Penetration Testing Report

Date: October 14, 2025
Version: 1.0

By	For
Aymaan Balbale (Penetration Tester) Mumbai, India Email: aymaanbalbale06@gmail.com Phone: +91 9619762744 Linkedin: linkedin.com/in/aymaan-balbale-4468b2336	**AccuKnox** (Hiring Team) Computer and Network sslscanSecurity Menlo Park, California.

Table of Contents

Legal Notice

Confidentiality:

This document contains sensitive and confidential information intended solely for the recipient, AccuKnox. It should not be distributed to or shared with any third parties without prior written permission from the author, Aymaan Balbale.

GDPR : N/A

Disclaimers :

This report is a "point-in-time" assessment based on the agreed-upon scope. The findings represent the security posture of the target system at the time of testing. New vulnerabilities may emerge, and this report does not guarantee the system is free from all possible security weaknesses. The information provided is for security assessment purposes only and should not be used for malicious activities.

Change Log

Date	Version	Comments
N/A	N/A	N/A
N/A	N/A	N/A

Executive Summary

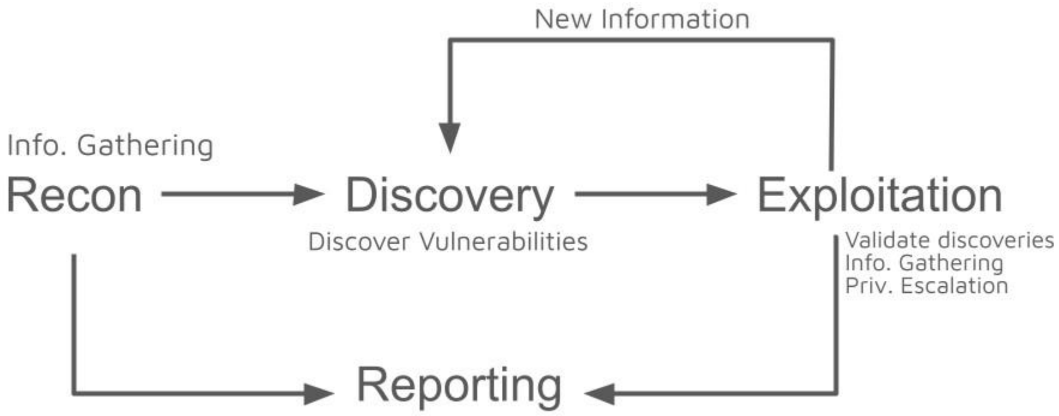
AccuKnox engaged [Aymaan balbale] to conduct a security assessment and penetration test against the itsecgames.com web application. The main goal of the engagement was to evaluate the security of the platform and identify possible threats and vulnerabilities. This report details the scope of the engagement, comprehensive information about all findings, and actionable recommendations.

Based on the security assessment, the current overall risk rating for itsecgames.com is **CRITICAL**.

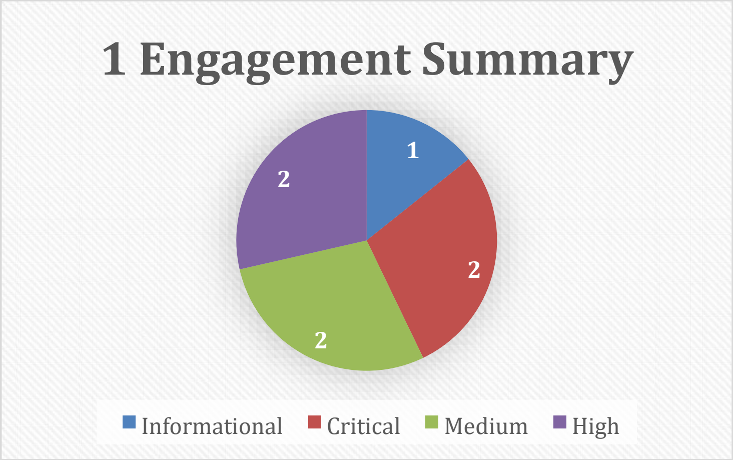
The vulnerabilities discovered can be used by malicious actors to cause a complete data breach, including the theft of user credentials, and potentially gain full remote control of the server. The summary below provides an overview of the findings, while the second section provides in-depth technical details, reproduction steps, and mitigation advice for a technical audience.

Methodology

The methodology followed a standard penetration testing lifecycle: Reconnaissance -> Discovery -> Reporting. Exploitation was not performed to remain within the defined scope.



The following charts summarize the findings grouped by severity of the threat:



1 Engagement Summary

1.1 Scope

As requested, the security assessment was carried out only on the following target:

- **Domain:** `itsecgames.com` (IP: `31.3.96.40`)

1.2 Risk Ratings

The vulnerability risk was calculated based on the Common Vulnerability Scoring System (CVSS v3.1), which is the industry standard for assessing the severity of security vulnerabilities.

