Job Title: Security Officer Trainee

http://www.itsecgames.com/

Objectives:

- Identify vulnerabilities on this domain name. You can use any publicly available tools. But you have to pull up the report and show the vulnerability reported by the tool.
- Detect potential vulnerabilities (misconfigurations, outdated software, CVEs).
- Assess SSL/TLS configuration and certificate health.
- Highlight any exposed information that could aid attackers (headers, banners, error messages.
- Provide a prioritized list of findings along with mitigation recommendations.

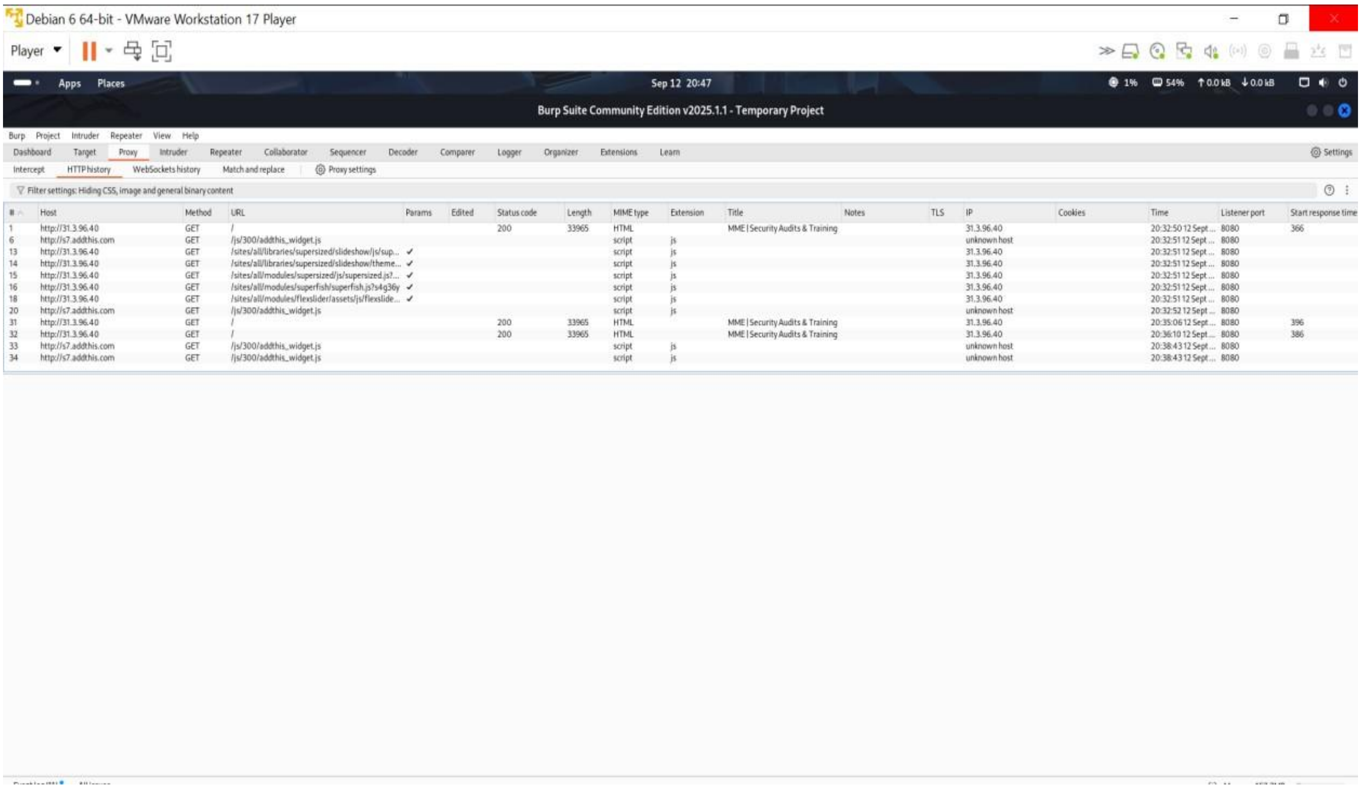
Name: Chethan S

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

Target IP: 31.3.96.40

Tool Used: Burp Suite (Community Addition)

