USTH-BS3 – Web Security -Lab 02 – XSS Attacks (1,5 hours)

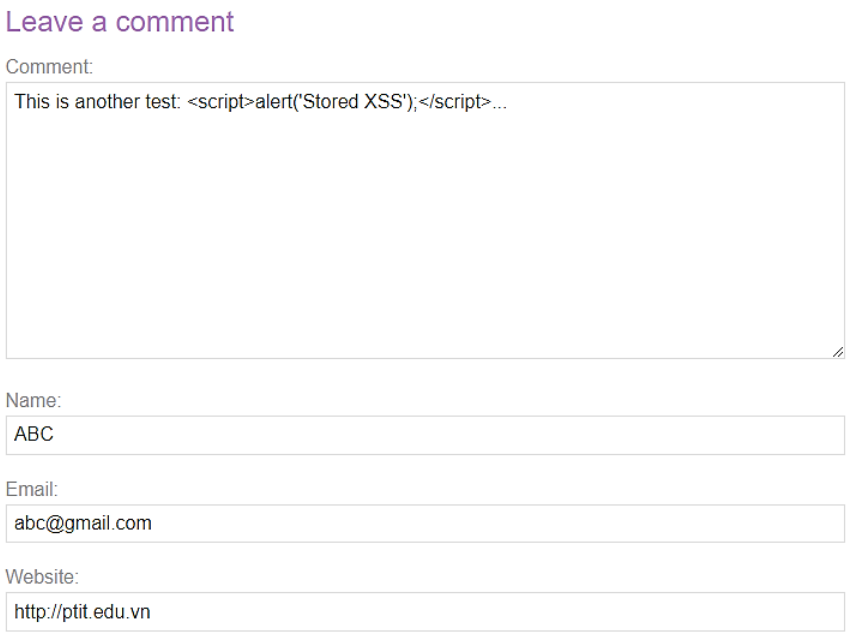
A. Lecture revision

- XSS vulnerabilities in web applications and causes
- XSS types (Stored XSS, Reflected XSS, DOM-Based XSS).
- Defensive measures
  + XSS filter
  + XSS escape

B. Lab 02 Content

1. Stored XSS

- Read additional information about Stored XSS at: https://portswigger.net/web-security/cross-site-scripting/stored
- Create and activate an account with portswigger.net at https://portswigger.net/users/register
- Do the stored XSS lab at https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded (click at 'Access the lab' button and provide the email and password to log in)
- Open post to read and go down for comment section:
  + Enter comment with a piece of JS code, such as "I am new to XSS <script>alert('Stored XSS');</script>...", name, email, website URL and click "Post Comment" button.
  + Back to the page and you will see the the pop-up message 'Stored XSS' on screen and the message "Congratulations, you solved the lab!"
  + Take the screenshot (with your entered information) and paste into the word result file as the evidence you've done the lab:



2. Reflected XSS

- Read additional information about Reflected XSS at: https://portswigger.net/web-security/cross-site-scripting/reflected
- Do the reflected XSS lab at https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

- Take the screenshot (with your entered information) and paste into the word result file as the evidence you've done the lab.

3. DOM-based XSS

- Read additional information about DOM-based XSS at: https://portswigger.net/web-security/cross-site-scripting/dom-based
- Do the DOM-based XSS lab at https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink-inside-select-element
- Take the screenshot (with your entered information) and paste into the word result file as the evidence you've done the lab.

4. Practice more XSS labs (Capture completed screenshots**):**

- https://portswigger.net/web-security/cross-site-scripting/contexts/lab-event-handlers-and-href-attributes-blocked
- https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-url-some-characters-blocked
- https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-perform-csrf

5. Web/JavaScript/SQL vulnerability challenges

- Read about Web App Exploitation and Security Vulnerabilities at: https://ctfacademy.github.io/web/index.htm#WebAppExploitation
- Complete 3 Challenges (take Capture completed screenshots**):**
  + https://ctfacademy.github.io/web/challenge1/index.htm
  + https://ctfacademy.github.io/web/challenge2/index.htm
  + https://ctfacademy.github.io/web/challenge3/index.htm