Vulnerability Assessment Report

VULNERABILITY DETAILS

VULNERABILITY NAME	SEVERITY	CVSS SCORE
Application is vulnerable to Cross-Site Scripting attack	Medium	5.4 AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Application includes Vulnerable and Outdated Components	Medium	5.1 AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Missing Security Header's and Banners	High	7.0 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N
Weak SSL TLS Cipher suite	High	7.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Server Header Disclosure	Low	3.1 AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Host Header injection	Medium	5.3 AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

The following table lists the OWASP Top 10 vulnerabilities and indicates which issues were identified in the **http://www.itsecgames.com/** application.

CATEGORY	FOUND
A1 - Broken Access Control	No
A2 - Cryptographic Failures	Yes
A3 - Injection	Yes
A4 - Insecure Design	Yes
A5 - Security Misconfiguration	Yes
A6 - Vulnerable and Outdated Components	Yes
A7 - Identification and Authentication Failures	No

Application is Vulnerable to Cross-Site Scripting attack

Cross-site Scripting (XSS) is a client-side code injection attack. The adversary aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The web application help field was affected by cross site scripting.

Tool Used: Wappalyzer chrome extension.

Affected URL/IP: http://www.itsecgames.com/

Severity: Medium

CVSS Score: 5.4 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Business Impact: An adversary can execute code in a victim's browser and can perform malicious activity, posing serious security threat to the application.

Technical Impact: Adversary can affect the web application help field and perform other attacks like social engineering, cookie stealing etc.

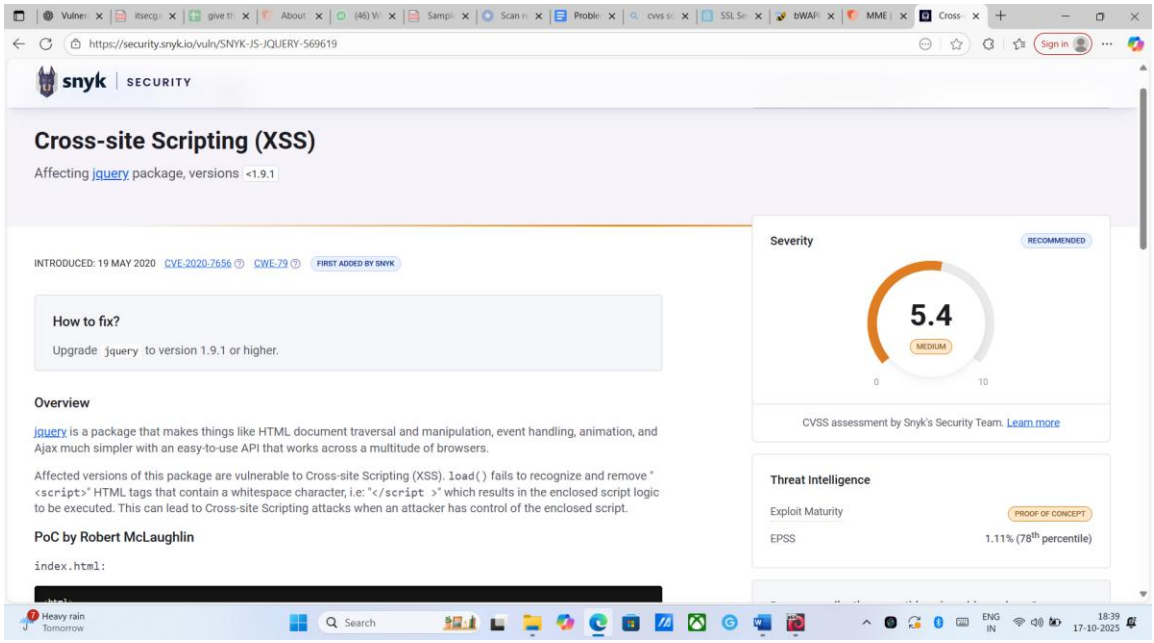
Suggested Remediation: The following recommendations will help to mitigate the risk –