Stage 1 : Identify vulnerabilities on this domain name. You can use any publicly available tools. But you have to pull up the report and show the vulnerability reported by the tool.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response time
1	http://31.3.96.40	GET	/			200	33965	HTML		MME | Security Audits & Training			31.3.96.40		20:32:50 12 Sept ...	8080	366
6	http://s7.addthis.com	GET	/js/300/addthis_widget.js					script	js				unknown host		20:32:51 12 Sept ...	8080	
13	http://31.3.96.40	GET	/sites/all/libraries/supersized/slideshow/js/sup...	✓				script	js				31.3.96.40		20:32:51 12 Sept ...	8080	
14	http://31.3.96.40	GET	/sites/all/libraries/supersized/slideshow/theme...	✓				script	js				31.3.96.40		20:32:51 12 Sept ...	8080	
15	http://31.3.96.40	GET	/sites/all/modules/supersized/js/supersized.js?...	✓				script	js				31.3.96.40		20:32:51 12 Sept ...	8080	
16	http://31.3.96.40	GET	/sites/all/modules/superfish/superfish.js?s4g36y	✓				script	js				31.3.96.40		20:32:51 12 Sept ...	8080	
18	http://31.3.96.40	GET	/sites/all/modules/flexslider/assets/js/flexslide...	✓				script	js				31.3.96.40		20:32:51 12 Sept ...	8080	
20	http://s7.addthis.com	GET	/js/300/addthis_widget.js					script	js				unknown host		20:32:52 12 Sept ...	8080	
31	http://31.3.96.40	GET	/			200	33965	HTML		MME | Security Audits & Training			31.3.96.40		20:35:06 12 Sept ...	8080	396
32	http://31.3.96.40	GET	/			200	33965	HTML		MME | Security Audits & Training			31.3.96.40		20:36:10 12 Sept ...	8080	386
33	http://s7.addthis.com	GET	/js/300/addthis_widget.js					script	js				unknown host		20:38:43 12 Sept ...	8080	
34	http://s7.addthis.com	GET	/js/300/addthis_widget.js					script	js				unknown host		20:38:43 12 Sept ...	8080	

Vulnerabilities Visible in the Given Image

1. **Unencrypted HTTP traffic**
   - All requests are made to http://31.3.96.40 (no HTTPS).
   - This allows **man-in-the-middle (MITM)** attacks and data interception.
2. **Outdated CMS (Drupal 7)**
   - Identified earlier by the response header X-Generator: Drupal 7.
   - Drupal 7 is **end of life (EOL)** → vulnerable to multiple **Remote Code Execution (RCE)** and **SQL Injection** CVEs.
3. **Outdated JavaScript Libraries**
   - **jQuery 1.5** (from 2011) is loaded. Known to have **XSS vulnerabilities** (e.g., CVE-2011-4969).
   - Other libraries (supersized.js, superfish.js, flexslider.js) are also old and may contain client-side vulnerabilities.

4. **Third-party Script Inclusion**

   - addthis_widget.js is fetched from s7.addthis.com.

   - Using external JavaScript over HTTP can expose the site to **supply-chain attacks** if the external source is compromised.

5. **Information Disclosure**

   - The CMS version (Drupal 7) and libraries are **easily fingerprinted** from headers and requests.

   - Attackers can match this info with known exploits.

