**Lab 5- Conducting a Cross Site Scripting (XXS) Attack**

**What Was Learned:**This lab focused on identifying and exploiting Cross-Site Scripting (XSS) vulnerabilities in web applications. Participants learned how XSS works, how to identify it in web applications, and how attackers can exploit such vulnerabilities to execute malicious scripts.

**Key Learnings:**

1. **Understanding XSS:**
   * XSS is a prevalent vulnerability in web applications caused by improper validation of user inputs, allowing attackers to inject and execute malicious scripts.
   * Highlighted XSS as one of the top vulnerabilities in the OWASP Top Ten.
2. **Tools and Setup:**
   * Used the XSS Game (<https://xss-game.appspot.com>) for practical, hands-on experience.
   * Explored different levels of XSS challenges, ranging from basic to advanced.
3. **Detecting Vulnerabilities:**
   * Entered basic HTML input (e.g., <h1>Header here</h1>) in a search box to confirm the website reflects user input without sanitization.
   * Determined the application was vulnerable to XSS when it displayed the input directly in the output without any encoding or validation.
4. **Executing Basic XSS:**
   * Injected JavaScript, such as <script>alert('1')</script>, to execute an XSS attack.
   * Observed a pop-up alert as proof of successful execution of malicious script.
5. **Persistent XSS Attack:**
   * Learned about persistent (or stored) XSS attacks through a forum example on Level 2 of the XSS Game.

Injected a script tag that loads an image with an error handler to trigger the malicious script every time the page is visited:  
html  
Copy code  
<img src="nonexistent.jpg" onerror="alert('Persistent XSS')">

* + Realized the persistent XSS attack’s potential to continuously affect all visitors to the vulnerable page.

1. **Advancing Understanding:**
   * Encouraged to proceed through higher levels of the XSS Game to explore more complex scenarios.
   * Emphasized the need to understand JavaScript and HTML to craft more sophisticated XSS payloads.

**Takeaways:**

* **Identification of XSS Vulnerabilities:** Recognized how unsanitized user inputs can lead to XSS vulnerabilities.
* **Execution of XSS Attacks:** Gained hands-on experience in injecting and executing XSS payloads to exploit vulnerabilities.
* **Significance of Persistent XSS:** Understood how persistent XSS can have a far-reaching impact by embedding malicious scripts into webpages visited by multiple users.
* **Ethical Considerations:** Reinforced the importance of responsibly reporting XSS vulnerabilities to web application owners and adhering to ethical hacking principles.
* **Defensive Measures:** Highlighted the necessity of input validation, output encoding, and content security policies to prevent XSS attacks.

This lab provided valuable insight into one of the most common web vulnerabilities and the methods attackers use to exploit it, emphasizing the importance of secure web development practices.