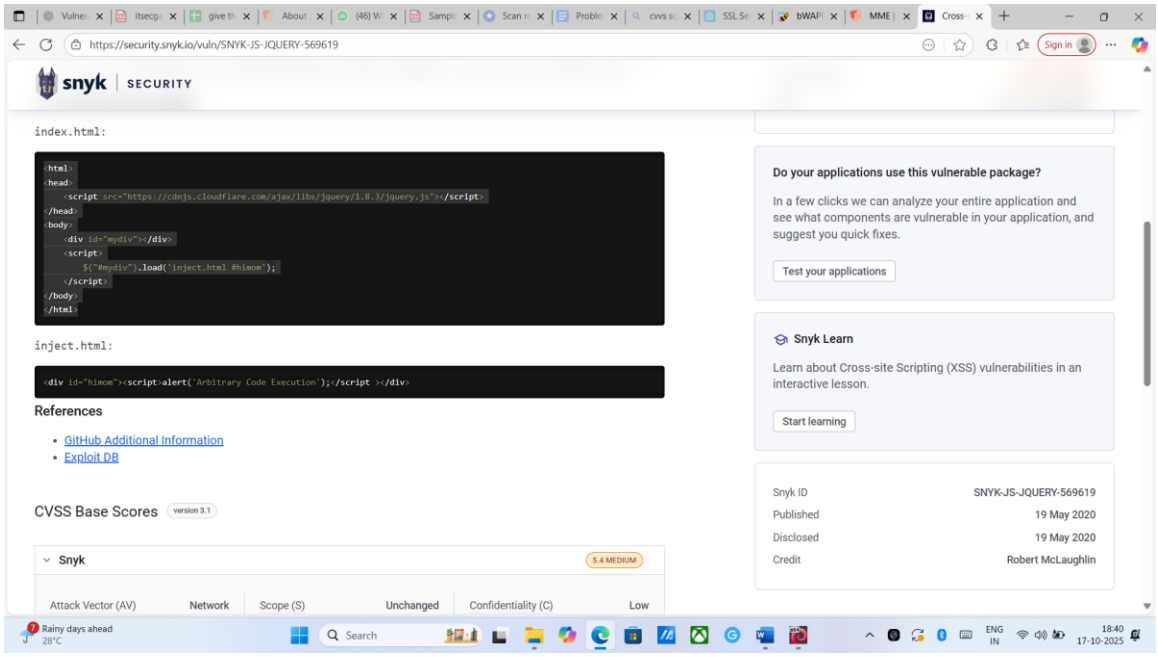
1. **Input Validation** is the practice of checking user input against a strict definition of what is allowed (e.g., only alphanumeric characters, a specific length, etc.).
2. **Input Sanitization** involves cleaning or filtering user input to remove potentially malicious elements, such as <script> tags or JavaScript event handlers.

2. **Output Encoding** is the process of converting potentially dangerous characters into a non-executable, "safe" equivalent before they are rendered in a web page.

3. **A Content Security Policy** (CSP) is a browser-side security layer that helps detect and mitigate certain types of attacks, including XSS and data injection.

4. **Implement HTTPONLY flag in session cookie** HTTPOnly is a crucial flag for session cookie security, but it is not a direct Cross-Site Scripting (XSS) remediation technique. It is an mitigation that limits the damage caused by a successful XSS attack**.**


https://security.snyk.io/vuln/SNYK-JS-JQUERY-569619
snyk | SECURITY
Cross-site Scripting (XSS)
Affecting jquery package, versions <1.9.1
INTRODUCTED: 19 MAY 2020 CVE-2020-7656 CWE-79 FIRST ADDED BY SNYK
How to fix?
Upgrade jquery to version 1.9.1 or higher.
Overview
jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.
Affected versions of this package are vulnerable to Cross-site Scripting (XSS). load() fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >" which results in the enclosed script logic to be executed. This can lead to Cross-site Scripting attacks when an attacker has control of the enclosed script.
PoC by Robert McLaughlin
index.html:
Severity
RECOMMENDED
5.4
MEDIUM
0
10
CVSS assessment by Snyk's Security Team. Learn more
Threat Intelligence
Exploit Maturity
PROOF OF CONCEPT
EPSS
1.11% (78th percentile)
Heavy rain
Tomorrow
Search
ENG
IN
18:39
17-10-2025


https://security.snyk.io/vuln/SNYK-JS-JQUERY-569619
snyk | SECURITY
index.html:
<html>
<head>
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/1.8.3/jquery.js"></script>
</head>
<body>

