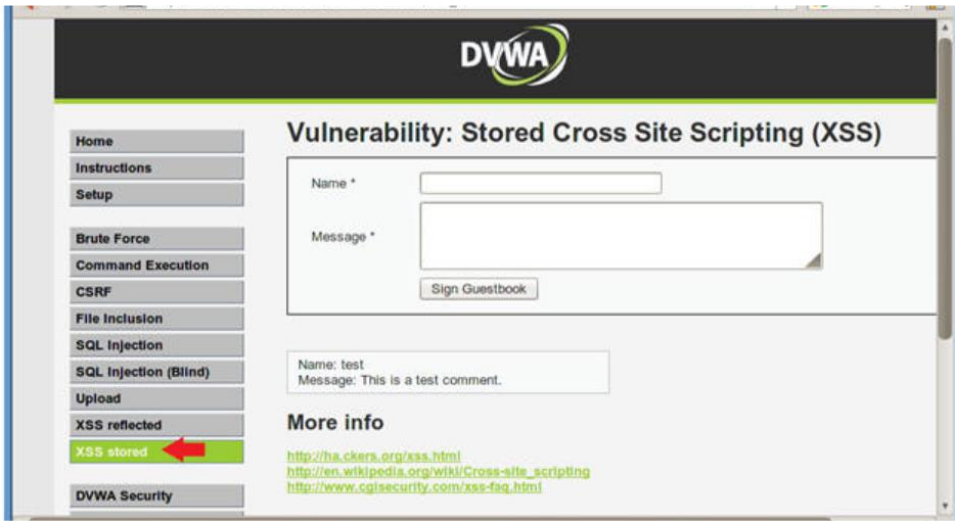
Aim: - XSS using DVWA

Cross-Site Scripting (XSS): -

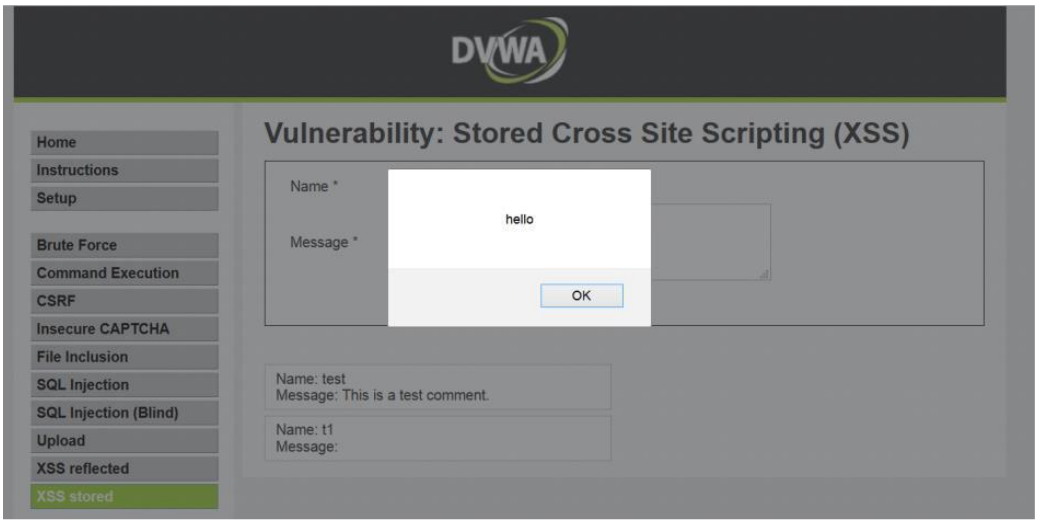
- Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications.
- XSS enables attackers to inject client-side script into Web pages viewed by other users.
- A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.
- In Addition, the attacker can send input (e.g., username, password, session ID, etc) which can be later captured by an external script.
- The victim's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

Process of XSS using DVWA: -

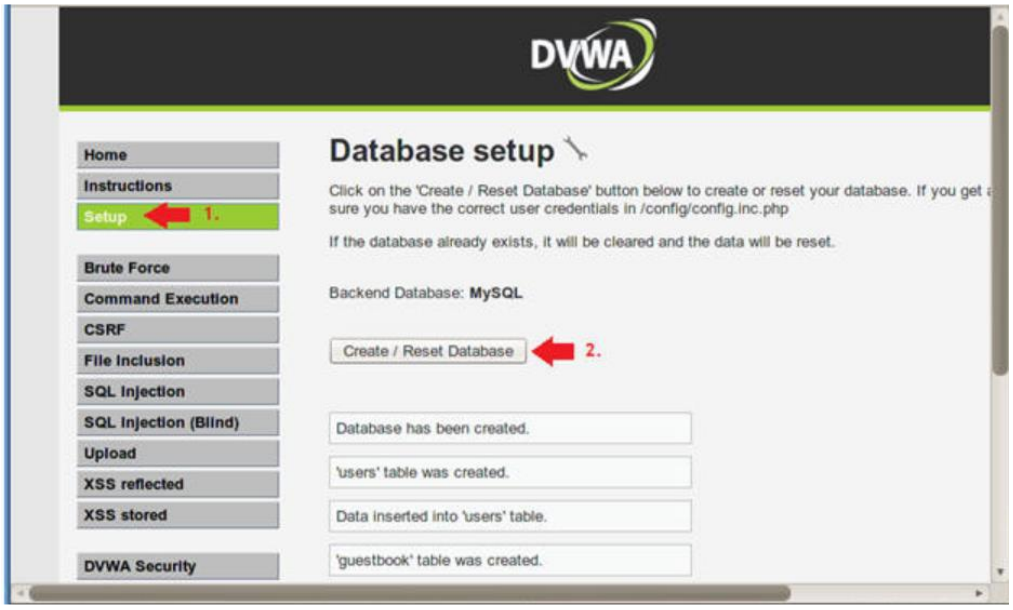
1. **XSS Stored Menu**
   Select "XSS Stored" from the left navigation menu.



