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 permisson to scan domain. The scan result screenshots can be seen in **"Scan Results"** folder for all scans done on the domain.

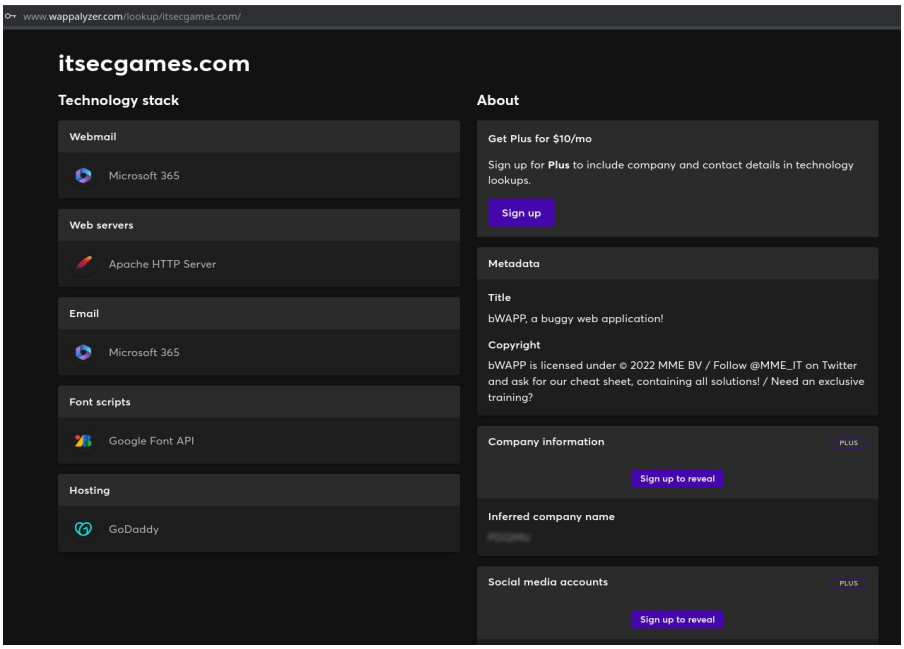
Tools Used For Analysis

- **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

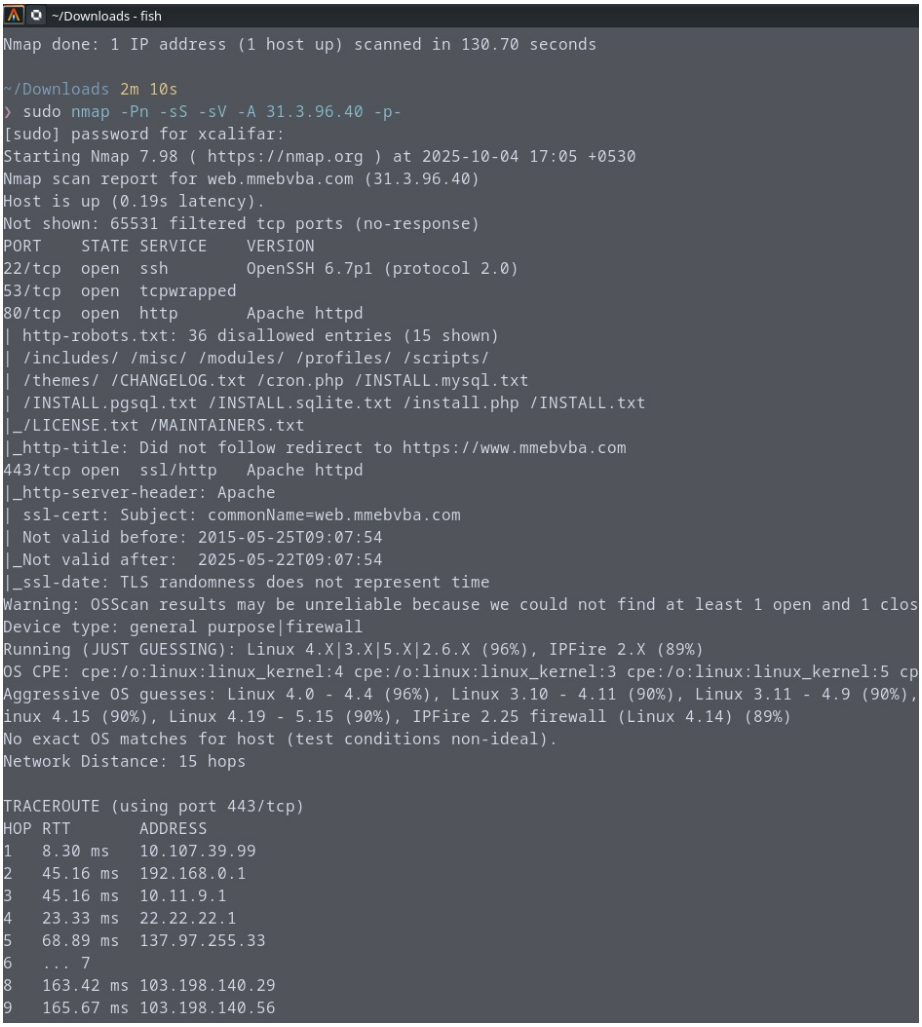
Wappalyzer

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