<script>
$("#mydiv").load('inject.html #himom');
</script>
</body>
</html>
inject.html:
<script>alert('Arbitrary Code Execution');</script >
References
GitHub Additional Information
Exploit DB
CVSS Base Scores
version 3.1
Snyk
5.4 MEDIUM
Attack Vector (AV) Network
Scope (S) Unchanged
Confidentiality (C) Low
Do your applications use this vulnerable package?
In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.
Test your applications
Snyk Learn
Learn about Cross-site Scripting (XSS) vulnerabilities in an interactive lesson.
Start learning
Snyk ID SNYK-JS-JQUERY-569619
Published 19 May 2020
Disclosed 19 May 2020
Credit Robert McLaughlin
Rainy days ahead
28°C
Search
ENG
IN
18:40
17-10-2025

Application includes Vulnerable and Outdated Components

The application is running on **outdated software components** that may contain **known security vulnerabilities**. These outdated libraries, frameworks, or server modules increase the attack surface and can be exploited by attackers using publicly available exploits..

The web application JavaScript Libraries(JQuery 1.5.1) was affected by this issue.

Tool Used: Wappalyzer chrome extension.

Affected URL/IP: http://www.itsecgames.com/

Severity: Medium

CVSS Score: 5.1 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

Business Impact

Using vulnerable and outdated components in the application poses a significant risk to business operations, data integrity, and reputation. Attackers can exploit known flaws in outdated software to compromise the system without needing to discover new vulnerabilities.

Technical Impact

Using outdated or vulnerable components introduces known weaknesses into the application's technology stack. These components may contain publicly disclosed vulnerabilities (CVEs) that attackers can easily exploit to compromise the system.

Suggested Remediation: The following recommendations will help to mitigate the risk

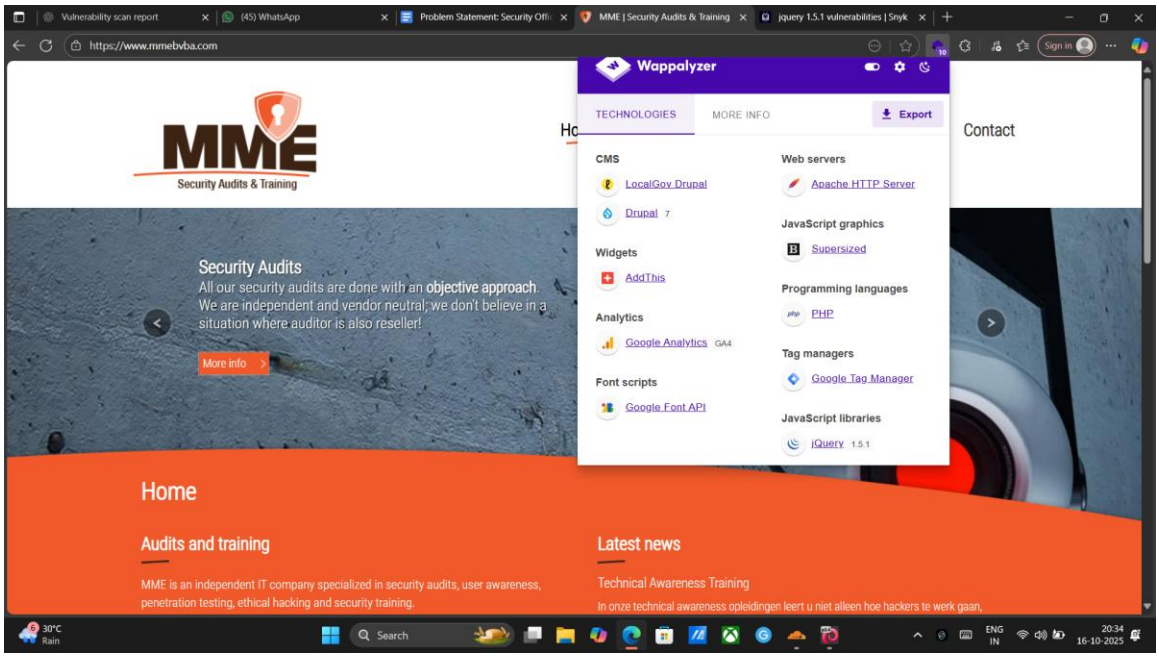
1. Update All Outdated Components.

