Lab 6 - Playing with XSS

Submission

You need to write a report which includes:

1. A concise description of your findings for each task.
2. Answers to all questions given in the tasks.
3. The Python scripts you write to accomplish the tasks (if any).
4. **Screen captures** to support your findings.

Submission requirement

1. Use Markdown to write your report; a report template will be provided by the instructor.

2. You can use your favorite Markdown editor. However, if you never used Markdown before, there are two recommended ones:

   1. https://marxi.co/ - A browser app
   2. https://typora.io/ - A cross-platform desktop MD editor

3. In your report, all codes should be placed in code blocks/fences. For example:

   ```
   def somefunc(param1='', param2=0):
       '''A docstring'''
       if param1 > param2: # interesting
           print 'Greater'
       return (param2 - param1 + 1) or None
   ```

4. Do not submit the MD file; instead, export as **pdf** for submission.

Objective

Cross-site scripting (XSS) is a type of vulnerability commonly found in web applications. This vulnerability makes it possible for attackers to inject malicious code (e.g. JavaScript programs) into victim's web browser. Using this malicious code, the attackers can steal the victim's credentials, such as session cookies. The access control policies (i.e., the same origin policy) employed by browsers to protect those credentials can be bypassed by exploiting the XSS vulnerability. Vulnerabilities of this kind can potentially lead to large-scale attacks.

Drills

Tasks

In this lab, you need to complete the **six** XSS challenge hosted at https://xss-game.appspot.com/.

- For each challenge, you need to Inject a script to pop up a JavaScript `alert('xxx')` in the frame; you need to replace `xxx` with a unique string you come up with throughout this lab.
- There are solutions you can find online. You are allowed to read those solutions and get some ideas.
- For **each challenge**, you need to submit:

  1. The attacking payload in a code block.

2. A paragraph that explains how the attack works (**should be in your own words! do not copy and paste any online material**).
3. Screenshots of a successful attack.