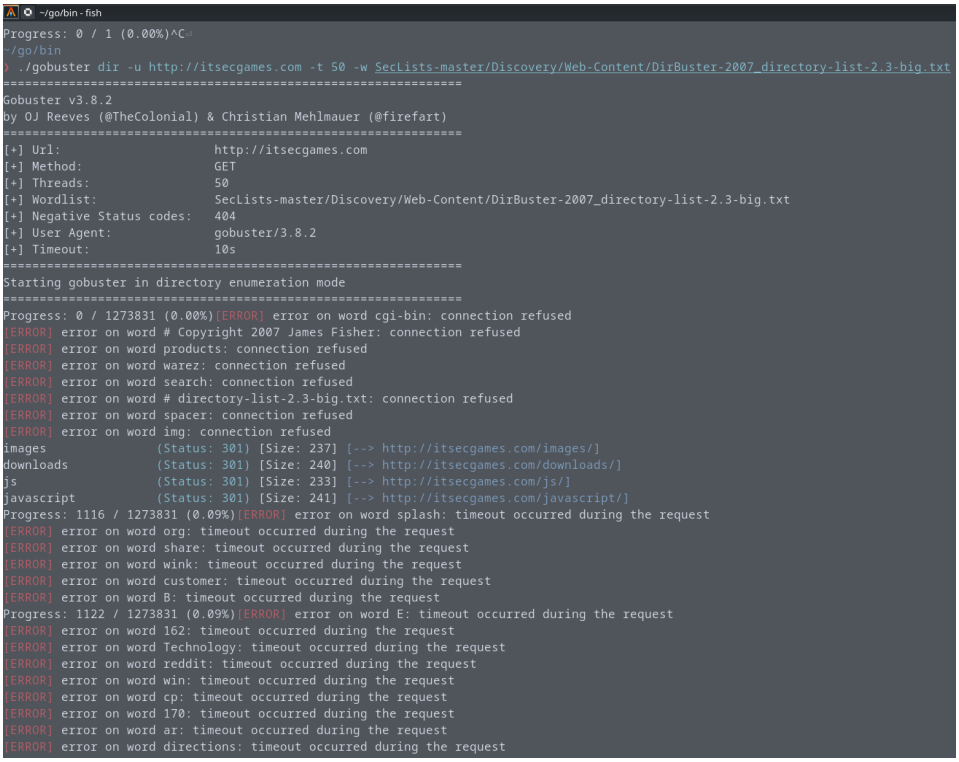
Nmap

- 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- Port 22 is running OpenSSH 6.7p1 which outdated and has vulnerabilities like CVE-2016-0777 and CVE-2018-1547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 muliple critical vulnerabilities like CVE-2020-13663 found in https://mmesec.com domain.
- Found TLS certificate expired on 22-5-2025



