

# Security Assessment

This is a report on security assessment in <http://www.itsecgames.com> domain, Including vulnerability assessment, mitigation methods and SSL/TLS analysis. All scans were done with publicly available tools with permission to scan domain. The scan result screenshots can be seen in "Scan Results" folder for all scans done on the domain.

---

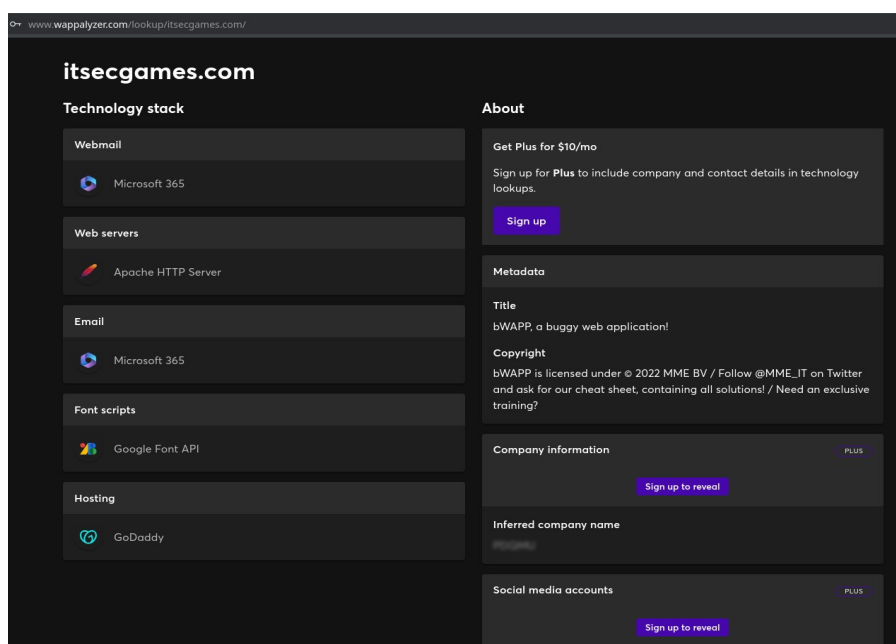
## Tools Used For Analysis

- **Wappalyzer** - (fingerprinting websites technologies)
  - **Nmap** - (port scanning and enumeration of services)
  - **Gobuster** - (fuzzing directories and virtual hosts)
  - **Nikto** - (vulnerability scanning tool for web servers)
  - **OWASP ZAP** - (web application security scanner)
  - **OpenVAS** - (vulnerability scanner)
  - **MX Toolbox** - (enumerates DNS, DMARC and SPF records)
  - **Hacker Target** - (Reverse IP lookup for domains in IP)
  - **SecurityHeaders.com** - (Checks for vulnerable and missing headers)
  - **SSL Labs** - (provides website SSL/TLS certificate status and information)
- 

## Findings

### Wappalyzer

- Found the website uses Apache HTTP Server and Microsoft for Emails



## Nmap

- The scan revealed open ports 22 (SSH), 80 (HTTP) and 443 (HTTPS)
- Port 22 is running OpenSSH 6.7p1 which outdated and has vulnerabilities like CVE-2016-0777 and CVE-2018-1547
- Found 36 exposed directories through robots.txt for <https://mmesec.com> domain hosted on same IP including CHANGELOG.txt and intallation files exposing technologies and versions
- Drupal version 7.69 exposed which is deprecated and has multiple critical vulnerabilities like CVE-2020-13663 found in <https://mmesec.com> domain.
- Found TLS certificate expired on 22-5-2025

```
~/Downloads - fish
Nmap done: 1 IP address (1 host up) scanned in 130.70 seconds

~/Downloads 2m 10s
> sudo nmap -Pn -sS -sV -A 31.3.96.40 -p-
[sudo] password for xcalifar:
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-04 17:05 +0530
Nmap scan report for web.mmebvba.com (31.3.96.40)
Host is up (0.19s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 (protocol 2.0)
53/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt
|_http-title: Did not follow redirect to https://www.mmebvba.com
443/tcp   open  ssl/http     Apache httpd
|_http-server-header: Apache
|_ssl-cert: Subject: commonName=web.mmebvba.com
|_Not valid before: 2015-05-25T09:07:54
|_Not valid after:  2025-05-22T09:07:54
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 4.X|3.X|5.X|2.6.X (96%), IPFire 2.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2
Aggressive OS guesses: Linux 4.0 - 4.4 (96%), Linux 3.10 - 4.11 (90%), Linux 3.11 - 4.9 (90%), Linux 4.15 (90%), Linux 4.19 - 5.15 (90%), IPFire 2.25 firewall (Linux 4.14) (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   8.30 ms  10.107.39.99
2   45.16 ms 192.168.0.1
3   45.16 ms 10.11.9.1
4   23.33 ms 22.22.22.1
5   68.89 ms 137.97.255.33
6   ... 7
8   163.42 ms 103.198.140.29
9   165.67 ms 103.198.140.56
```

