Cross-Site Scripting (XSS) Teacher Workout Instructions

Introduction

The goal of this workout is to teach students how to perform multiple types of cross-site scripting (XSS) attacks on a web server. There are three different types of XSS attacks to explore: DOM-based reflected and stored cross-site scripting. Students can choose any of the three to work on first.

DOM-Based XSS

In the DOM-Based XSS section, the student is tasked to change the title of the webpage and create an alert box using the URL of the webpage and JavaScript. The students must use the bad_request variable that they are given as part of their instructions. The URL path will look similar to **https://cybergym-classified-v7k2apwaqa-uc.a.run.app/workouts/xss/<workout_id>?bad_request=<script>JScode</script>** The ? acts as a separator for the URL resource path and query parameters.

To update the title of the HTML page to “Classified DOMED” the students must run the script inside the URL

```
<script>document.title="Classified DOMED";</script>
```

To prompt the message, “Successful DOM-Based Attack” the students must run the script inside the URL

```
<script>alert("Successful DOM-Based Attack");</script>
```

Reflected XSS

In the Reflected XSS section, the student is tasked to change the CSS for ‘Hello, Stranger’ to their favorite color and navigate to another site like https://www.google.com/. The students must use the text field to inject their JavaScript.

To change the color for ‘Hello, Stranger’ the student must identify the ID for the header and run the script inside the text field

```
<script>document.getElementById("stranger").style.color =
"FAVORITECOLOR";</script>
```

To navigate to another site the student must run the script inside the text field

```
 <script>window.location.replace("URL-TO-SITE");</script>
```

Stored XSS

In the Stored XSS section, the student is tasked to prompt a calculation for (23*5-4+3+57/27-42). Any script that is injected in this section is persistent and will be present when the student reloads the page.

To prompt a calculation for (23*5-4+3+57/27-42) the student must run the script inside the feedback text field

```
<script>alert(23*5-4+3+57/27-42);</script>
```

Exploration

The student is encouraged to explore the XSS sections using different scripts after the completion of tasks. These can be found on the internet or written themselves!