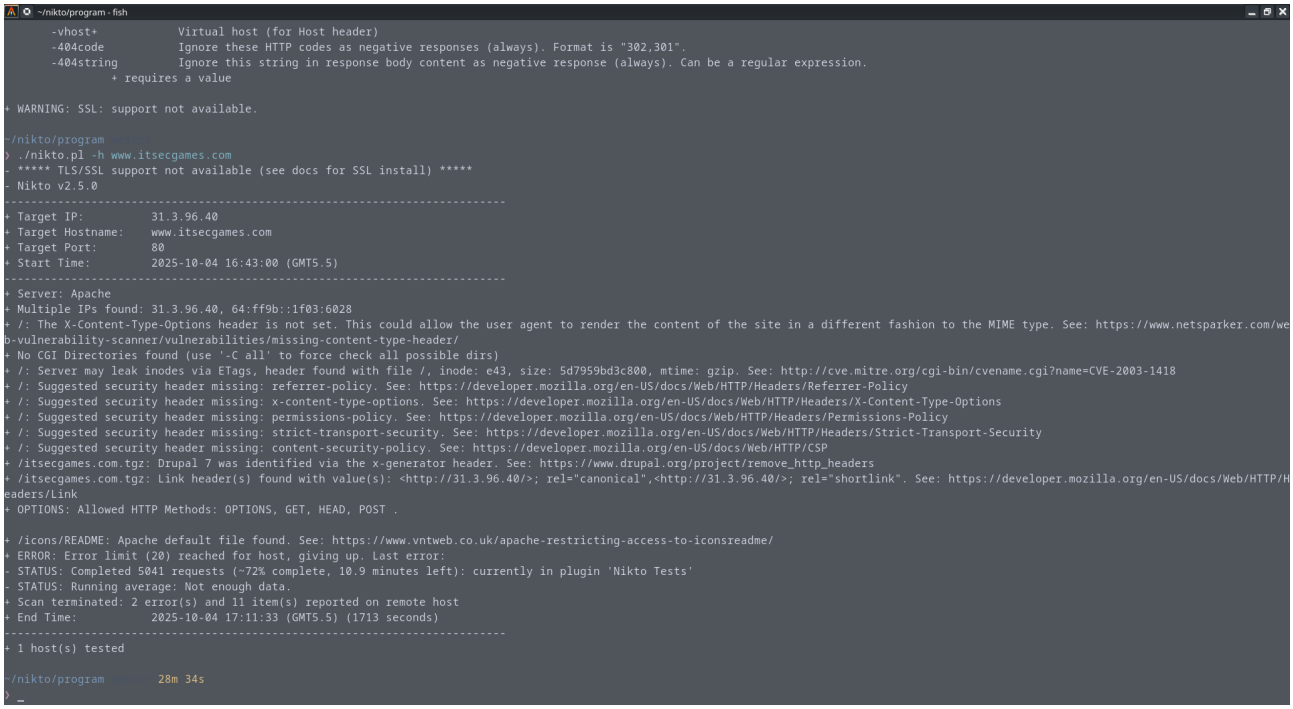
Gobuster

- Found Directories called images, downloads, js and javascrip with resticted access