2. Implement a Component Inventory and Monitoring Process.

3. Remove Unused or Deprecated Components.

4. Strengthen Update and Deployment Practices

5. Improve Cryptographic and Server Configurations



JavaScript libraries

jQuery 1.5.1

Application Missing Security Header's and Banners

The application's HTTP responses are missing several **important security headers and server banner configurations** that help protect against common web-based attacks. Security headers play a vital role in hardening web applications by instructing browsers on how to handle content, reducing the risk of **Cross-Site Scripting (XSS)**, **Clickjacking**, and **MIME-type sniffing** attacks.

Tool Used: https://securityheaders.com (Website)

Affected URL/IP: http://www.itsecgames.com/

Severity: High

CVSS Score: 7.0 (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N)

Business Impact

The absence of key security headers and the exposure of server banners can have a significant impact on the organization's overall security posture. Although these issues may seem low-level or configuration-related, they can indirectly lead to data compromise, reputational harm, and compliance violations if exploited by attackers in conjunction with other vulnerabilities.

Technical Impact

The absence of essential HTTP security headers and the exposure of server banners can lead to multiple technical risks that weaken the security posture of the web application. These configurations help protect users and the application from various client-side and reconnaissance-based attacks.

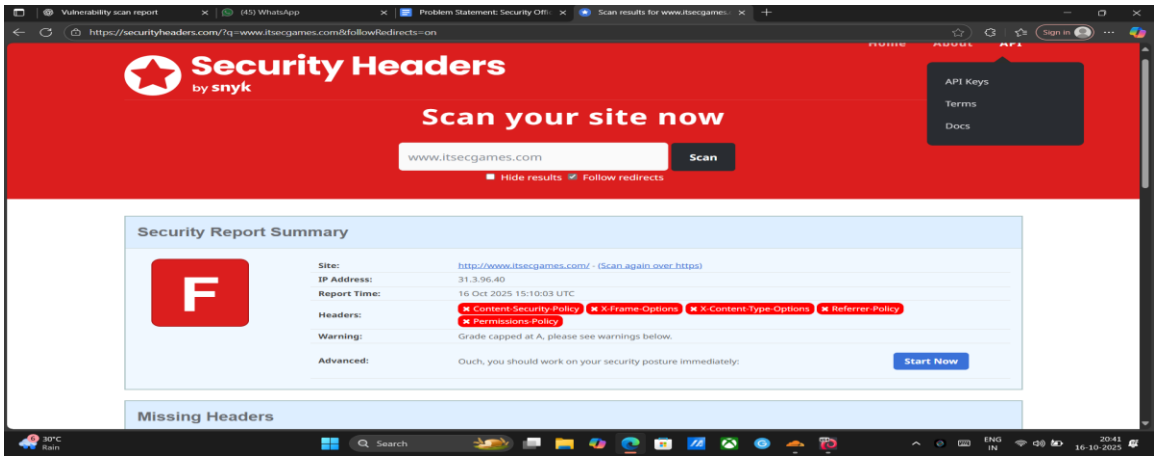
Suggested Remediation: The following recommendations will help to mitigate the risk

1. Implement Essential Security Headers.

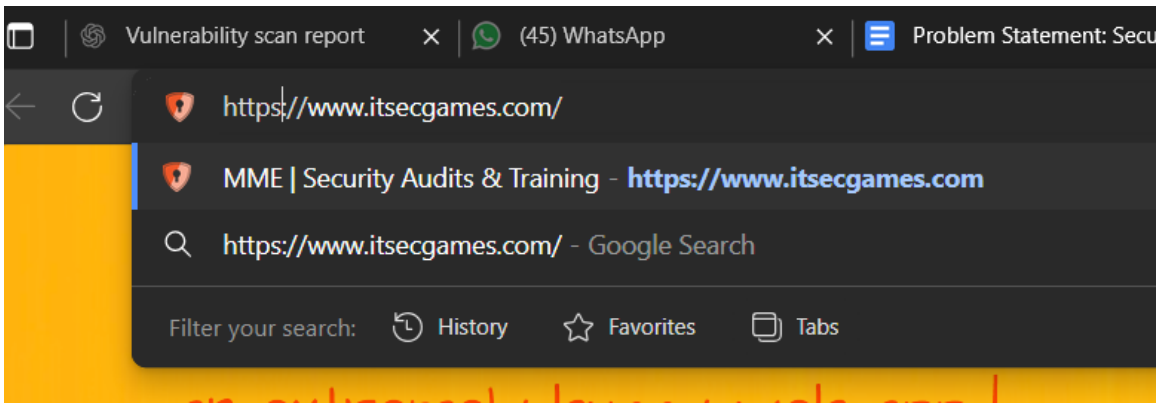
2. Enforce HTTPS Across the Application.

