**Batch: B1 Roll No.: 16010121045**

**Experiment No. 5**

|  |
| --- |
| **Title:**  XSS using DVWA |

**Objective:** Introduction to Open Web Application Security Project and implementation

of XSS.

**Expected Outcome of Experiment: To implement Cryptanalysis Tools .**

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO3** | Explore Kali Linux Security and Forensics Tools |

**Books/ Journals/ Websites referred:**

[**http://www.dvwa.co.uk/**](http://www.dvwa.co.uk/)

[**https://ensurtec.com/dvwa-part-2-exploiting-cross-site-scripting-xss-vulnerabilities/**](https://ensurtec.com/dvwa-part-2-exploiting-cross-site-scripting-xss-vulnerabilities/)

[**https://www.computersecuritystudent.com/SECURITY\_TOOLS/DVWA/DVWAv107/lesson9/index.html**](https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson9/index.html)

[**https://pentest-tools.com/blog/xss-attacks-practical-scenarios**](https://pentest-tools.com/blog/xss-attacks-practical-scenarios)

**Abstract**:-

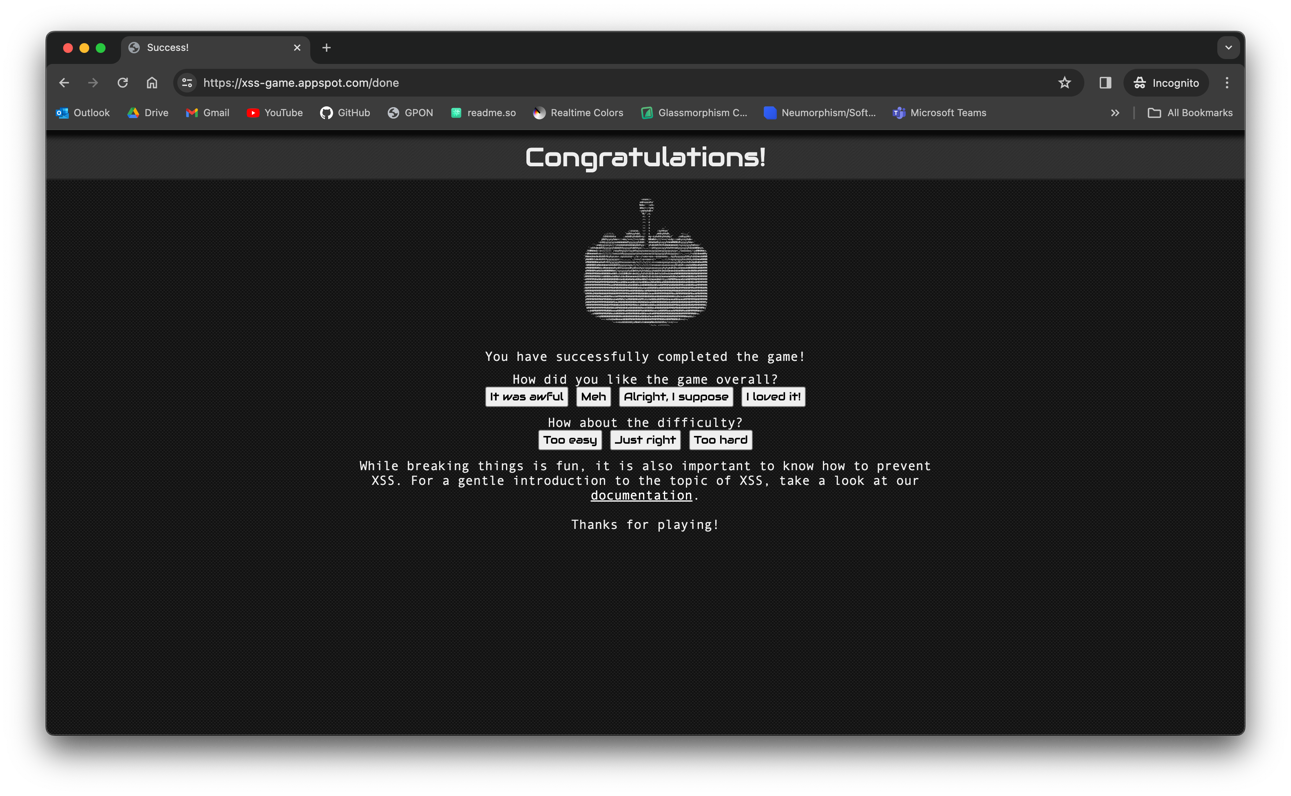
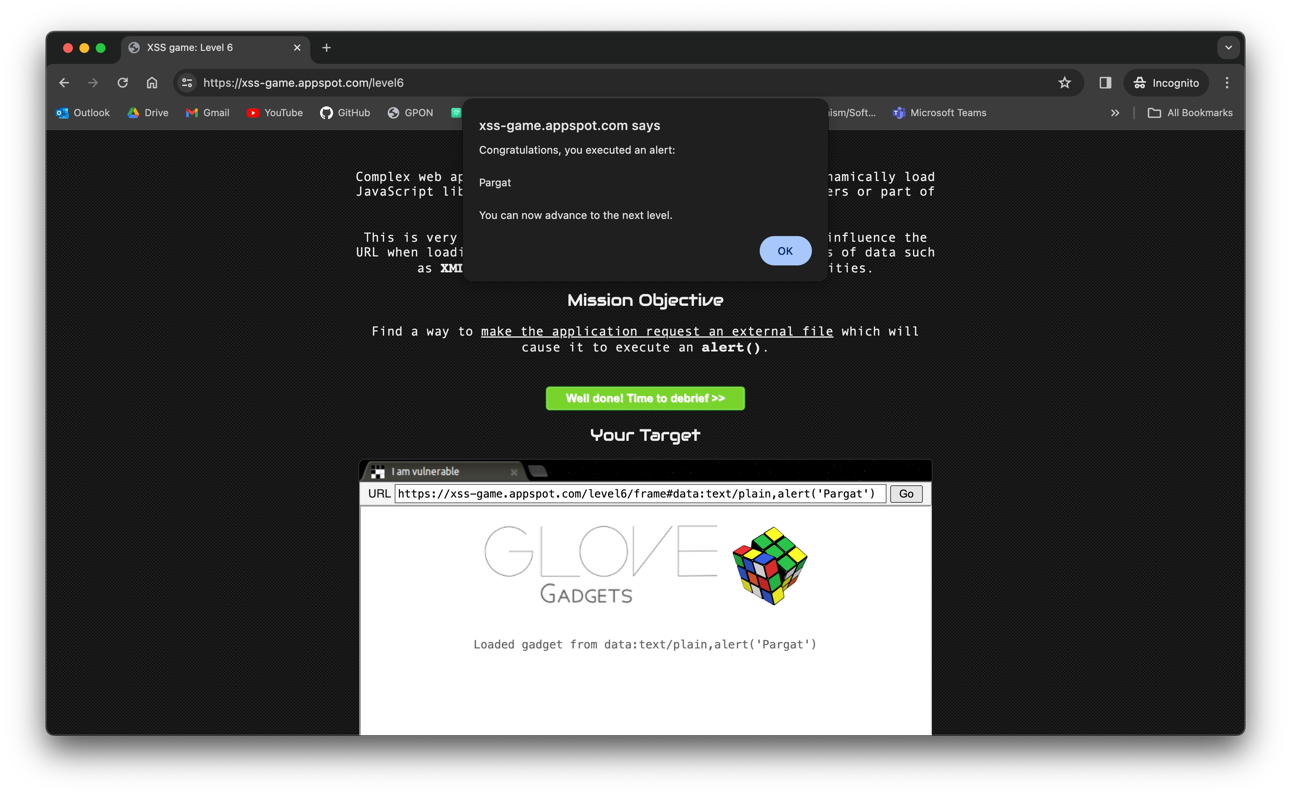
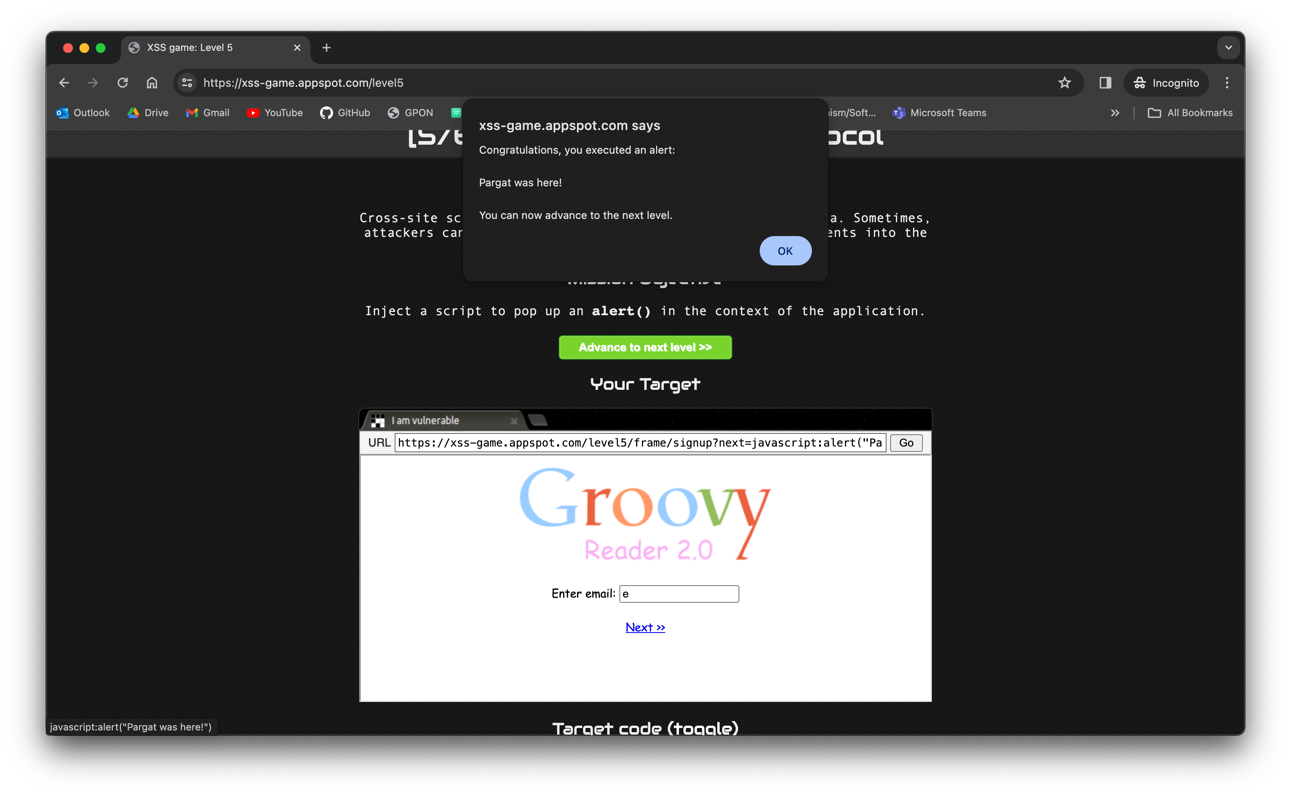
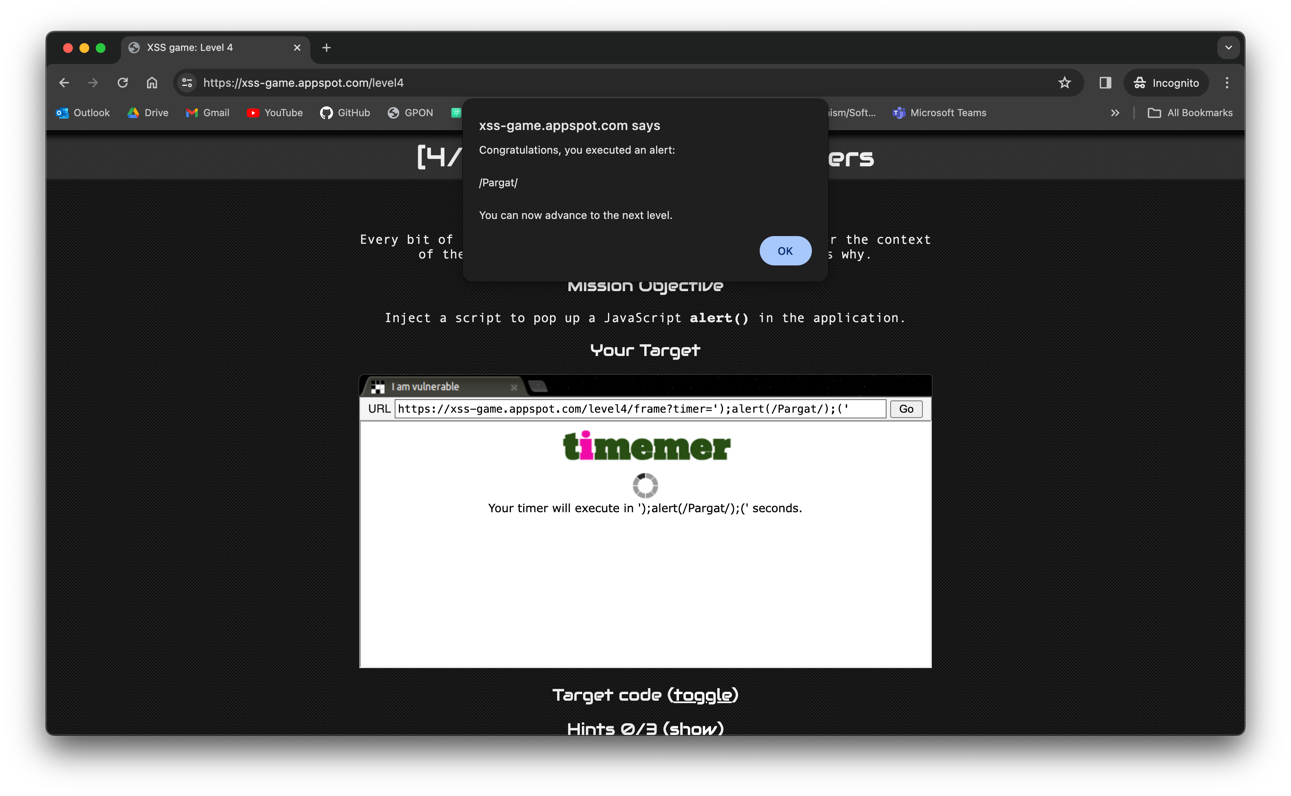
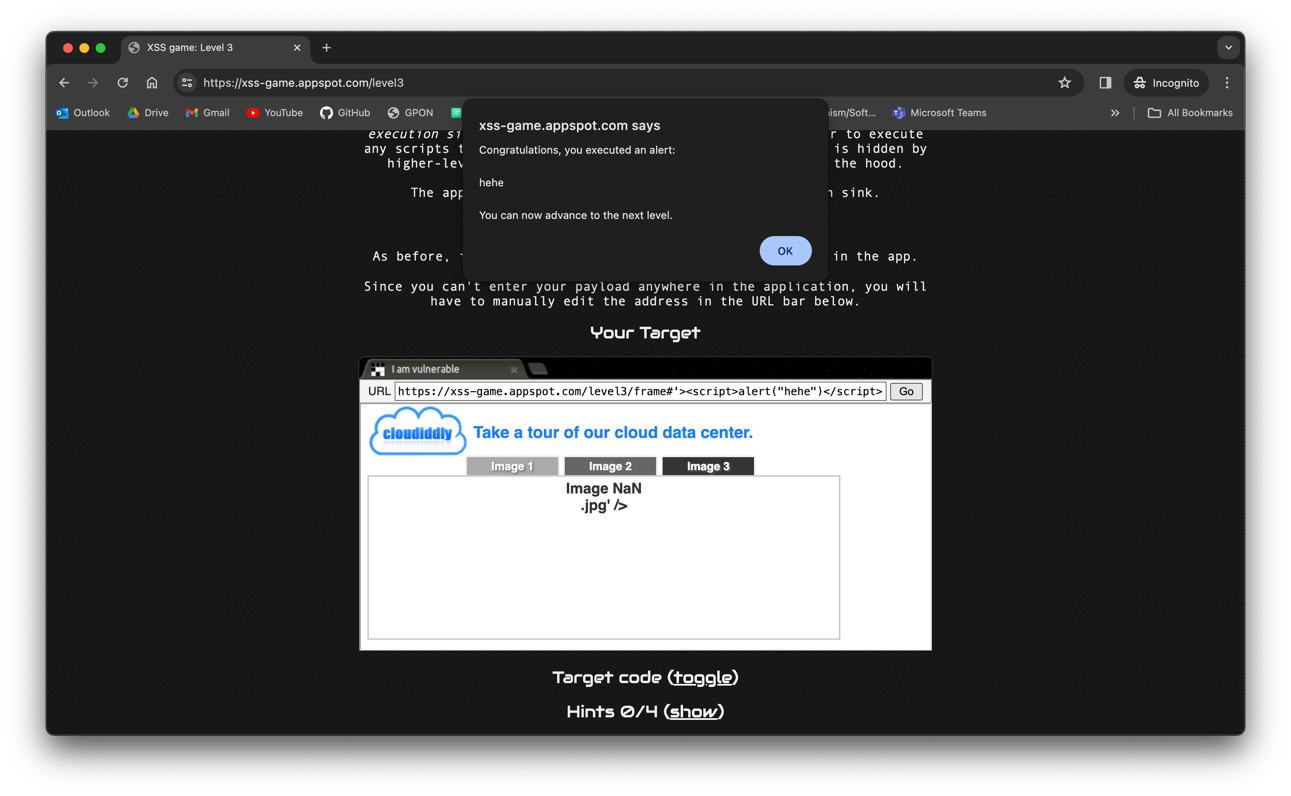
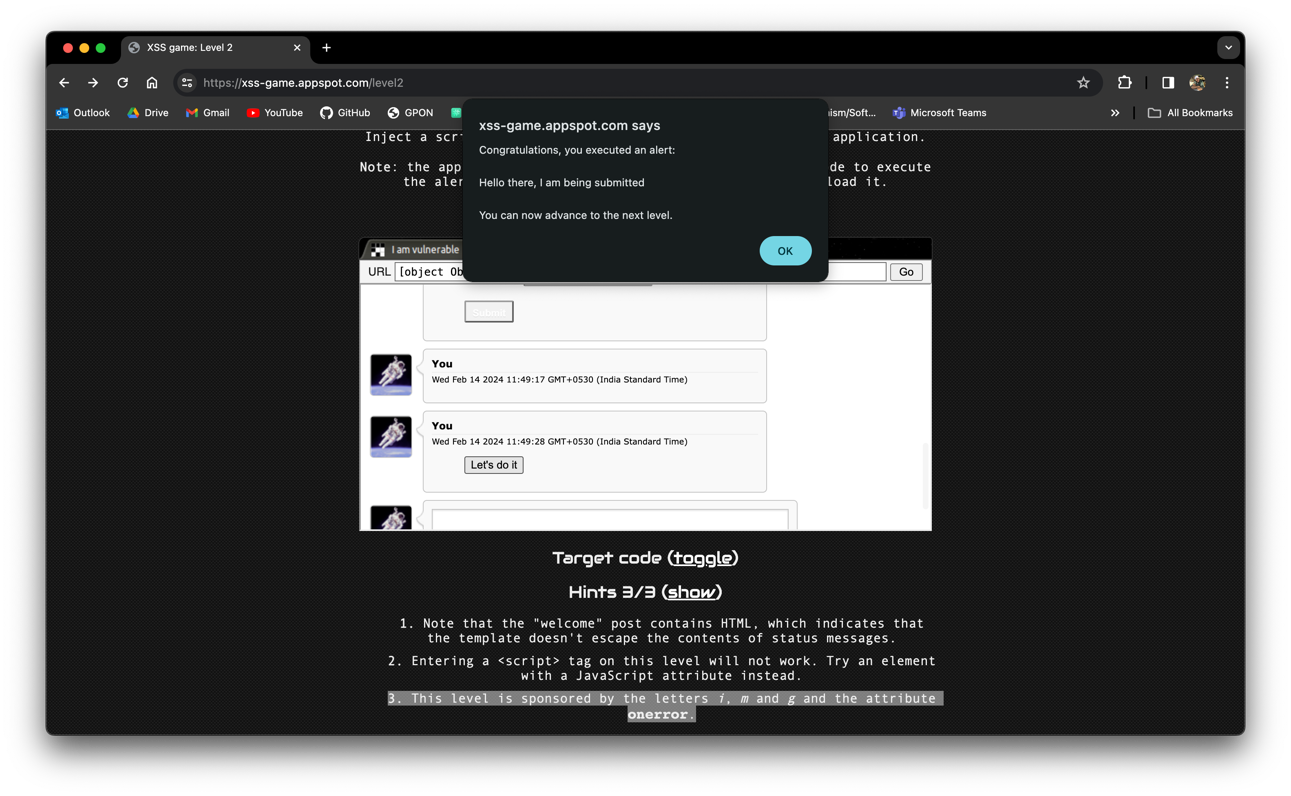
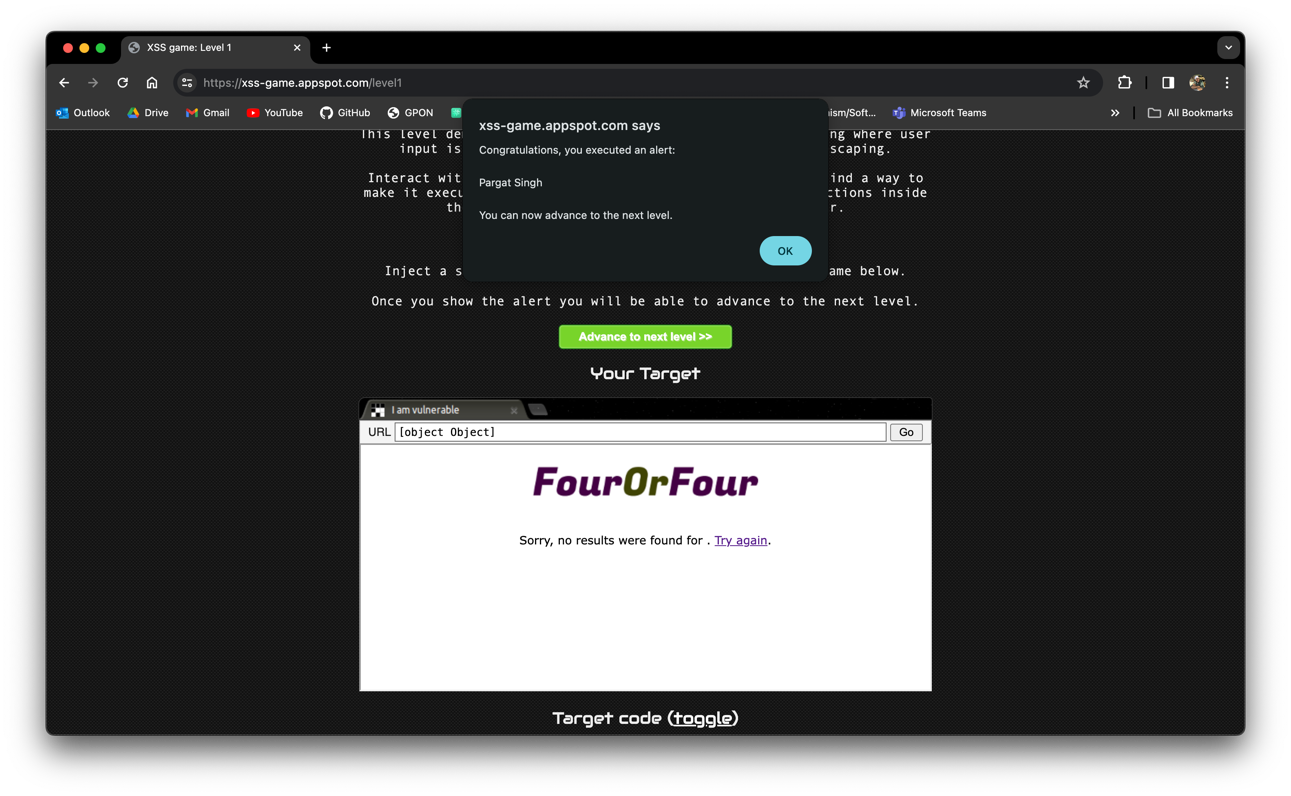
Web application security is a crucial aspect of ensuring the integrity, confidentiality, and availability of web-based systems. It involves protecting web applications from various cyber threats and vulnerabilities that could compromise sensitive data or disrupt services. One of the most prevalent threats to web application security is Cross-Site Scripting (XSS), a type of attack that allows malicious actors to inject and execute scripts within web pages viewed by other users. This paper explores the concept of web application security, focusing on XSS attacks, and discusses countermeasures to mitigate both XSS and other common attacks.