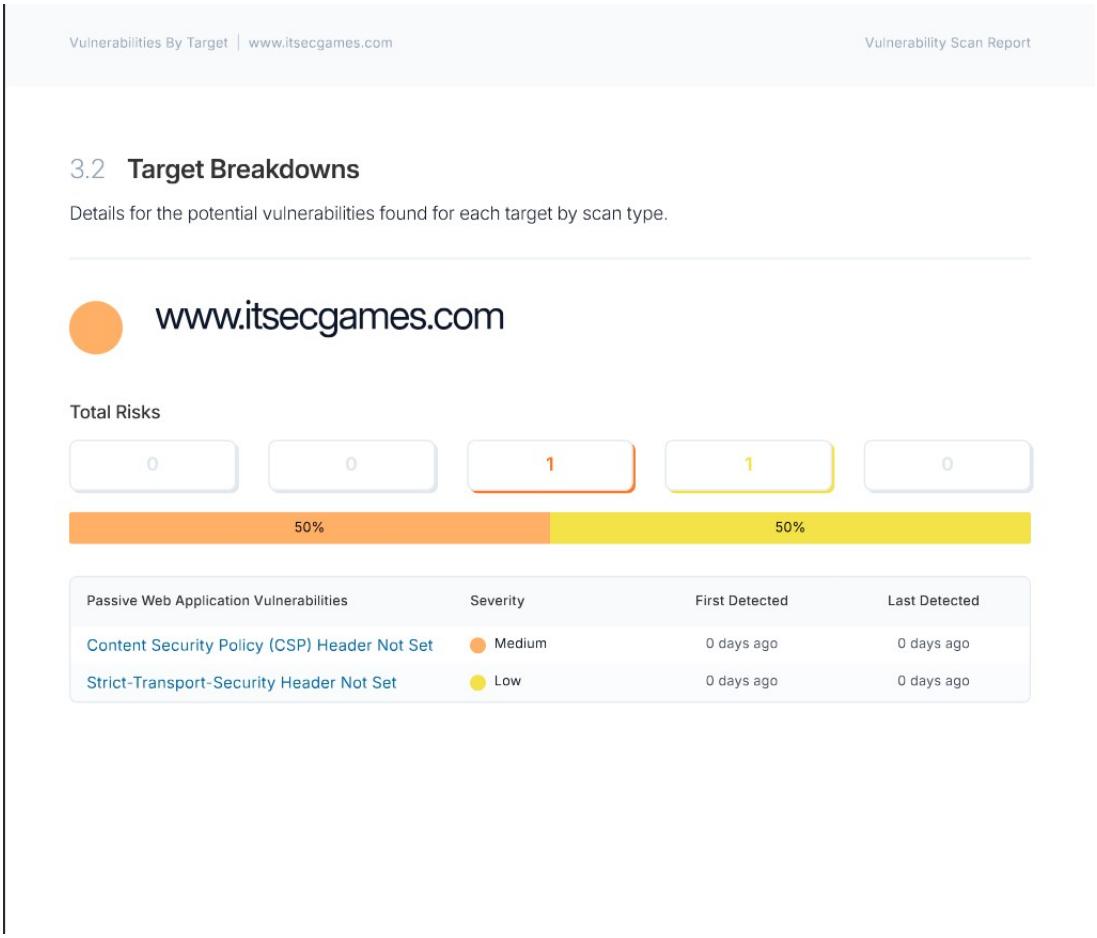
Nikto

- 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 verifiying only whitelisted data are being loaded in the website
- Drupal version 7 was indentified 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-Orgin-Resource-Sharing (CORS) is incorrectly configured.
- Strict-Transport-Security_Header (HSTS) not set which allows downgrade attacks from HTTTPS to HTTP
- No TLS/SSL Support found