## Gobuster

- Found Directories called images, downloads, js and javascript with restricted access

```
~/.go/bin - fish
Progress: 0 / 1 (0.00%)^C=
~/go/bin
> ./gobuster dir -u http://itsecgames.com -t 50 -w SecLists-master/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-big.txt
=====
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://itsecgames.com
[+] Method: GET
[+] Threads: 50
[+] Wordlist: SecLists-master/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8.2
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
Progress: 0 / 1273831 (0.00%) [ERROR] error on word cgi-bin: connection refused
[ERROR] error on word # Copyright 2007 James Fisher: connection refused
[ERROR] error on word products: connection refused
[ERROR] error on word warez: connection refused
[ERROR] error on word search: connection refused
[ERROR] error on word # directory-list-2.3-big.txt: connection refused
[ERROR] error on word spacer: connection refused
[ERROR] error on word img: connection refused
images (Status: 301) [Size: 237] [-> http://itsecgames.com/images/]
downloads (Status: 301) [Size: 240] [-> http://itsecgames.com/downloads/]
js (Status: 301) [Size: 233] [-> http://itsecgames.com/js/]
javascript (Status: 301) [Size: 241] [-> http://itsecgames.com/javascript/]
Progress: 1116 / 1273831 (0.09%) [ERROR] error on word splash: timeout occurred during the request
[ERROR] error on word org: timeout occurred during the request
[ERROR] error on word share: timeout occurred during the request
[ERROR] error on word wink: timeout occurred during the request
[ERROR] error on word customer: timeout occurred during the request
[ERROR] error on word B: timeout occurred during the request
Progress: 1122 / 1273831 (0.09%) [ERROR] error on word E: timeout occurred during the request
[ERROR] error on word 162: timeout occurred during the request
[ERROR] error on word Technology: timeout occurred during the request
[ERROR] error on word reddit: timeout occurred during the request
[ERROR] error on word win: timeout occurred during the request
[ERROR] error on word cp: timeout occurred during the request
[ERROR] error on word 170: timeout occurred during the request
[ERROR] error on word ar: timeout occurred during the request
[ERROR] error on word directions: timeout occurred during the request
```