Mitigations Or Patch management:

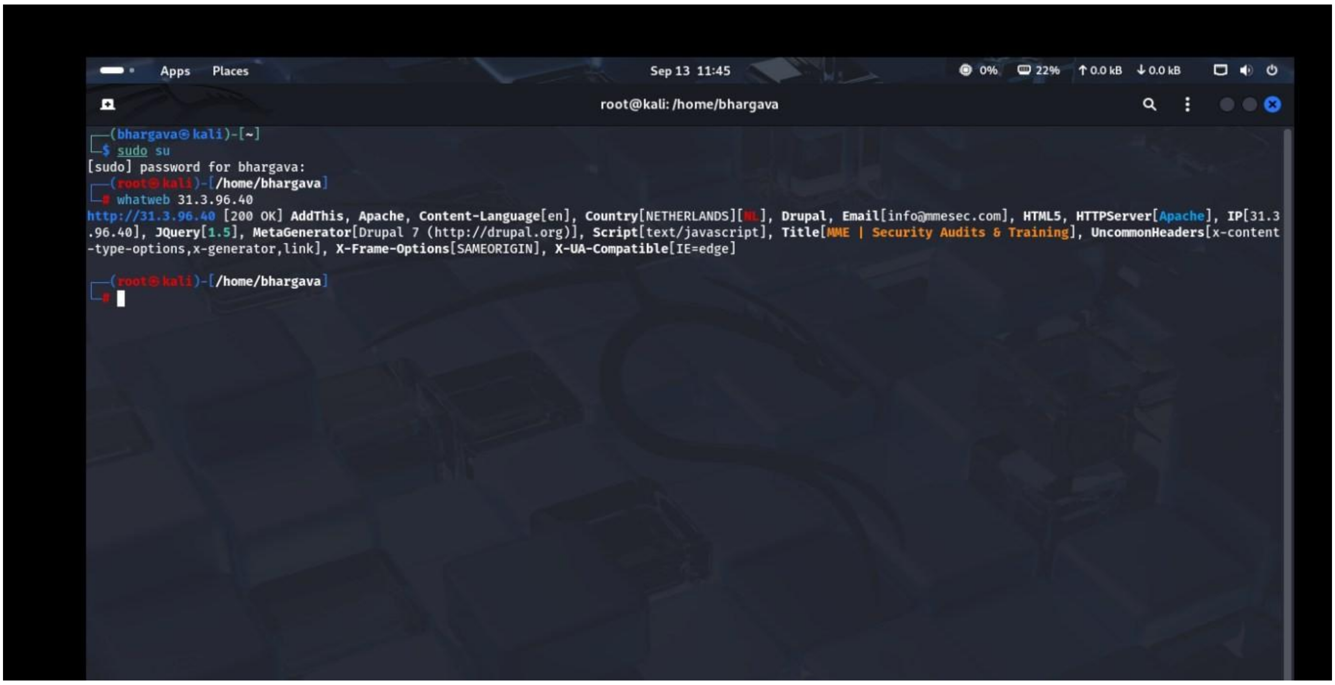
- Implement HTTPS - Set up SSL/TLS certificates and redirect all requests from HTTP to HTTPS. Use HSTS (Strict-Transport-Security) so that the attacker cannot downgrade the connection.
- Upgrade Drupal - Move from Drupal 7 (EOL) to one of the supported versions (Drupal 9 or 10), and therefore get security patches, as well as eliminate wellknown RCE/SQLi bugs.
- Update jQuery & JS Libraries - Make sure the jQuery 1.5 is replaced with the latest stable version, and update or remove obsolete libraries (Supersized, Superfish & Flexslider).
- Secure 3rd Party Scripts - Host scripts locally if you can, and load them using HTTPS. Use Subresource Integrity (SRI) check from CORS enabled CDN's.
- Harden HTTP Headers - Add modern headers:

- Content-Security-Policy (CSP)
- X-Content-Type-Options: nosniff
- X-Frame-Options: DENY or frame-ancestors 'self'
- Referrer-Policy
- Remove Version Disclosure - Disable or obfuscate headers like X-Generator: Drupal so that the attacker cannot fingerprint the CMS.
- Regular Vulnerability Scanning - use tools such as Nikto, OpenVAS or Burp Suite Pro to ensure that your environment is kept up, reviewed and remediated to fix new vulnerabilities.
- Patch Management & Monitoring - Ensure your server software, CMS specific modules and plugins are up to date and enable logging/monitoring for abnormal or suspicious events.