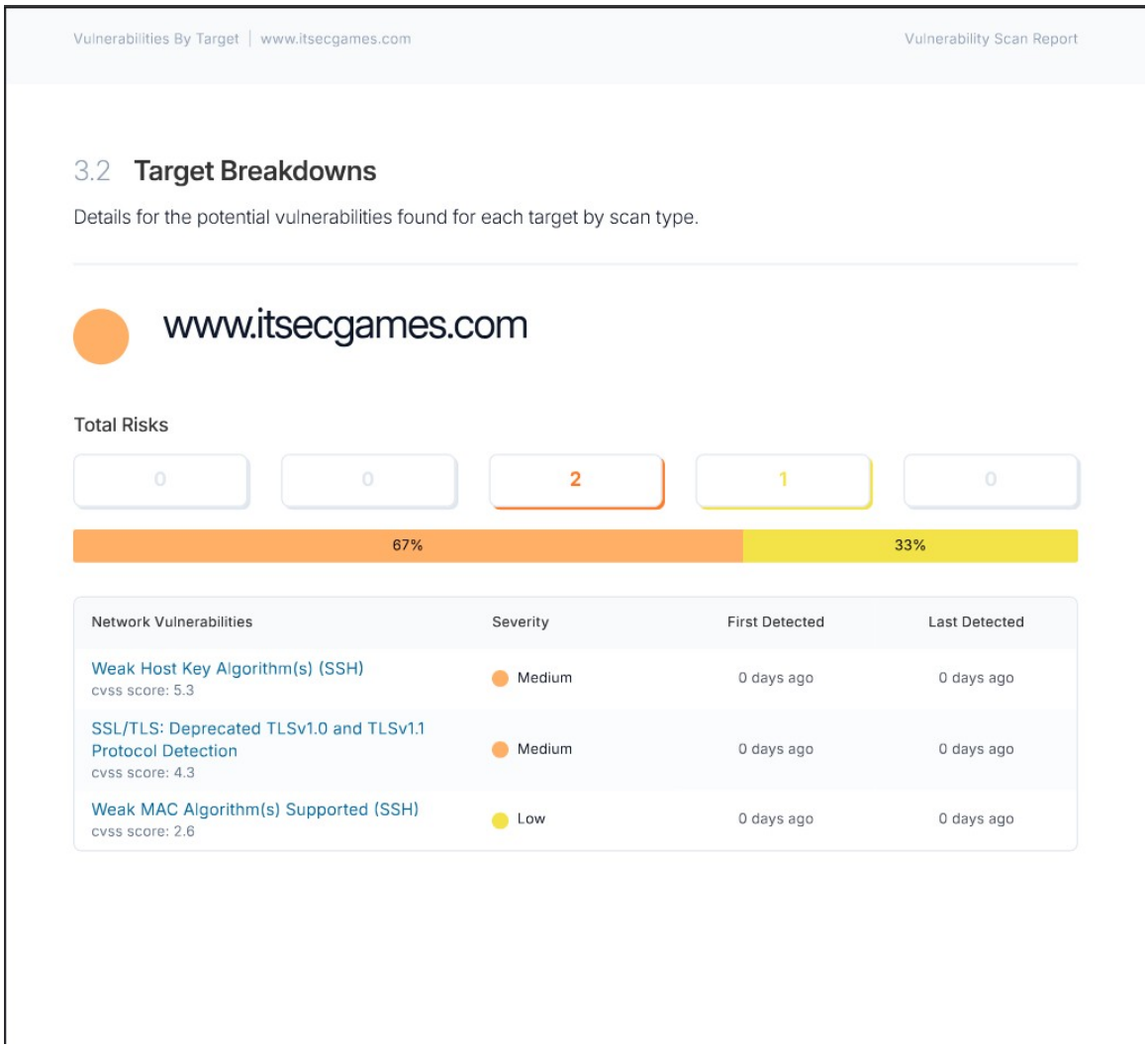
OWASP ZAP *(Hosted scan.com)*

- 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



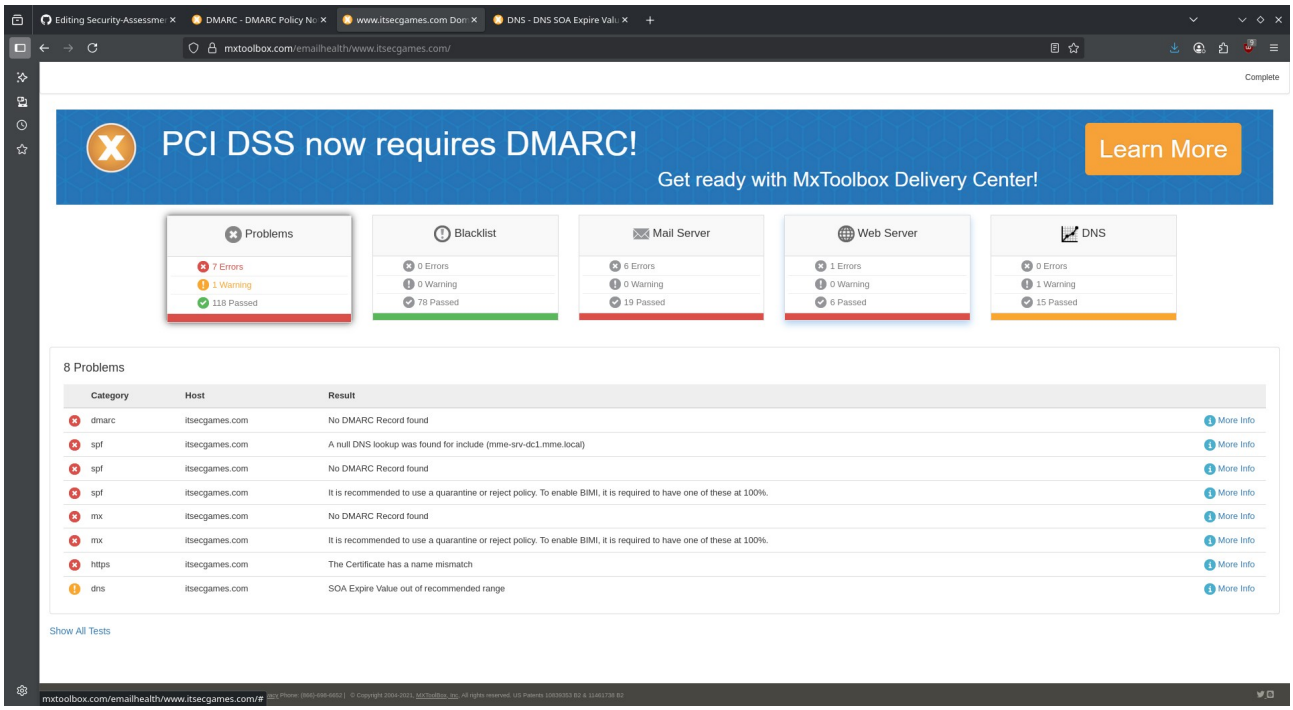
OpenVAS *(Hosted Scan.com)*

- Weak Host Key Algorithm found for SSH which uses ssh-dss (Digital signature algorithm) which is depricated