---

## Nikto

- X-Content-Type-Options header missing which can make it vulnerable to content sniffing attacks incorrectly assessing MIME type of files
- Missing X-Frame-Options header which makes it vulnerable to click jacking through iframes
- Referrer-Policy header missing which can leak sensitive information from url to other sites when clicking links.
- Server may leak inode number or multipart MIME boundary, which reveals child process IDs (PID) through E-Tag CVE-2003-1418
- Content-Security-Policy header not found which prevents attacks by verifying only whitelisted data are being loaded in the website
- Drupal version 7 was identified through x-generator header, Drupal 7 is outdated and has multiple vulnerabilities
- Apache default files /icons/README was found which can leak information on server and version
- HTTP OPTIONS method is allowed which can be used to gain information of webserver and its users if Cross-Origin-Resource-Sharing (CORS) is incorrectly configured.
- Strict-Transport-Security\_Header (HSTS) not set which allows downgrade attacks from HTTPS to HTTP
- No TLS/SSL Support found

```
-vhost+          Virtual host (for Host header)
-404code         Ignore these HTTP codes as negative responses (always). Format is "302,301".
-404string       Ignore this string in response body content as negative response (always). Can be a regular expression.
+ requires a value

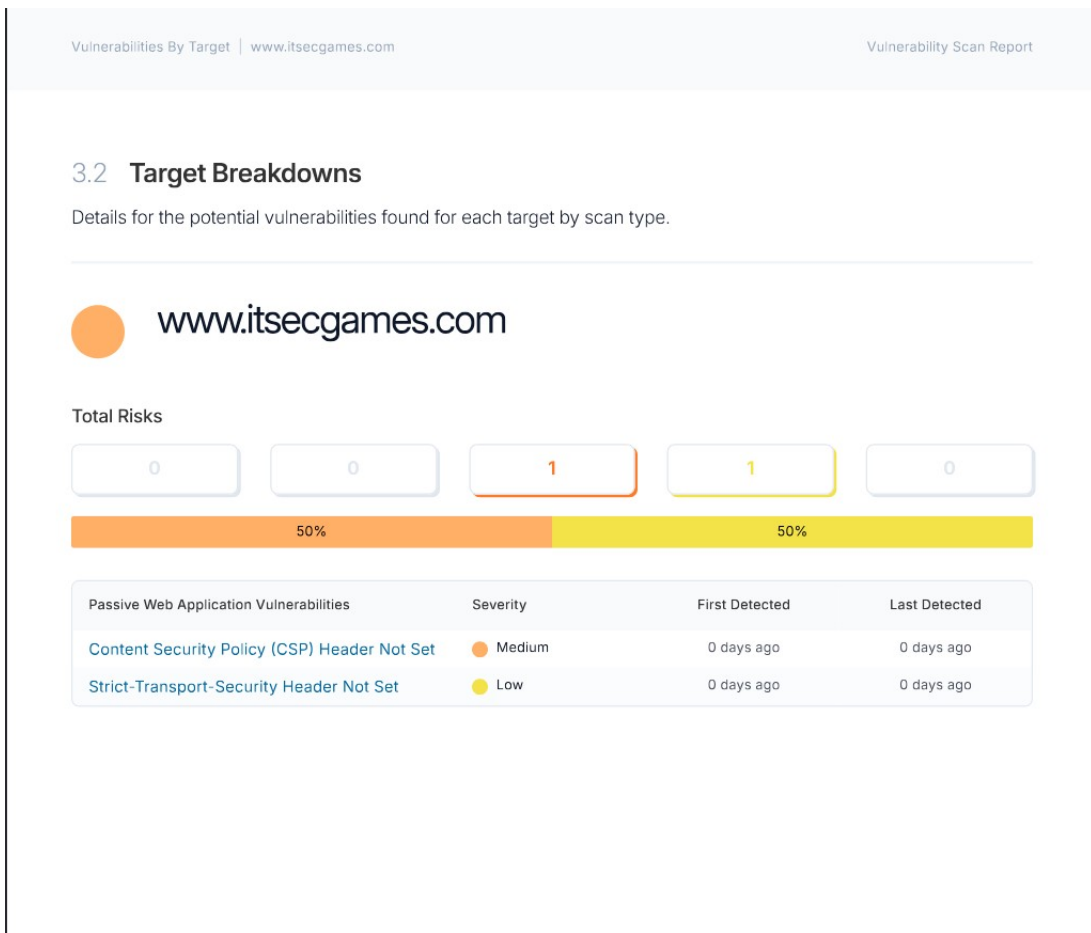
+ WARNING: SSL: support not available.

~/nikto/program
> ./nikto.pl -h www.itsecgames.com
+**** TLS/SSL support not available (see docs for SSL install) ****+
+ Nikto v2.5.0
+-----+
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:       80
+ Start Time:        2025-10-04 16:43:00 (GMT5.5)
+-----+
+ Server: Apache
+ Multiple IPs found: 31.3.96.40, 64:ff9b::1f03:6028
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: Suggested security header missing: referrer-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy
+ /: Suggested security header missing: x-content-type-options. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /: Suggested security header missing: permissions-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy
+ /: Suggested security header missing: strict-transport-security. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: Suggested security header missing: content-security-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
+ /itsecgames.com.tgz: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /itsecgames.com.tgz: Link header(s) found with value(s): <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink". See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Link
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ STATUS: Completed 5041 requests (~72% complete, 10.9 minutes left): currently in plugin 'Nikto Tests'
+ STATUS: Running average: Not enough data.
+ Scan terminated: 2 error(s) and 11 item(s) reported on remote host
+ End Time:          2025-10-04 17:11:33 (GMT5.5) (1713 seconds)
+-----+
+ 1 host(s) tested

~/nikto/program      28m 34s
>
```

