Security Assessment Report

Vulnerability Type: Reflected Cross-Site Scripting (XSS)
Target: PortSwigger Academy Lab – Reflected XSS into HTML context
Assessor: Abdelalim Saada
Tools Used: Firefox Developer Tools, Burp Suite (optional), PortSwigger Academy

1. Vulnerability Description

Reflected Cross-Site Scripting (XSS) occurs when user input is immediately echoed in the response page without proper encoding or sanitization, allowing attackers to inject malicious JavaScript into the client's browser.

In this lab, the search parameter was vulnerable. The input from the user was reflected back into the HTML response inside a `<h4>` tag without proper encoding.

2. Steps to Reproduce

1. **Access the lab**:
    - Open the PortSwigger lab: *Reflected XSS into HTML context with nothing encoded*
2. **Test harmless HTML**:
    - Input tested:
    - `<h4>test</h4>`
    - Observed that the text was rendered as an actual HTML header. This indicates the input was not encoded.
3. **Inject JavaScript payload**:
    - Final payload:
    - `<script>alert(1)</script>`
    - This triggered a JavaScript `alert(1)` popup, confirming execution.
4. **Captured Screenshot**:
    - Screenshot shows:
        - Input in search bar
        - Response rendering unescaped input
        - Alert popup

3. Root Cause

- The application fails to **sanitize or encode** user-supplied input before reflecting it into the HTML response.
- The reflected content is injected **directly into the HTML context**, allowing script execution.

4. Risk Assessment

Category	Details
Impact	High – Can lead to session hijacking, phishing
Likelihood	High – No filtering or sanitization applied
OWASP	A03:2021 – Injection (XSS)

5. Mitigation Recommendations

1. **Contextual Output Encoding**
   Use libraries like:
   - `OWASP Java Encoder`
   - `React's dangerouslySetInnerHTML` should be avoided
2. **Input Validation (optional)**
   - Reject unnecessary HTML/script input on the client and server side.
3. **Use Content Security Policy (CSP)**
   - Prevent inline script execution:
   - `Content-Security-Policy: script-src 'self';`
4. **Avoid reflecting user input directly into HTML without sanitization**

6. OWASP Mapping

OWASP Top 10	Vulnerability Type	Found
A03:2021	Injection (XSS)	☑ Yes