Ethical Hacking Internship – Task 2 Report

# Vulnerability Report – Reflected XSS

Title:  
Reflected Cross-Site Scripting (XSS) in `search.asp` on testasp.vulnweb.com

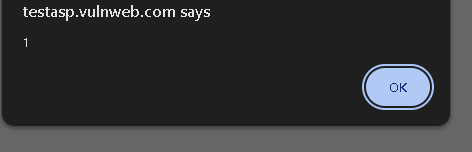
Summary:  
The search endpoint reflects user input without proper sanitization or encoding, allowing an attacker to inject arbitrary JavaScript. This leads to a Reflected XSS vulnerability.

Affected URL:  
http://testasp.vulnweb.com/search.asp?query=<script>alert(1)</script>

Steps to Reproduce:  
1. Open your browser and navigate to:  
 http://testasp.vulnweb.com/search.asp?query=<script>alert(1)</script>  
2. An alert dialog (alert(1)) appears, confirming the XSS vulnerability.  
3. The site then proceeds to render the page content.

Impact  
- Attacker can execute arbitrary JavaScript in the user’s browser.  
- Can be used for session hijacking, phishing, or browser-based attacks.  
- Affects all users clicking maliciously crafted links.

Screenshot:



# Vulnerability Report – SQL Injection

**Title:**  
SQL Injection in id parameter on showforum.asp – testasp.vulnweb.com

**Summary:**  
The id parameter in the showforum.asp page is vulnerable to SQL Injection. Unsanitized user input is directly included in backend SQL queries, allowing attackers to break query logic and interact with the database.

**Affected URL**

http://testasp.vulnweb.com/showforum.asp?id=1'

**Steps to Reproduce:**

1. Navigate to:

http://testasp.vulnweb.com/showforum.asp?id=1

1. Append a single quote ' to the URL:

http://testasp.vulnweb.com/showforum.asp?id=1'

1. The server responds with:

500 - Internal Server Error

indicating that the SQL query was broken by the input.

1. This proves that the input is **not properly sanitized**, and the application is vulnerable to injection.

**Impact:**

* Attackers may extract or manipulate database contents.
* Risk of login bypass, data leakage, or privilege escalation.
* Can lead to full database compromise if exploited further.