**Related Theory: -**

1. **Various Attacks on Web Application Security:** Web applications are susceptible to a wide range of attacks, including injection attacks (such as SQL injection and Command injection), cross-site request forgery (CSRF), cross-site scripting (XSS), session fixation, and more. These attacks exploit vulnerabilities in the application's code, input validation, authentication mechanisms, or session management.
2. **XSS Attacks:** XSS attacks occur when an attacker injects malicious scripts (usually JavaScript) into web pages viewed by other users. There are three main types of XSS attacks:
   * **Stored XSS:** Malicious scripts are stored on the server and executed when a user accesses the vulnerable page.
   * **Reflected XSS:** Malicious scripts are reflected off a web server and executed in the context of the victim's browser.
   * **DOM-based XSS:** Malicious scripts manipulate the Document Object Model (DOM) of a web page, leading to script execution in the victim's browser.
3. **Countermeasures for Web Application Security:**
   * **Input Validation:** Validate and sanitize all user input to prevent injection attacks.
   * **Parameterized Queries:** Use parameterized queries or prepared statements to prevent SQL injection attacks.
   * **Output Encoding:** Encode output data to prevent XSS attacks by converting potentially dangerous characters into their HTML entity equivalents.
   * **Content Security Policy (CSP):** Implement CSP headers to restrict the execution of scripts and mitigate XSS vulnerabilities.
   * **Session Management:** Use secure session management practices, such as session tokens with sufficient entropy, secure cookie attributes, and session expiration.
   * **Regular Security Audits:** Conduct regular security audits and penetration testing to identify and remediate vulnerabilities in web applications.