- Depricated 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



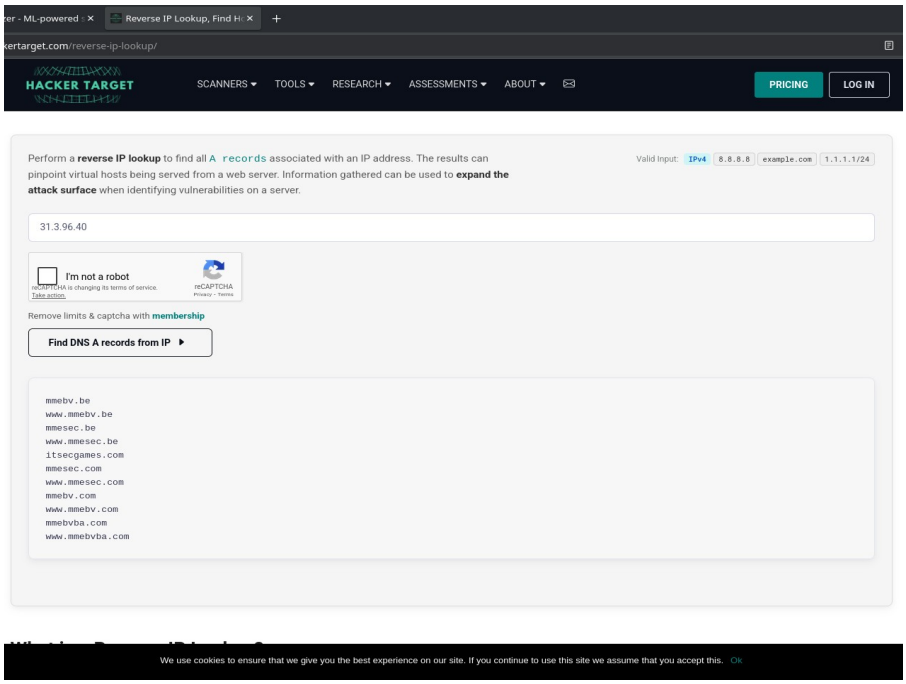
MX Toolbox

- 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 direcory 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 querries sooner than reccomended