2. **Basic XSS Test**
   1. Name: Test 1
   2. Message: <script>alert("hello")</script>
   3. Click Sign Guestbook



3. **Reset Database**
    1. Select "Setup" from the left menu navigation.
    2. Click on the Create / Reset Database Button.



4. **XSS Stored Menu**
    1. Select "XSS Stored" from the left navigation menu.

5. **XSS Test 2**
    1. Name: Test 2
    2. Message: <iframe src="http://wikipedia.org"></iframe>
    3. Click Sign Guestbook

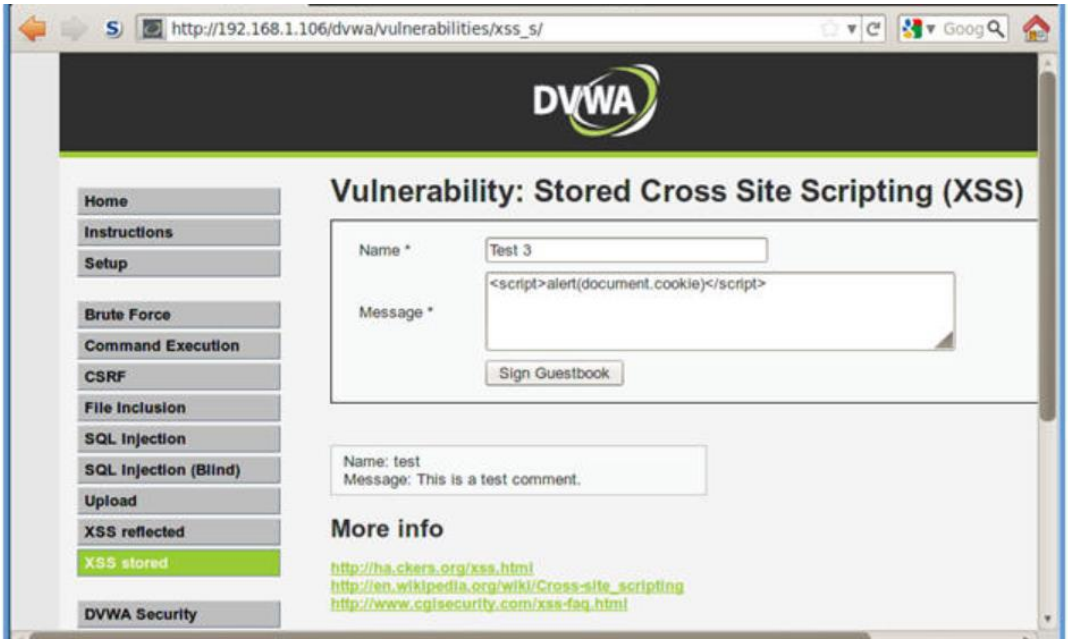
6. **XSS Stored COOKIE Exploit Test**

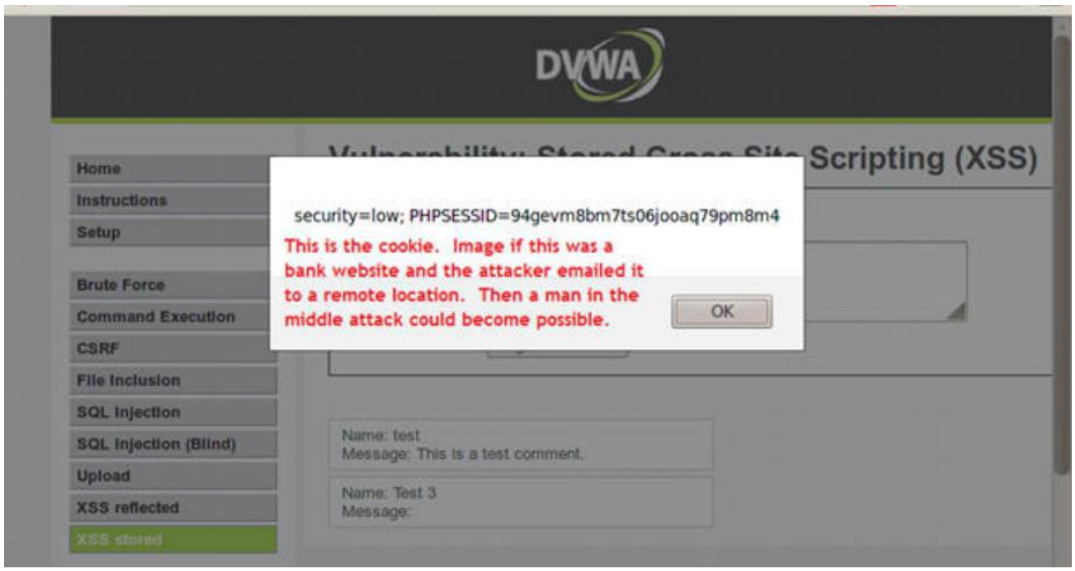
   Reset Database

   1. Select "Setup" from the left menu navigation.
   2. Click on the Create / Reset Database Button.

7. **XSS Test 3**

   1. Name: Test 3
   2. Message: <script>alert(document.cookie)</script>
   3. Click Sign Guestbook




DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Scripting (XSS)
security=low; PHPSESSID=94gevm8bm7ts06jooaq79pm8m4
This is the cookie. Image if this was a bank website and the attacker emailed it to a remote location. Then a man in the middle attack could become possible.
OK
Name: test
Message: This is a test comment.
Name: Test 3
Message: