

Amir Mansha

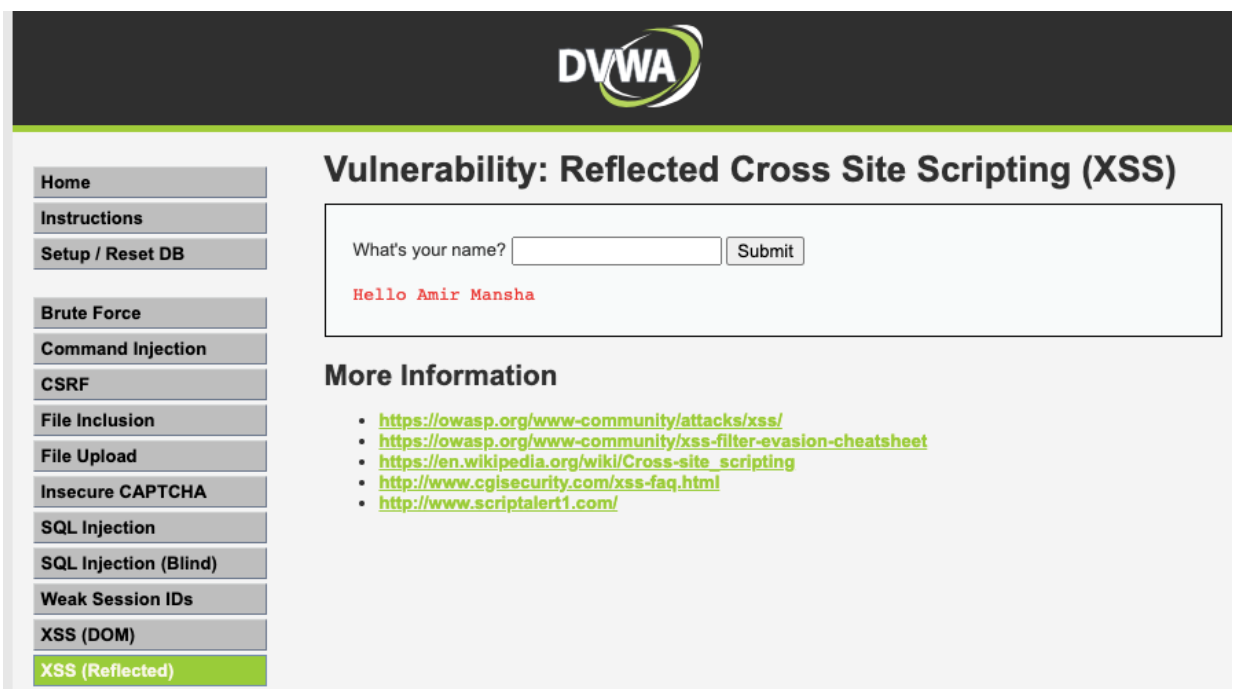
CYSE 230 – 001

Lab #4 Cross site scripting

11/14/20

TASKS

1.) Type name in textbox



The screenshot shows the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, on the left, is a sidebar menu with buttons for 'Home', 'Instructions', 'Setup / Reset DB', 'Brute Force', 'Command Injection', 'CSRF', 'File Inclusion', 'File Upload', 'Insecure CAPTCHA', 'SQL Injection', 'SQL Injection (Blind)', 'Weak Session IDs', 'XSS (DOM)', and 'XSS (Reflected)'. The 'XSS (Reflected)' button is highlighted in green. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. It contains a form with the text 'What's your name?' followed by a text input field and a 'Submit' button. Below the input field, the text 'Hello Amir Mansha' is displayed in red. Underneath the form, there is a section titled 'More Information' with a list of links: <https://owasp.org/www-community/attacks/xss/>, <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>, https://en.wikipedia.org/wiki/Cross-site_scripting, <http://www.cgisecurity.com/xss-faq.html>, and <http://www.scriptalert1.com/>.

2.) Make name bold

Vulnerability: Reflected Cross

What's your name?

Submit

Hello Amir

3.) Make name purple

Vulnerability: Reflected Cross Site

What's your name?

Submit

Hello Amir

4.) Use a website to load in the frame. I used <https://www.dunyabanquet.com/> it is an afghan restaurant.

What's your name?

Submit

Hello



5.) Type an alert message and then the document cookie alert message. I used safari web browser.

what is your name!!!

Close

security=low;
PHPSESSID=811d54086e064a1fd2497881f90fb723

Close