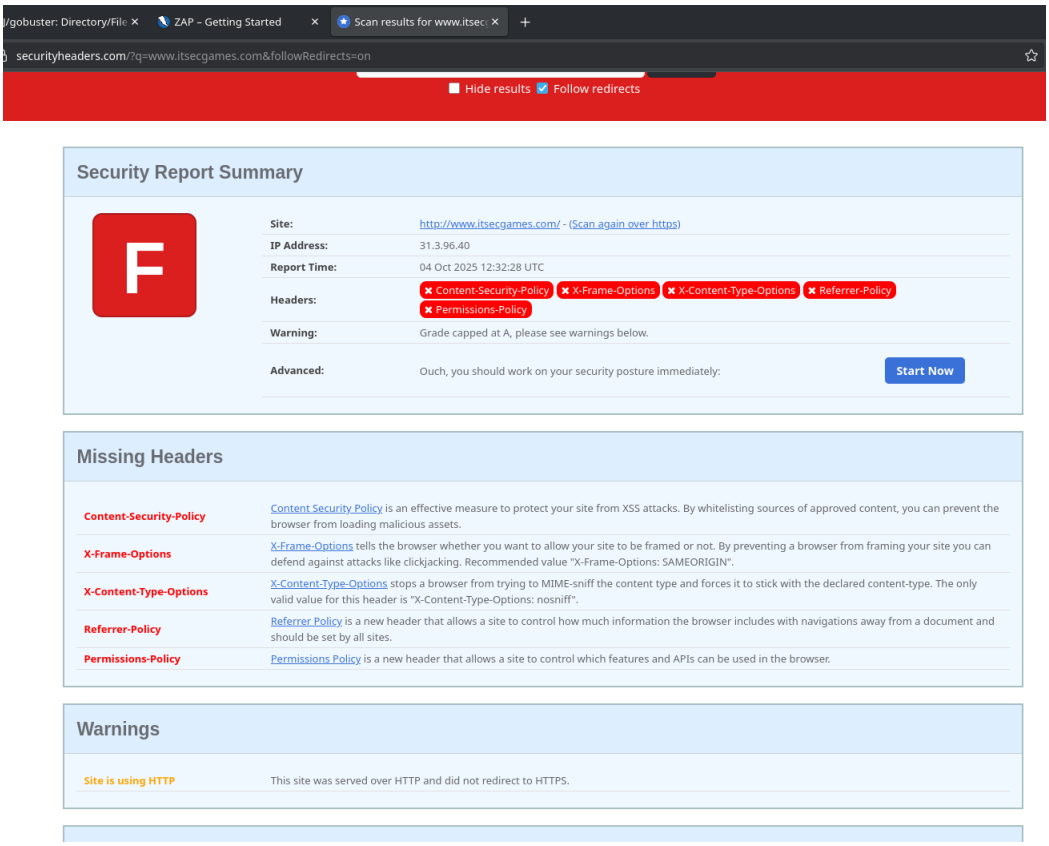
Hacker Target

- Found Multiple hosts on the ip 31.3.96.40 on reverse DNS lookup
    - mmebv.be
    - www.mmebv.be
    - mmesec.be
    - www.mmesec.be
    - itsecgames.com
    - mmesec.com
    - www.mmesec.com
    - mmebv.com
    - www.mmebv.com
    - mmebvba.com
    - www.mmebvba.com