Risk	CVSS v3.1 Score	Recommendation
Informational	0.0	N/A
Low	0.1 - 3.9	Fix when time permits.
Medium	4.0 - 6.9	Fix within the next update cycle..
High	7.0 - 8.9	Fix immediately if there are 0 critical vulnerabilities.
Critical	9.0 - 10.0	Fix immediately.

1.3 Findings Overview

Below is a list of all the issues found during the engagement along with a brief description, its impact and the risk rating associated with it. Please refer to the "Risk Ratings" section for more information on how this is calculated.

ID	Risk	Description
1	Critical	Publicly exposed database backups leading to full data compromise.
2	Critical	Invalid SSL/TLS certificate enabling Man-in-the-Middle attacks
3	High	Outdated CMS (Drupal 7) with known remote code execution vulnerabilities.
4	High	Outdated SSH server (OpenSSH 6.7p1) with known public exploits.
5	Medium	Missing HTTP security headers increasing risk of client-side attacks.
6	Medium	Outdated TLS protocols (1.0, 1.1) enabled, weakening encryption.
7	Low	Web Application Firewall (WAF) detected, indicating a positive security control.

2.1 Publicly Exposed Database Backups CRITICAL **ID:** 1

I discovered that the web server hosts publicly accessible database backup files. An attacker can download these files directly without any authentication, resulting in a complete data breach.

URL	`http://itsecgames.com/database.tar.bz2` `https://itsecgames.com/MFH9vl9x.sql`
Parameter	N/A
References	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure
Reproduction	nikto -h http://itsecgames.com
Response	/database.tar.bz2: Drupal 7 was identified via the x-generator header. /MFH9vl9x.sql: The X-Content-Type-Options header is not set.

Impact:

As a result of this vulnerability, a malicious actor can:

1. Download the entire application database.
2. Retrieve all user data, including usernames and hashed passwords.
3. Gain access to sensitive configuration details.

Mitigation:

- Immediately **remove** `database.tar.bz2` and `MFH9vl9x.sql` from the web root.
- Store all backups in a secure, non-public location with strict access controls.
- Audit web server logs to determine if these files were accessed by unauthorized parties.

2.2 Invalid SSL/TLS Certificate **CRITICAL** **ID:** 2

The SSL/TLS certificate for itsecgames.com is expired, self-signed, and issued for a different domain (mmebv.be). This completely breaks the chain of trust and renders HTTPS ineffective.

URL	https://itsecgames.com
Parameter	N/A
References	https://www.google.com/search?q=https://owasp.org/www-project-top-ten/2013/a6sensitive-data-exposure
Reproduction	sslscan itsecgames.com
Response	`Subject: web.mmebvba.com Issuer: web.mmebvba.com Not valid after: May 22 09:07:54 2025 GMT`

Impact: A malicious actor can perform a Man-in-the-Middle (MitM) attack to intercept, read, and modify all traffic between users and the server, including login credentials.

Mitigation:

- Obtain a valid SSL certificate from a trusted Certificate Authority (e.g., Let's Encrypt).
- Ensure the certificate's Common Name (CN) and Subject Alternative Names (SANs) correctly list `itsecgames.com`.

.

2.3 Outdated CMS (Drupal 7) High **ID:** 3

The web server is running Drupal 7, an outdated Content Management System with a history of critical, unauthenticated remote code execution vulnerabilities like "Drupalgeddon 2" (CVE2018-7600).

URL	https://itsecgames.com
Parameter	N/A
References	https://nvd.nist.gov/vuln/detail/CVE-2018-7600
Reproduction	nikto -h https://itsecgames.com
Response	/: Drupal 7 was identified via the x-generator header.

Impact: An attacker can use publicly available exploits to take full control of the web server.

Mitigation:

- Develop an immediate plan to migrate the website to a supported platform (e.g., Drupal 10+).
- Apply all available security patches for Drupal 7 as an interim measure.

2.4 Outdated SSH Server (OpenSSH 6.7p1) High **ID:** 4

The server is running a version of OpenSSH from 2014, which has numerous known vulnerabilities.

URL	SSH on port 22
Parameter	N/A
References	https://nvd.nist.gov/vuln/detail/cve-2016-10009
Reproduction	nmap -sV itsecgames.com
Response	22/tcp open ssh OpenSSH 6.7p1 (protocol 2.0)

Impact: An attacker could potentially exploit these known vulnerabilities to gain remote access to the server.

Mitigation:

- Update the OpenSSH server package to the latest stable version provided by the OS distributor.

