Vulnerability Assessment Report

Name: Raj Talukder

Date: April 08, 2025

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

Tools Used: HostedScan OWASP Scanner, OpenVAS

# 1. Introduction

This report presents the results of a vulnerability assessment conducted on the target website (http://www.itsecgames.com) using multiple tools: HostedScan (OWASP Scanner) and OpenVAS. The goal is to identify potential security weaknesses and provide recommendations for mitigation.

# 2. Tools Used

## 2.1 HostedScan (OWASP Vulnerability Scanner)

HostedScan provides automated OWASP vulnerability scans targeting web applications. It checks for common issues such as outdated protocols, insecure cipher suites, and information disclosure.

## 2.2 OpenVAS (Greenbone Vulnerability Scanner)

OpenVAS is a powerful open-source framework for conducting full-system vulnerability assessments. It detects a wide range of security issues, especially network-related and protocol vulnerabilities.

# 3. Scan Results Summary

## 3.1 HostedScan OWASP Report

Total Vulnerabilities Found:

- High: 1  
- Medium: 2  
- Low: 1

• High: Vulnerable Cipher Suites for HTTPS (CVSS Score: 7.5)  
 - Weak ciphers like 3DES are supported, allowing SWEET32 attacks.  
 - Fix: Disable 3DES and configure secure ciphers.  
  
• Medium: Cleartext transmission of sensitive data over HTTP (CVSS Score: 4.8)  
 - Fix: Enforce HTTPS for all pages.  
  
• Medium: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (CVSS Score: 4.3)  
 - Fix: Use TLS 1.2 or higher only.  
  
• Low: TCP Timestamp Disclosure (CVSS Score: 2.6)  
 - Fix: Disable TCP timestamps to avoid information disclosure.

## 3.2 OpenVAS Report Summary

The OpenVAS scan confirms the same critical findings:  
- SSL/TLS weaknesses  
- Deprecated protocols  
- Information leakage due to HTTP and TCP timestamps

# 4. Recommendations

1. Update the SSL/TLS configuration to use secure cipher suites (AES-GCM, ECDHE).  
2. Enforce HTTPS across the entire application.  
3. Disable TLS 1.0 and 1.1.  
4. Disable TCP timestamps in the server's network configuration.  
5. Rescan the server after applying fixes to confirm resolution.

# 5. Conclusion

The vulnerability assessment identified several moderate to high security issues related to outdated protocols and insecure transmission. Implementing the recommended mitigations will significantly improve the overall security posture of the target system.

# 6. Appendix: OpenVAS Service Error

The following screenshot shows an error encountered while starting the OpenVAS (GVM) service. This error indicates that the 'gvmd' service failed to start due to a timeout. To troubleshoot, refer to the command: 'journalctl -xeu gvmd.service'.