Stage2: Detect potential vulnerabilities (misconfigurations, outdated software, CVEs).

Tool used: **WhatWeb** identify web technologies (CMS, frameworks, servers).

Findings:



```
┌──(bhargava㉿kali)-[~]
└─$ sudo su
[sudo] password for bhargava:
┌──(root㉿kali)-[/home/bhargava]
└─# whatweb 31.3.96.40
http://31.3.96.40 [200 OK] AddThis, Apache, Content-Language[en], Country[NETHERLANDS][NL], Drupal, Email[info@mmesec.com], HTML5, HTTPServer[Apache], IP[31.3
.96.40], JQuery[1.5], MetaGenerator[Drupal 7 (http://drupal.org)], Script[text/javascript], Title[MME | Security Audits & Training], UncommonHeaders[x-content
-type-options,x-generator,link], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge]

┌──(root㉿kali)-[/home/bhargava]
└─# 
```

- **Issue:**

Outdated software:

- Drupal 7 (EOL → exploitable, known RCE CVEs).
- jQuery 1.5 (10+ years old, vulnerable to XSS CVEs).

- **Misconfigurations / Weaknesses:**
  - Reliance on legacy X-UA-Compatible.
  - Missing modern security headers (HSTS, CSP).
  - Using EOL CMS = High security risk.

- **Mitigations:**

Old Software:

- Drupal 7 (EOL): Move to a supported version of Drupal (10.x) or another CMS. If you’re unable to upgrade, at least apply the latest security patches now.
- jQuery 1.5: Please upgrade to the most recent stable jQuery (≥3.7) and remove any libraries not in use so that you can reduce your attack surface.

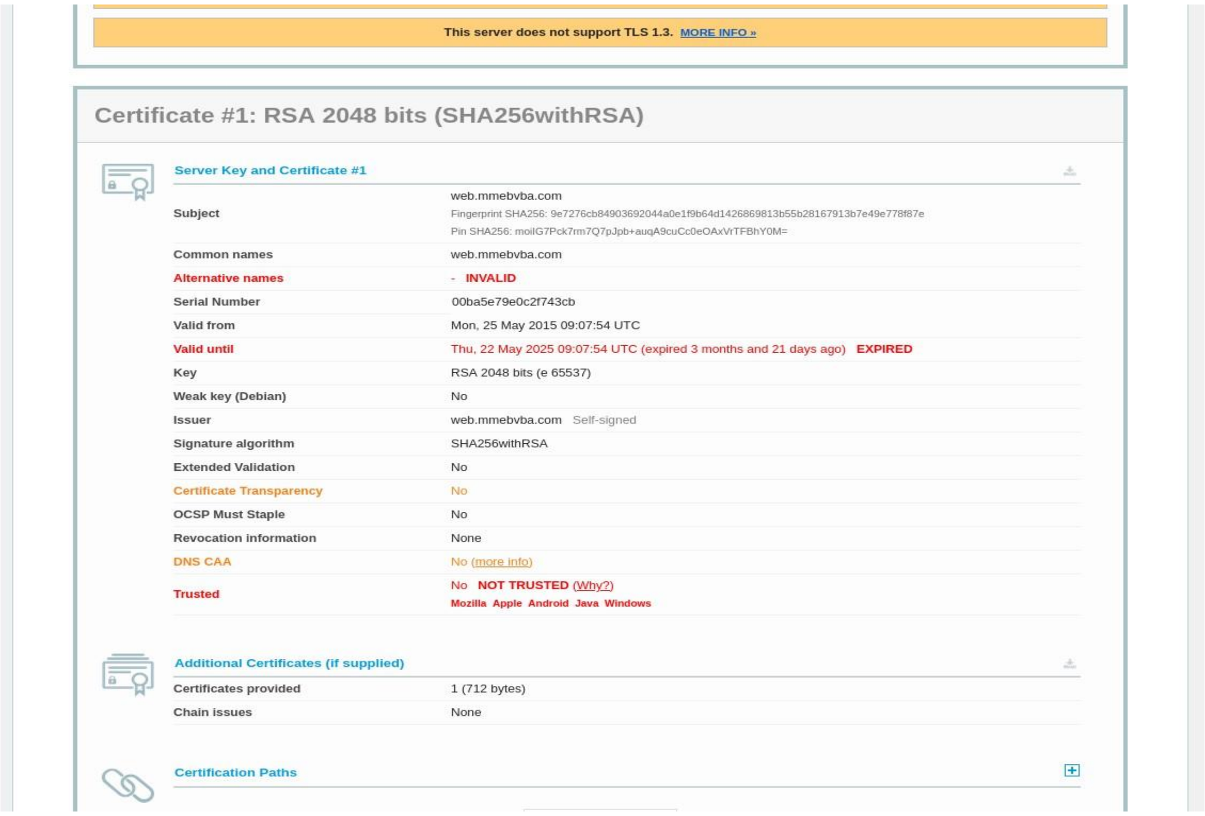
Misconfigurations / Weaknesses:

- X-UA-Compatible (legacy header): Remove it, modern browsers no longer rely on it.
- Missing Security Headers:
- Implement HSTS (Strict-Transport-Security) to mandate HTTPS.
- Implement CSP (Content-Security-Policy) to prevent XSS.
- Potentially implement X-Frame-Options, X-Content-Type-Options and Referrer-Policy.

Stage3: Assess SSL/TLS configuration and certificate health.

Tool used: https://www.ssllabs.com/ssltest/

Findings:



This server does not support TLS 1.3. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

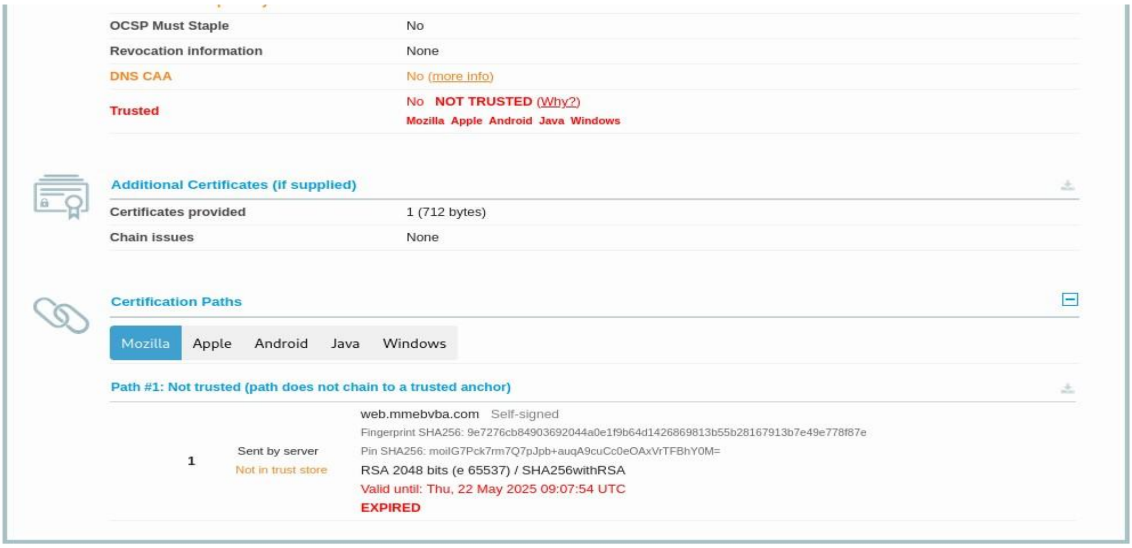
Server Key and Certificate #1

Subject	web.mmebvba.com Fingerprint SHA256: 9e7276cb84903692044a0e1f9b64d1426869813b55b28167913b7e49e778f87e Pin SHA256: moilG7Pck7rm7Q7pJpb+auqA9cuCc0eOAxVrTFBhY0M=
Common names	web.mmebvba.com
Alternative names	- INVALID
Serial Number	00ba5e79e0c2f743cb
Valid from	Mon, 25 May 2015 09:07:54 UTC
Valid until	Thu, 22 May 2025 09:07:54 UTC (expired 3 months and 21 days ago) EXPIRED
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	web.mmebvba.com Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	1 (712 bytes)
Chain issues	None