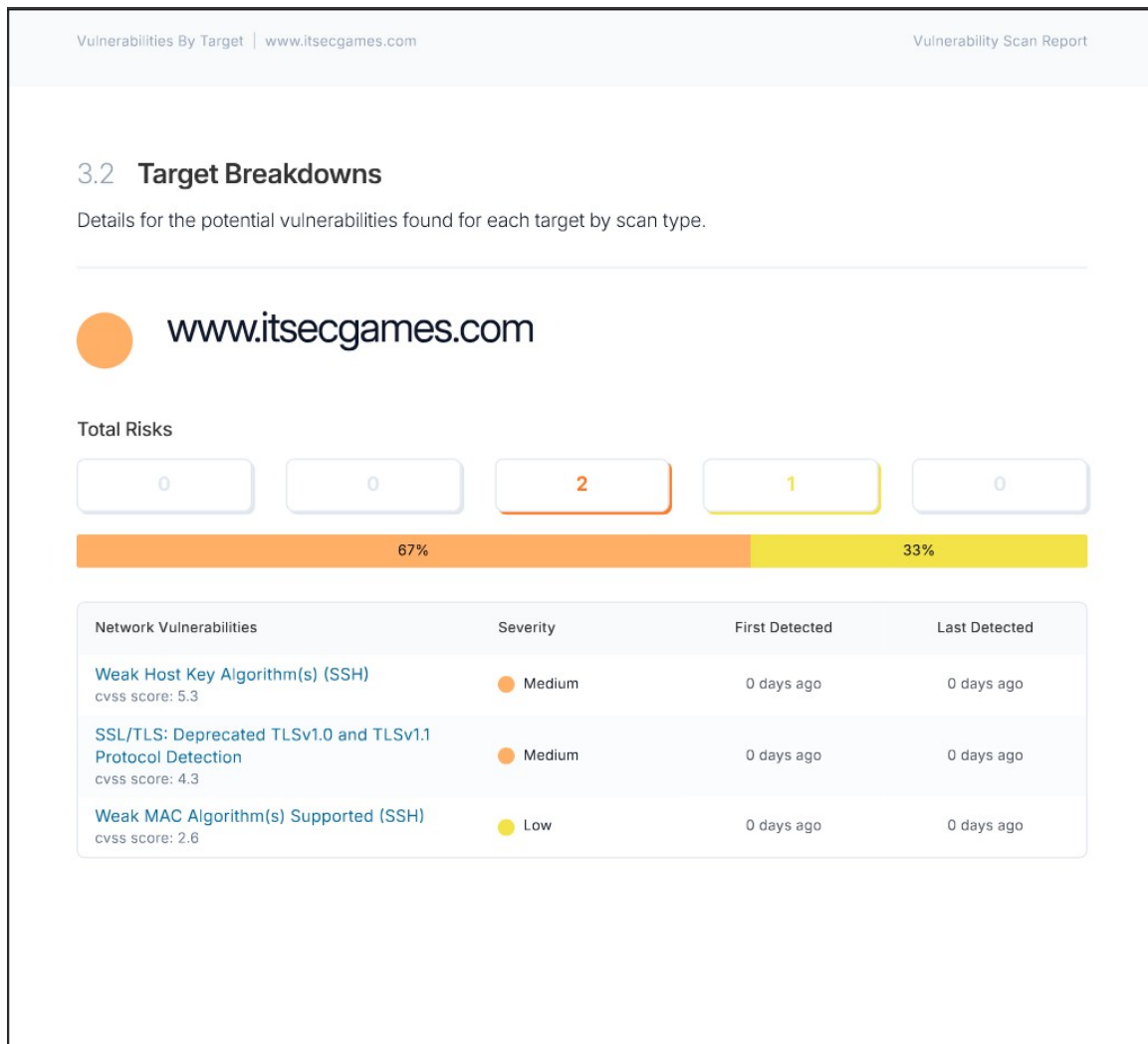
## OWASP ZAP (Hosted scan.com)