3. Enforce HTTPS Across the Application.

4. Test and Validate Headers.


Security Headers
by snyk
Scan your site now
www.itsecgames.com
Scan
Hide results
Follow redirects
API Keys
Terms
Docs
Security Report Summary
F
Site:
http://www.itsecgames.com/ - (Scan again over https)
IP Address:
31.3.96.40
Report Time:
16 Oct 2025 15:10:03 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


Not secure www.itsecgames.com
bWAPP
an extremely buggy web app !
MME
Home
Bugs
Download
Talks & Training
Blog
/ Home /
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.
What makes bWAPP so unique? Well, it has over 100 web vulnerabilities!
It covers all major known web bugs, including all risks from the OWASP Top 10 project.
bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL. It can also be installed with WAMP or XAMPP.
Another possibility is to download the bee-box, a custom Linux VM pre-installed with bWAPP.
Download our What is bWAPP? introduction tutorial, including free exercises...
bWAPP is for web application security-testing and educational purposes only.
Have fun with this free and open source project!
Cheers, Malik Mesellem
bWAPP is licensed under © 2022 MME BV / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?


Vulnerability scan report
(45) WhatsApp
Problem Statement: Secu
https://www.itsecgames.com/
MME | Security Audits & Training - https://www.itsecgames.com
https://www.itsecgames.com/ - Google Search
Filter your search:
History
Favorites
Tabs

Weak SSL TLS Cipher suite

The application's web server supports **weak or outdated SSL/TLS cipher suites and protocols** that do not provide adequate encryption strength or protection against modern cryptographic attacks. These insecure configurations can allow attackers to **decrypt, manipulate, or intercept sensitive data** transmitted between the client and the server.

Tool Used: https://www.ssllabs.com/ssltest(Website)

Affected URL/IP: http://www.itsecgames.com/

Severity: High

CVSS Score: 7.4 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

Business Impact

The presence of weak or outdated SSL/TLS cipher suites poses a serious risk to the confidentiality and integrity of data exchanged between the web application and its users. If attackers successfully exploit these weaknesses, it can lead to data breaches, loss of customer trust, and potential legal or regulatory penalties.

Technical Impact

The support of weak or deprecated SSL/TLS protocols and cipher suites significantly undermines the security of encrypted communications between the client and the server. Attackers can exploit these weaknesses to compromise the confidentiality, integrity, and authenticity of transmitted data.

Suggested Remediation: The following recommendations will help to mitigate the risk

1. Disable Deprecated Protocols.

2. Use Strong Cipher Suites Only.

3. Enable Perfect Forward Secrecy (PFS).

4. Use a Strong SSL/TLS Certificate.

5. Regularly Test SSL/TLS Configuration**.**

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 4 months and 25 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**

Certificate #2: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	mmebv.be Fingerprint SHA256: e4610949eeaead224d4e39edad971658f39747ed0285164b036b0cbba0b14259 Pin SHA256: 77XOqDT8oAgSOBWYYKlRCPojlEhg3VtziqTv17LgAyk=
Common names	mmebv.be
Alternative names	mmebv.be mmebv.com mmebvba.com mmesec.be mmesec.com www.mmebv.be www.mmebv.com www.mmebvba.com www.mmesec.be www.mmesec.com **MISMATCH**
Serial Number	05edaf58b09fd6823687e53f6c6caa4636c3
Valid from	Sun, 05 Oct 2025 09:59:50 UTC
Valid until	Sat, 03 Jan 2026 09:59:49 UTC (expires in 2 months and 16 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R13 AIA: http://r13.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL CRL: http://r13.c.lencr.org/68.crl
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	No **NOT TRUSTED** (Why?) **Mozilla Apple Android Java Windows**

Server Header Disclosure

The web application discloses **server information and version details** in its HTTP response headers. This information typically appears in fields such as Server, X-Powered-By, or X-AspNet-Version. it was observed that the application's HTTP responses include detailed server and technology information (e.g., Server: Apache/2.4.38 (Debian) or X-Powered-By: PHP/7.4.3). Exposing these details provides valuable insights to attackers during the **reconnaissance phase**, helping them identify specific software versions and potential vulnerabilities associated with them.