Certification Paths



OCSP Must Staple	No
Revocation information	None
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows

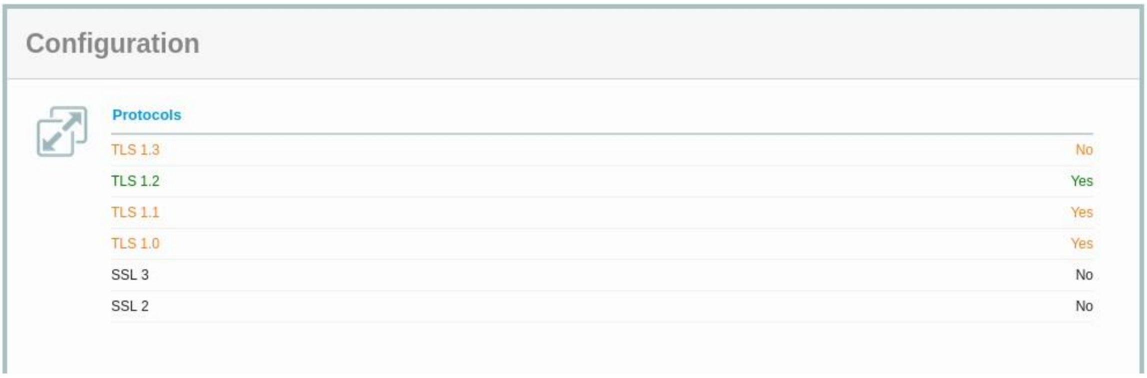
Additional Certificates (if supplied)

Certificates provided	1 (712 bytes)
Chain issues	None

Certification Paths

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server Not in trust store	web.mmebvba.com Self-signed Fingerprint SHA256: 9e7276cb84903692044a0e1f9b64d1426869813b55b28167913b7e49e778f87e Pin SHA256: moilG7Pck7rm7Q7pJpb+auqA9cuCc0eOAxVrTFBhY0M= RSA 2048 bits (e 65537) / SHA256withRSA Valid until: Thu, 22 May 2025 09:07:54 UTC EXPIRED



Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

SSL/TLS configuration and certificate health:

- Expired Certificate – The SSL certificate has expired, thus creating trust issues. → Renew with a valid CA certificate
- Self-Signed and Not Trusted – The certificate was self-signed and not chained to a trusted root. → Get a trusted public CA.
- Weak Protocols Enabled – TLS 1.0 and 1.1 are still enabled. → Disable them and only allow TLS 1.2+.
- TLS 1.3 Not Supported – The server does not support TLS 1.3. → Enable TLS 1.3 for stronger security.
- Invalid Certificate Names – The SAN/altnames are invalid. → Issue the correct CN/SANs.
- No OCSP Stapling / Revocation Information – There are missing methods for revocation. → Enable OCSP Stapling.
- No CAA /CT – There are no CAA records or CT log entries. → Add DNS CAA and enable CT.

Stage4: Highlight any exposed information that could aid attackers (headers, banners, error messages).

Server header (e.g., Server:) → exposes server/version → attackers find out relevant CVEs. Fix: hide/obfuscate banner & patch.

X-Powered-By → exposes framework/runtime (e.g., PHP) → allows targeted exploits. Fix: remove header & upgrade runtime.

Expired / self-signed cert → shows no trust/ops hygiene → users/browser warn; MITM. Fix: install valid CA-signed cert.

Certificate name mismatch (invalid SAN/CN) → exposes real hostnames → causes trust errors. Fix: issue cert with valid CN/SAN.

Old TLS version enabled (TLS1.0/1.1) → vulnerability to downgrade/crypto attacks. Fix: disable TLS1.0/1.1, enable TLS1.2+.