Functional and Performance Testing Documentation

This document outlines the results of the vulnerability assessment and performance testing conducted on the target applications. It is divided into two main stages: the Vulnerability Assessment Report and the Nessus Vulnerability Scanner Overview, followed by a sample vulnerability report.

Stage 1: Vulnerability Assessment Report

Target Website: http://www.itsecgames.com/

Vulnerability Overview Table

Sr. No	Vulnerability Type	CWE ID
1	Insecure Direct Object References (IDOR)	CWE-639
2	Cross-Site Request Forgery (CSRF)	CWE-352
3	Improper Security Configuration	CWE-16
4	Unchecked URL Redirects and Forwards	CWE-601
5	XML External Entity (XXE) Vulnerability	CWE-611

Detailed Vulnerability Reports

1. **Insecure Direct Object References (IDOR)**
    - **CWE:** CWE-639
    - **Category:** Broken Access Control (OWASP/SANS A01:2021)
    - **Overview:**
      The application is vulnerable to IDOR flaws, allowing attackers to modify URL parameters (e.g., altering account_id values) to access unauthorized data.
    - **Business Impact:**
        - Exposure of confidential user data.
        - Unauthorized modifications to records.
        - Privacy violations.
    - **Method of Discovery:**
        - Intercepted HTTP traffic using Burp Suite.
        - Manually altered identifier parameters.
        - Verified unauthorized access via response validation.
2. **Cross-Site Request Forgery (CSRF)**
    - **CWE:** CWE-352

- **Category:** Software and Data Integrity Failures (OWASP/SANS A08:2021)
- **Overview:**
  The lack of proper CSRF protections allows attackers to trick users into submitting unauthorized actions, such as changing passwords.
- **Business Impact:**
  - Unauthorized user account modifications.
  - Loss of account control.
  - Financial fraud risks.
- **Method of Discovery:**
  - Crafted a fake HTML form to simulate a password change.
  - Induced a logged-in user to submit the form.
  - Confirmed execution without proper CSRF tokens.

3. **Security Misconfiguration**
   - **CWE:** CWE-16
   - **Category:** Security Misconfiguration (OWASP/SANS A05:2021)
   - **Overview:**
     The system uses default credentials, enabled debug modes, and exposes sensitive configuration files.
   - **Business Impact:**
     - Increased attack surface.
     - Leakage of internal system details.
     - Risk of unauthorized administrative access.
   - **Method of Discovery:**
     - Tested with default credentials (e.g., bee/bug).
     - Identified exposed files (e.g., phpinfo.php).
     - Discovered backup files using brute-force directory scanning.
4. **Unchecked URL Redirects and Forwards**
   - **CWE:** CWE-601
   - **Category:** Server-Side Request Forgery (SSRF) (OWASP/SANS A10:2021)
   - **Overview:**
     Weak redirect mechanisms enable attackers to construct malicious URLs, redirecting users to fraudulent sites.
   - **Business Impact:**

        - Increased risk of phishing.
        - Credential theft.
        - Erosion of customer trust.
    - **Method of Discovery:**
        - Modified URL parameters on a known redirect endpoint.
        - Confirmed lack of validation on redirection targets.

5. **XML External Entity (XXE) Vulnerability**
    - **CWE:** CWE-611
    - **Category:** Insecure Design (OWASP/SANS A04:2021)
    - **Overview:**
      Improper XML processing allows attackers to execute SSRF attacks, access local files, or cause a denial-of-service.
    - **Business Impact:**
        - Exposure of sensitive files (e.g., system password files).
        - Potential SSRF attacks.
        - Increased risk of application crashes.
    - **Method of Discovery:**
        - Located the XML processing endpoint (e.g., redirect.php?url=).
        - Injected a crafted XML payload with an external entity.
        - Observed data extraction confirming the vulnerability.

Target Website: https://owasp.org/www-project-juice-shop/

Vulnerability Overview Table

S.No	Vulnerability Type	CWE ID
1	Cross-Site Scripting (XSS)	CWE-79
2	Cross-Site Request Forgery (CSRF)	CWE-352
3	Insecure Direct Object References (IDOR)	CWE-639
4	SQL Injection	CWE-89
5	Broken Authentication	CWE-287

Detailed Vulnerability Reports

1. **Cross-Site Scripting (XSS)**

- **CWE:** CWE-79
- **Category:** Injection
- **Overview:**
  The application is vulnerable to XSS due to unsanitized user input in the search functionality, allowing execution of malicious scripts.
- **Method of Discovery:**
  - Injected sample script payloads into search fields.
  - Monitored reflected output for script execution.
- **Business Impact:**
  - Unauthorized session access.
  - Theft of sensitive user data.
  - Reputational damage due to site defacement.