- Strict-Transport-Security\_Header (HSTS) not set which allows downgrade attacks
- Content-Security-Policy header not found on website which makes it more vulnerable to attacks



## OpenVAS (Hosted Scan.com)

- Weak Host Key Algorithm found for SSH which uses ssh-dss (Digital signature algorithm) which is deprecated
- Deprecated TLS version 1.0 and 1.1 protocols found on certificate which is vulnerable to multiple CVE's
- Weak MAC algorithm umac-64-etm@openssh supported on SSH



## MX Toolbox

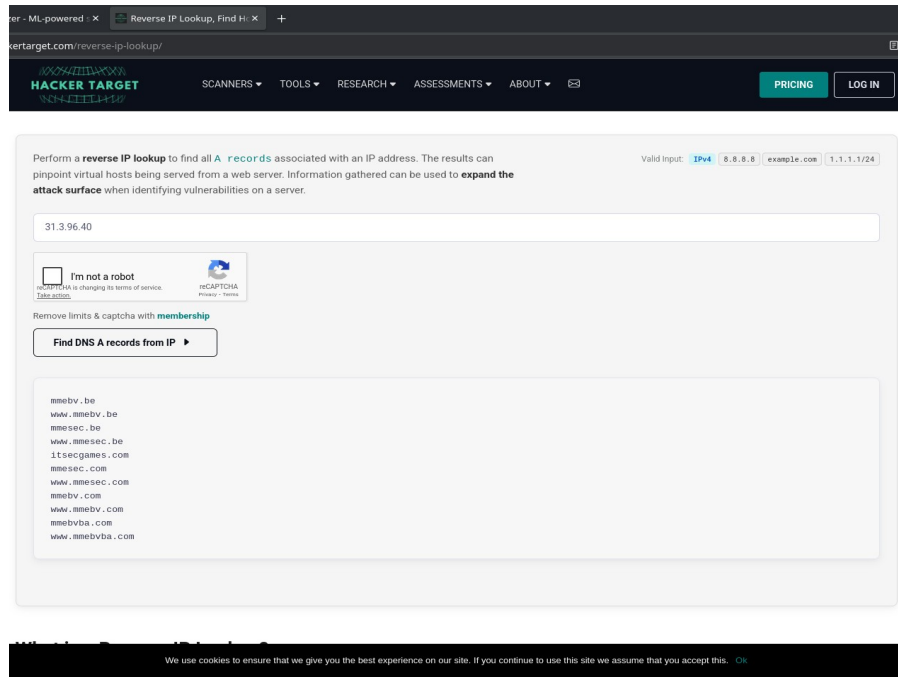
- No DMARC record published
- DMARC(Domain-based Message Authentication) policy is not enabled which makes it vulnerable to email spoofing with the lack of email verification
- TLS/SSL Certificate name mismatch in domain pointing to a different domain
- A null DNS lookup was found for include (mme-srv-dc1.mme.local) which leaks internal Active directory naming structure
- SOA (Start of Authority) Expire Value out of recommended range which may cause downtime if primary DNS server fails, secondary server may stop responding to DNS queries sooner than recommended

**PCI DSS now requires DMARC!** Get ready with MxToolbox Delivery Center! [Learn More](#)

Category	Host	Result	More Info
dmARC	itsecgames.com	No DMARC Record found	<a href="#">More Info</a>
SPF	itsecgames.com	A null DNS lookup was found for include (mme-srv-dc1.mme.local)	<a href="#">More Info</a>
SPF	itsecgames.com	No DMARC Record found	<a href="#">More Info</a>
SPF	itsecgames.com	It is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%.	<a href="#">More Info</a>
MX	itsecgames.com	No DMARC Record found	<a href="#">More Info</a>
MX	itsecgames.com	It is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%.	<a href="#">More Info</a>
HTTPS	itsecgames.com	The Certificate has a name mismatch	<a href="#">More Info</a>
DNS	itsecgames.com	SOA Expire Value out of recommended range	<a href="#">More Info</a>