**Implementation**

<https://xss-game.appspot.com/>

****

**DVWA**

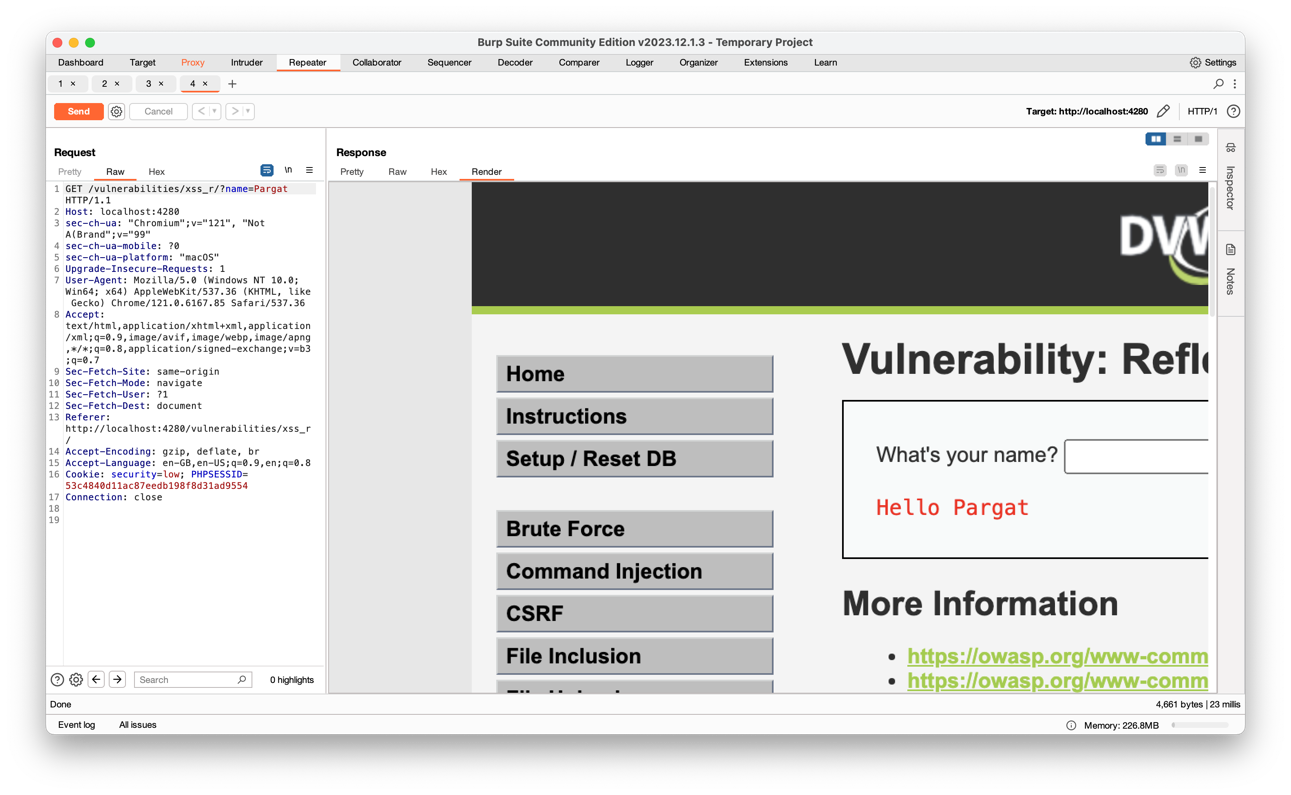
**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**DVWA Blind**

****

**A screenshot of a computer

Description automatically generated**

**Conclusion:-** Completed introduction to Open Web Application Security Project and implementation of XSS.

**Postlab Questions:**

5.1 **What is OWASP? List the latest web security application risks by OWASP.**

* OWASP is the Open Web Application Security Project, a community-driven organization dedicated to improving web application security. The latest web security application risks by OWASP, often referred to as the OWASP Top 10, include vulnerabilities such as Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, and Insufficient Logging & Monitoring.

5.2 **Explain countermeasures for injection attacks.**

* Countermeasures for injection attacks involve implementing input validation and using parameterized queries or prepared statements to prevent attackers from injecting malicious code into application inputs. Additionally, enforcing proper authentication and authorization mechanisms can help mitigate injection vulnerabilities.

5.3 **List the types of XSS attacks.**

* The types of XSS attacks are:
  + Stored XSS
  + Reflected XSS
  + DOM-based XSS

Top of Form

Bottom of Form