(Additional findings for Medium and Informational vulnerabilities would follow the same format.)

2.5 Missing HTTP Security Headers Medium **ID:** 5

The server fails to send important security headers that instruct browsers to enable built-in security features. This absence weakens the site's defenses against common client-side attacks.

URL	https://itsecgames.com
Parameter	N/A
References	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html
Reproduction	nikto -h https://itsecgames.com
Response	The anti-clickjacking X-Frame-Options header is not present. The XContent-Type-Options header is not set. The site uses TLS and the StrictTransport-Security HTTP header is not defined.

Impact: The missing headers expose users to attacks such as:

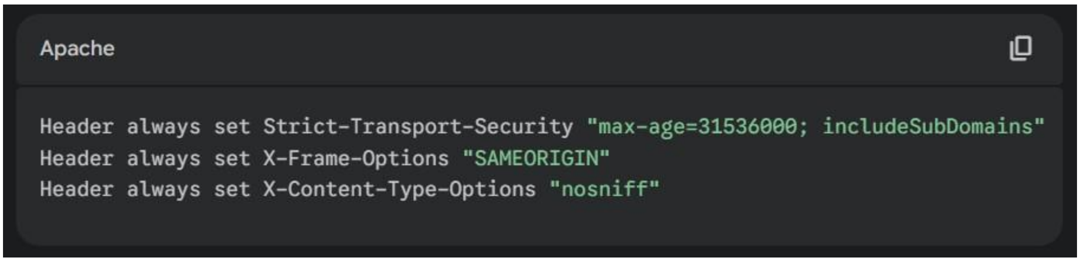
1. **Clickjacking:** An attacker can load the site in a hidden frame to trick users into performing unintended actions.

2. **SSL Stripping:** Without HSTS, an attacker can downgrade a user's connection from secure HTTPS to unencrypted HTTP.

.

Mitigation:

- Configure the Apache server to send the following HTTP headers with every response: "



```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
```

2.6 Outdated TLS Protocols Enabled Medium **ID:** 6

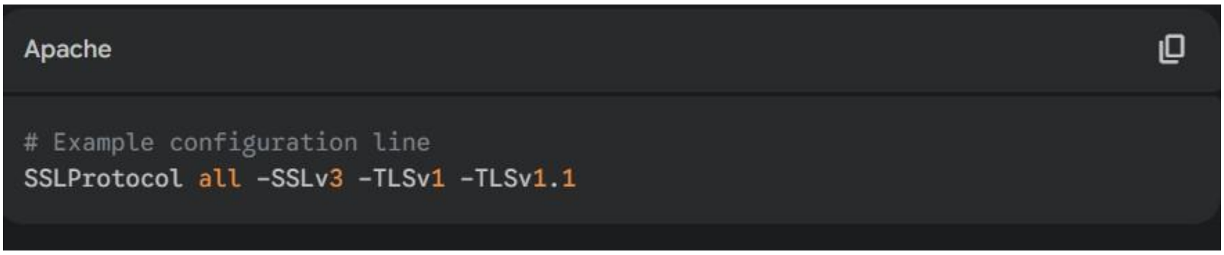
The server supports obsolete and insecure protocols (TLS 1.0 and TLS 1.1), which have known cryptographic weaknesses and are deprecated by all modern browsers and security standards.

URL	HTTPS on port 443
Parameter	N/A
References	https://www.google.com/search?q=https://www.nist.gov/blogs/it-security/nist-guidancedeprecating-tls-10-and-tls-11
Reproduction	sslscan itsecgames.com
Response	TLSv1.0 enabled TLSv1.1 enabled

Impact: A sophisticated attacker could potentially force a user's browser to connect using these weaker protocols, making the encrypted traffic easier to intercept and decrypt.

Mitigation:

- Modify the Apache SSL/TLS configuration file to disable these protocols and allow Only modern, secure versions.



```
# Example configuration line
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

2.7 Web Application Firewall (WAF) Detected Informational **ID: 7**

During testing, automated attempts to interact with the Drupal login form (/user/login) were consistently blocked with a 403 Forbidden error. This indicates the presence of a security control.

URL	https://itsecgames.com/user/login
Parameter	N/A
References	https://owasp.org/www-community/Web_Application_Firewall
Reproduction	curl -d "name=admin&pass=admin" https://itsecgames.com/user/login -k
Response	HTTP/1.1 403 Forbidden

Impact: This is a **positive security finding**. It shows that a defensive mechanism is in place that is effective at blocking basic automated attacks against authenticated endpoints..

Mitigation:

- No mitigation is required. It is recommended to maintain and regularly update the rules to ensure continued effectiveness against emerging threats.