## Hacker Target

- Found Multiple hosts on the ip 31.3.96.40 on reverse DNS lookup
  - mmebv.be
  - [www.mmebv.be](http://www.mmebv.be)
  - mmesec.be
  - [www.mmesec.be](http://www.mmesec.be)
  - itsecgames.com
  - mmesec.com
  - [www.mmesec.com](http://www.mmesec.com)
  - mmebv.com
  - [www.mmebv.com](http://www.mmebv.com)
  - mmebvba.com
  - [www.mmebvba.com](http://www.mmebvba.com)



## SecurityHeaders.com

- X-Frame-Options header is not found which makes website vulnerable to clickjacking through i-frames
- Permission-policy header is missing which controls browser access to websites API's and features for more security
- Content-Security-Policy header not found on website which makes it more vulnerable to attacks
- X-Content-Type-Options header missing which can make it vulnerable to content sniffing attacks
- Referrer-Policy header missing which can leak sensitive information from url to other sites when clicking links.

Security Report Summary

**F**

Site: <http://www.itsecgames.com/> - (Scan again over https)

IP Address: 31.3.96.40

Report Time: 04 Oct 2025 12:32:28 UTC

Headers: **✖ Content-Security-Policy** **✖ X-Frame-Options** **✖ X-Content-Type-Options** **✖ Referrer-Policy** **✖ Permissions-Policy**

Warning: Grade capped at A, please see warnings below.

Advanced: Ouch, you should work on your security posture immediately. [Start Now](#)

Missing Headers

**Content-Security-Policy** [Content Security Policy](#) is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

**X-Frame-Options** [X-Frame-Options](#) tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".

**X-Content-Type-Options** [X-Content-Type-Options](#) stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".

**Referrer-Policy** [Referrer Policy](#) is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

**Permissions-Policy** [Permissions Policy](#) is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

**Site is using HTTP** This site was served over HTTP and did not redirect to HTTPS.

## SSL Labs

- TLS/SSL Certificate name mismatch domain name pointing to domain web.mmebvba.com
- Server dosent support TLS 1.3 only supports deprecated TLS versions 1.0 and 1.1
- Server dosent support forward secrecey previous communications can be decrypted if TLS decryption key leaks
- The certificate expired at 22/5/2025
- The cerificate is self signed by web.mmebvba.com so it dosent have a root of trust form a Certificate Authority (CA) and is not trusted by browser.

at D: x SSL Server Test: www.itsec: x +

ssltest/analyze.html?id=www.itsecgames.com

**Qualys. SSL Labs** Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.itsecgames.com

**SSL Report: www.itsecgames.com (31.3.96.40)**

Assessed on: Sat, 04 Oct 2025 15:24:12 UTC | [Hide](#) | [Clear cache](#) [Scan Another »](#)

Summary

Overall Rating

**T**

If trust issues are ignored: B

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

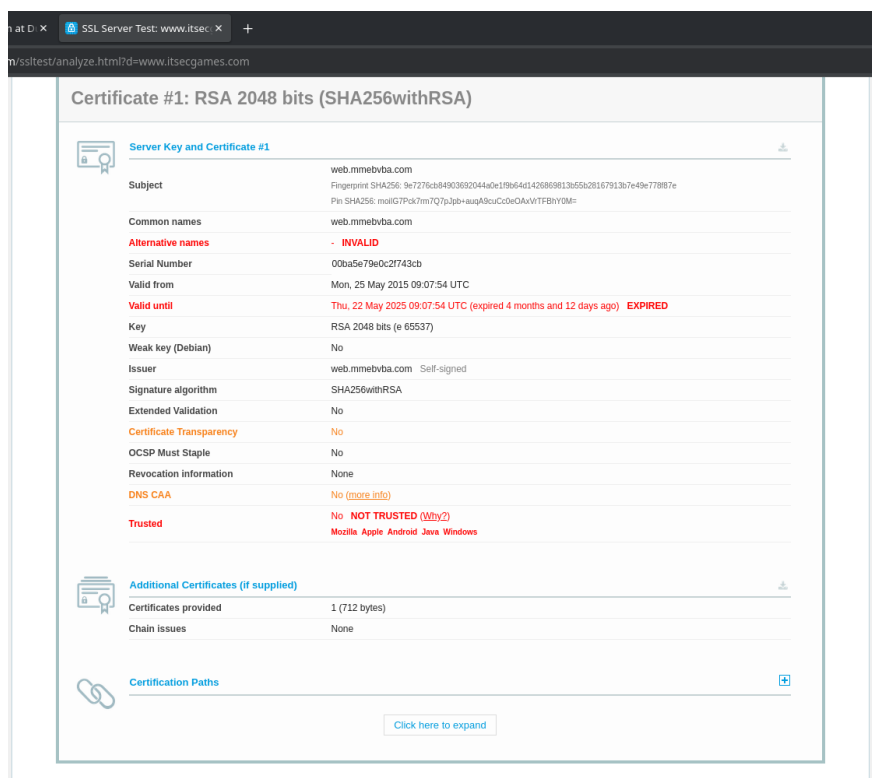
This server's certificate is not trusted, see [below](#) for details.

