Vulnerability Assessment Report

Security Testing on testasp.vulnweb.com

Presented by: Akshay Bagul

Introduction

What is Vulnerability Assessment?

Vulnerability assessment is the process of identifying, classifying, and reporting security weaknesses in a system or network. It involves a systematic examination of potential vulnerabilities that could be exploited by attackers. The assessment aims to provide a comprehensive overview of the security posture, enabling organizations to prioritize remediation efforts and reduce their overall risk.

Objective

The primary objective is to test testasp.vulnweb.com for security flaws and vulnerabilities. This involves simulating real-world attack scenarios to uncover weaknesses in the application's security controls. The goal is to identify potential entry points for attackers and assess the effectiveness of existing security measures in preventing unauthorized access and data breaches.

Goal

The ultimate goal is to document findings in a clear and concise report, providing actionable recommendations for remediation. This includes detailing the identified vulnerabilities, their potential impact, and the steps required to mitigate the associated risks. The report serves as a valuable resource for developers and security teams, enabling them to prioritize and address the most critical security issues effectively.

Testing Methodology

1

Information Gathering

Website structure and endpoints.

2

Manual Testing

Common attack payloads.

3

Automated Scanning

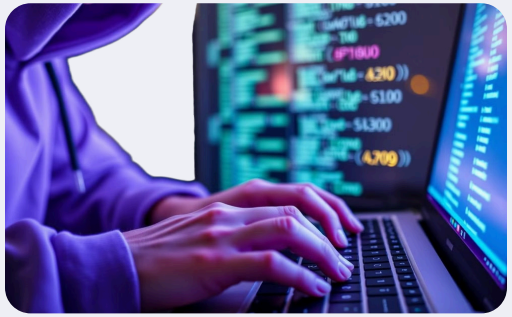
Tools like Acunetix and Burp Suite.

4

Reporting

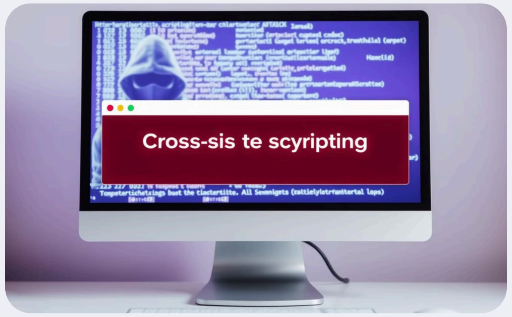
Documenting findings.

Findings Overview



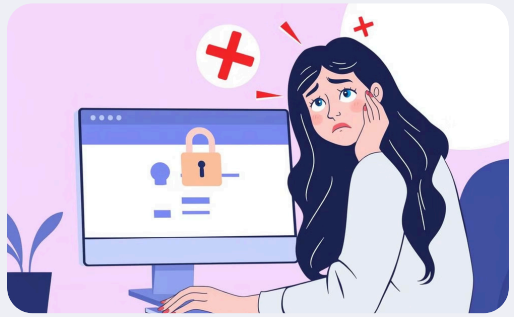
SQL Injection

Severity: High. Confirmed.



Cross-Site Scripting (XSS)

Severity: High. Confirmed.

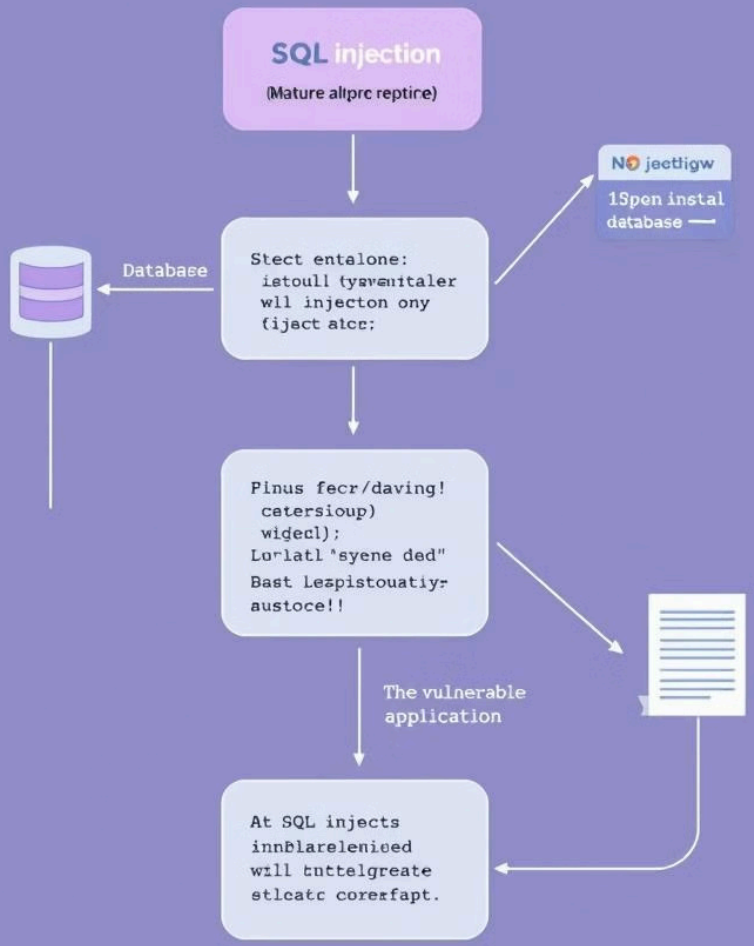


Insecure Direct Object References (IDOR)

Severity: Medium. Confirmed.

Security Misconfigurations

Severity: Low. Confirmed.



SQL Injection (SQLi) - Critical

1 Description

Manipulate database with malicious SQL queries.

2 Impact

Attackers can extract database information.

3 Recommendation

Use prepared statements.

Navigate to the login page: http://testasp.vulnweb.com/Login.asp

Enter **1' OR '1'='1** as both the username and password.

Reflected XSS (Cross-Site Scripting) - High

Description

Inject malicious JavaScript into a webpage.

Impact

Attackers can steal user cookies.

Recommendation

Implement proper input encoding.

Navigate to the search page: http://testasp.vulnweb.com/Search.asp?tfSearch=

Insecure Direct Object Reference (IDOR) - Medium

Description

Access restricted data by manipulating URL parameters.

Impact

Unauthorized access to restricted forum threads.

Recommendation

Implement proper access controls.

Access this URL: http://testasp.vulnweb.com/showthread.asp?id=10

Security Misconfigurations - Low

Findings 1

Website is not using HTTPS.

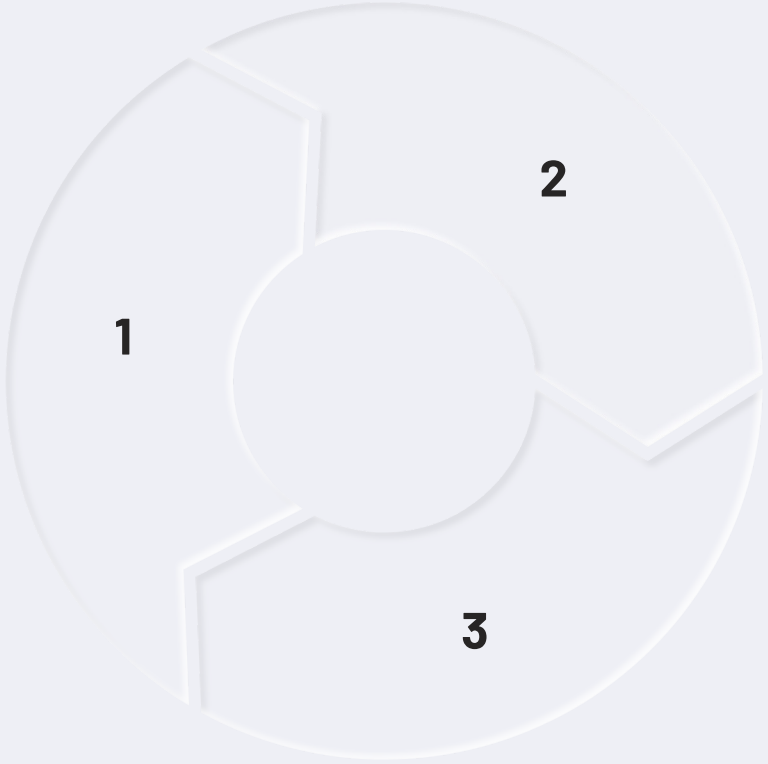
2 **Impact**

Attackers can intercept login credentials.

Recommendation 3

Enable HTTPS using an SSL certificate.

Conclusion & Recommendations



High-risk vulnerabilities

Data breaches

Account takeovers

Fix SQL Injection using parameterized queries.

Mitigate XSS with proper input encoding.