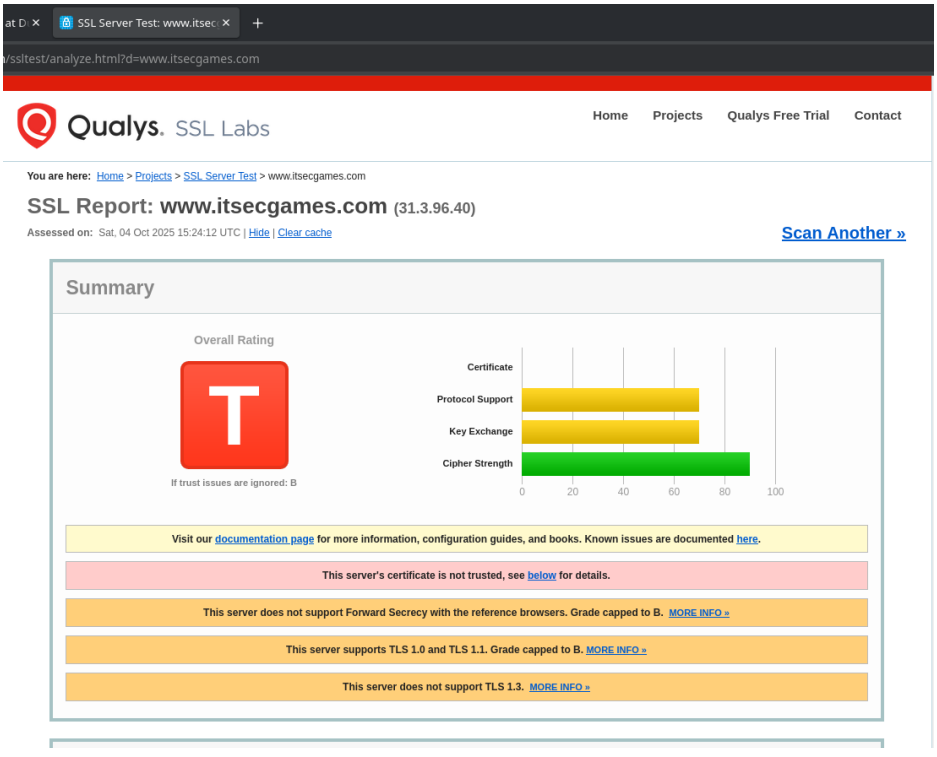
SecurityHeaders.com

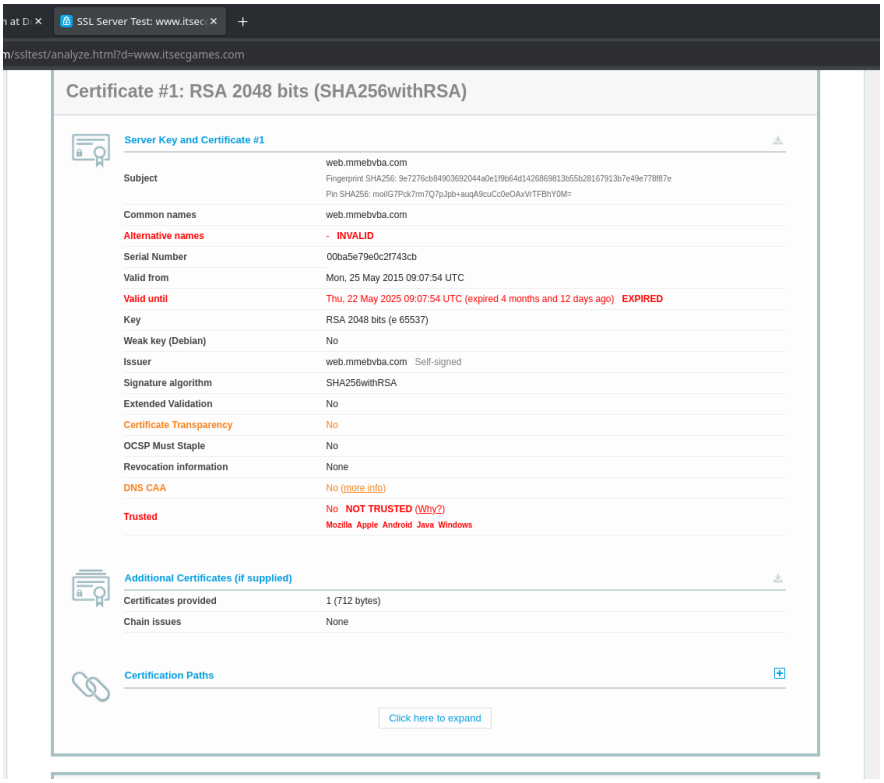
- X-Frame-Options header is not found which makes website vulnerable to clickjacking through i-frames
- Permission-policy header is missing which controls browser access to websites API's and features for more security
- Content-Security-Policy header not found on website which makes it more vulnerable 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.



SSL Labs

- TLS/SSL Certificate name mismatch domain name pointing to domain web.mmebvba.com
- Server dosent support TLS 1.3 only supports depricated 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.





Vulnerabilities and Mitigations

Severity	Vulnerability	Repoted Tool	Risk	Mitigation
Medium	Depricated 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 relevent 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	Depricated Drupal version 7.69 found on mmesec.com host	Nmap, Nikto	Muliple 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	Repoted 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 specifing required sources
Low	HTTP OPTIONS method enabled	Nikto	Can be used to gain information of webserver and its users if Cross-Orgin-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 querries 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 direcory naming structure	Avoid leaking internal Zones filter DNS and Seperate internal and external DNS