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

This server does not support TLS 1.3. [MORE INFO »](#)





## Vulnerabilities and Mitigations

Severity	Vulnerability	Reputed Tool	Risk	Mitigation
Medium	Deprecated OpenSSH version 6.7p1, Weak SSH host key and MAC Algorithm	Nmap, OpenVAS	Brute force attacks, Known CVE's	Upgrade to newer OpenSSH version
Low	Exposed CHANGELOG.txt, install.php, MAINTAINERS.txt and other file paths mostly relevant to mmesec.com host in the same ip present in robots.txt, also have no restricted access to their paths	Nmap, Nikto	Leaking web server Technologies and versions	Remove files from webroot and restrict access
High	Deprecated Drupal version 7.69 found on mmesec.com host	Nmap, Nikto	Multiple known exploits	Updating Drupal version
High	Expired Self Signed certificate with outdated TLS versions 1.0 and 1.1 having name mismatch pointing to web.mmebvba.com domain and no forward secrecy	Nmap, OpenVAS, SSL Labs, MX Toolbox, Nikto	Traffic being sent in clear text	Getting a valid certificate from trusted CA with proper domain name
Medium	X-Frame-Options header missing	SecurityHeaders.com	Click Jacking using iframes	Add X-Frame-Options:SAMEORGIN header

Severity	Vulnerability	Reputed Tool	Risk	Mitigation
Medium	X-Content-Type-Options header missing	SecurityHeaders.com, Nikto	MIME Sniffing with spoofed file extentions	Add X-Content-Type-Options:nosniff header
Medium	Referrer-Policy header missing	SecurityHeaders.com, Nikto	sensitive information leakage from URL	Add referrer-Policy header as no-referrer or strict-origin-when-cross-origin
High	E-Tag present in website	Nikto	Server may leak inode number or multipart MIME boundary, which reveals child process IDs (PID)	Disable E-tag
Medium	Content-Security-Policy header missing	OSWAP Zap, SecurityHeaders.com, Nikto	Vulnerability to XSS, CSRF and external code executions	Enable Content-Security-Policy header specifying required sources
Low	HTTP OPTIONS method enabled	Nikto	Can be used to gain information of webserver and its users if Cross-Origin-Resource-Sharing (CORS) is incorrectly configured	Disable OPTIONS and other unwanted methods
Medium	Strict-Transport-Security_Header (HSTS) header missing	OSWAP Zap, Nikto	Vulnerability to cryptographic downgrade attacks	Enable Strict-Transport-Security_Header
Low	DMARC(Domain-based Message Authentication Reporting and Conformance) policy is not enabled	MX Toolbox	vulnerability to email spoofing with the lack of email verification	Setup DMARC for message authentication
Low	Permission-policy header missing	SecurityHeaders.com	Less contol over browser access to API's and features	Setup Permission-Policiy header with required API's and Features
Low	SOA (Start of Authority) Expire Value out of recommended range	MX Toolbox	If primary DNS server fails, Secondary server may stop responding to DNS queries sooner than reccomended	Set recommended SOA expiration retry and refresh values
Low	Internal Active directory name mme-srv-dc1.mme.local found on DNS lookup	MX Toolbox	leaks internal Active directory naming structure	Avoid leaking internal Zones filter DNS and Seperate internal and external DNS