2. **Cross-Site Request Forgery (CSRF)**
   - **CWE:** CWE-352
   - **Category:** CSRF
   - **Overview:**
     Insufficient CSRF protections enable attackers to perform unintended actions on behalf of authenticated users.
   - **Method of Discovery:**
     - Generated crafted attack vectors.
     - Verified that actions occurred without proper verification.
   - **Business Impact:**
     - Unauthorized transactions.
     - Modification of user data.
     - Potential financial loss.
3. **Insecure Direct Object References (IDOR)**
   - **CWE:** CWE-639
   - **Category:** Authorization
   - **Overview:**
     Manipulating object identifiers in requests allows attackers to access data that should remain restricted.
   - **Method of Discovery:**
     - Altered URL parameters to test unauthorized data access.

        - Confirmed access to restricted resources.
    - **Business Impact:**
        - Exposure of confidential information.
        - Data integrity issues.
        - Regulatory compliance risks.

4. **SQL Injection**
    - **CWE:** CWE-89
    - **Category:** Injection
    - **Overview:**
      Input fields, especially in the login process, are susceptible to SQL injection, enabling manipulation of database queries.
    - **Method of Discovery:**
        - Entered malicious SQL commands in input fields.
        - Analyzed database error responses.
    - **Business Impact:**
        - Unauthorized database access.
        - Potential data corruption or loss.
        - Severe financial and reputational damage.

5. **Broken Authentication**
    - **CWE:** CWE-287
    - **Category:** Authentication
    - **Overview:**
      Weak authentication and session management allow attackers to bypass security controls and impersonate users.
    - **Method of Discovery:**
        - Tested login with weak credentials.
        - Exploited session management vulnerabilities.
    - **Business Impact:**
        - Unauthorized account access.
        - Compromise of sensitive user data.
        - Loss of customer trust and legal liabilities.

Stage 2: Nessus Vulnerability Scanner Overview

Overview

Nessus is a leading vulnerability scanner designed to systematically detect weaknesses across networks, applications, and configurations. It plays a critical role in proactive cybersecurity by simulating real-world attacks and providing detailed vulnerability reports.

Key Features

- **Automated Deep Scanning:**
  Performs comprehensive scans to detect misconfigurations, outdated software, and known vulnerabilities.
- **Compliance Auditing:**
  Supports standards such as PCI DSS, HIPAA, and ISO 27001, ensuring regulatory compliance.
- **Plugin-Driven Detection:**
  Leverages an extensive library of plugins to stay current with emerging threats.
- **Configuration Analysis:**
  Evaluates system settings to identify exploitable areas.
- **SIEM Integration:**
  Seamlessly integrates with SIEM solutions to enhance incident response and threat intelligence.

Role in Cybersecurity

Organizations use Nessus for:

- Regular security assessments.
- Prioritizing vulnerabilities for remediation.
- Informing patch management and system hardening decisions.
- Generating detailed compliance and penetration testing reports.

Sample Vulnerability Report: Cross-Site Scripting (XSS)

Vulnerability: Cross-Site Scripting (XSS)

- **Severity:** High
- **Scanning Tool:** OWASP ZAP (Zed Attack Proxy)
- **Tested Port:** 80 (HTTP)

Description

The target web application demonstrates a significant XSS vulnerability within its search functionality. Due to improper sanitization of user input, attackers can inject malicious scripts that execute in the context of other users' browsers. This can lead to unauthorized session access and data theft.

Mitigation Strategies

- **Input Validation:**
  Enforce strict input validation and output encoding to neutralize malicious scripts.
- **Content Security Policy (CSP):**
  Implement CSP headers to restrict the execution of untrusted code.
- **Regular Updates:**
  Continuously update and patch the application to address known vulnerabilities.

Business Impact

- **Data Theft:**
  Unauthorized access to user sessions can result in the exposure of sensitive information.
- **Reputation Damage:**
  Website defacement and compromised user trust can harm brand image.
- **Legal Risks:**
  Non-compliance with data protection regulations may lead to severe legal penalties.

This documentation provides a comprehensive overview of the vulnerability assessment and performance testing conducted for the cybersecurity project, covering detailed vulnerability reports for two target websites, an in-depth overview of the Nessus scanner, and a sample XSS vulnerability report.

Cite: