Vulnerability Assessment Report

1. Introduction

A Vulnerability Assessment (VA) is a systematic process of identifying, analyzing, and prioritizing security weaknesses in systems, networks, or applications. The goal of this assessment is to detect vulnerabilities before attackers can exploit them and to recommend appropriate mitigation strategies to reduce risk.

---

2. Scope of Assessment

The scope of this vulnerability assessment included:

* Web application security
* Server and system configuration
* Input validation and authentication mechanisms
* Common OWASP Top 10 vulnerabilities

Assessment Type:

* Manual Testing
* Automated Scanning
* Limited Exploitation (Non-destructive)

---

3. Tools Used

* **Burp Suite** – Web application testing
* **Nmap** – Network and port scanning
* **Nikto** – Web server vulnerability scanning

* **OWASP ZAP** – Automated vulnerability detection
* **DVWA / OWASP Juice Shop** – Test environment

---

4. Methodology

The assessment followed a structured approach:

1. **Information Gathering**

   * Identified target services and technologies
   * Mapped application endpoints

2. **Scanning**

   * Performed automated vulnerability scans
   * Identified potential weaknesses

3. **Vulnerability Analysis**

   * Validated findings manually
   * Removed false positives

4. **Risk Assessment**

   * Evaluated impact and likelihood
   * Assigned severity levels

5. **Reporting**

   * Documented vulnerabilities and mitigations

---

5. Identified Vulnerabilities

5.1 SQL Injection (SQLi)

Description:
Improper input validation allowed malicious SQL queries to be executed.

Impact:

* Authentication bypass
* Unauthorized database access

Risk Level: High

5.2 Cross-Site Scripting (XSS)

Description:
User input was reflected or stored without proper output encoding.

Impact:

* Session hijacking
* Credential theft

Risk Level: Medium to High

5.3 Security Misconfiguration

Description:
Default settings and verbose error messages were enabled.

Impact:

* Information disclosure
* Easier exploitation

Risk Level: Medium

5.4 Broken Authentication

Description:
Weak password policies and missing account lockout mechanisms were obser ved.

Impact:

* Credential stuffing attacks
* Account compromise

Risk Level: High

---

6. Vulnerability Summary Table

Vulnerability	Severity	Affected Area	Potential Impact
SQL Injection	High	Login / Input Fields	Data breach

Stored XSS	High	User Content	Persistent attack
Reflected XSS	Medium	URL Parameters	Session theft
Security Misconfiguration	Medium	Server	Info disclosure
Weak Authentication	High	Login System	Account takeover

---

7. Risk Analysis

* **High-risk vulnerabilities** could lead to complete system compromise.
* **Medium-risk vulnerabilities** increase attack surface and assist attackers.
* **Low-risk issues** may still contribute to chained attacks.

Risk prioritization is essential for effective remediation.

---

8. Recommended Mitigations

8.1 Input Validation & Injection Prevention

* Use parameterized queries
* Implement server-side validation
* Sanitize all user inputs

8.2 XSS Protection

* Apply output encoding
* Implement Content Security Policy (CSP)
* Use HTTPOnly and Secure cookies

8.3 Authentication Security

* Enforce strong password policies
* Implement MFA
* Add account lockout and rate limiting

8.4 Configuration Hardening

* Disable unnecessary services
* Remove default credentials
* Hide detailed error messages

---

9. Result

The vulnerability assessment successfully identified multiple security weaknesses within the tested environment. Several high-risk vulnerabilities were found that could be exploited to compromise sensitive data and system integrity if left unpatched.