Tool Used: PortSwigger Burp Suite.

Affected URL/IP: http://www.itsecgames.com/

Severity: Low

CVSS Score: 3.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

Business Impact

The exposure of detailed server information and version numbers through HTTP headers can have a **significant impact on the organization's overall security posture**. While this issue may appear low in isolation, it provides **valuable intelligence to attackers**, enabling them to identify and exploit specific weaknesses in the organization's technology stack.

Technical Impact

The disclosure of detailed server and technology information through HTTP response headers allows attackers to **accurately fingerprint the application's backend environment**. This information is highly valuable during the **reconnaissance phase** of an attack, as it helps identify potential vulnerabilities specific to the disclosed software versions.

Suggested Remediation: The following recommendations will help to mitigate the risk

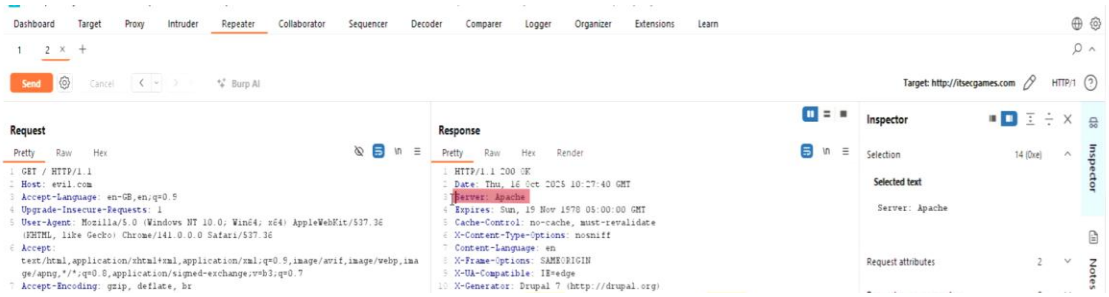
1. Disable or Modify Server Identification Headers

2. Use a Reverse Proxy or Web Application Firewall (WAF)

3. Remove Framework or Platform Disclosure

4. Regular Security Header Review

5. Apply Principle of Minimal Disclosure


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
1
2
Send
Cancel
Burp AI
Target: http://itsecgames.com
HTTP/1
Request
Pretty
Raw
Hex
GET / HTTP/1.1
Host: evil.com
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Date: Thu, 16 Oct 2025 10:27:40 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Inspector
Selection
14 (0xe)
Selected text
Server: Apache
Request attributes
2
Inspector
Notes

Host Header injection

Host Header Injection occurs when an application uses the incoming Host HTTP header in a security-sensitive context (URL generation, password resets, redirects, or logging) without proper validation. An attacker can supply a malicious Host value to manipulate links, cause cache poisoning, bypass access controls, or craft malicious emails and password-reset links that point to attacker-controlled domains.

Tool Used: PortSwigger Burp Suite.

Affected URL/IP: http://www.itsecgames.com/

Severity: Medium

CVSS Score: 5.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

Business Impact

Exploitation of a Host Header Injection vulnerability can have serious business and reputational consequences. Although it may seem like a low-level technical flaw, its impact can escalate significantly when the application uses the Host header for generating dynamic links, password reset URLs, or security tokens.

Technical Impact

A **Host Header Injection** vulnerability allows an attacker to manipulate the Host HTTP header, which the application uses for generating URLs, redirects, or security-sensitive operations, without proper validation. This misconfiguration can lead to multiple **technical security issues** and facilitate more advanced attacks..

Suggested Remediation: The following recommendations will help to mitigate the risk

1. Validate Host Header Against a Whitelist**.**

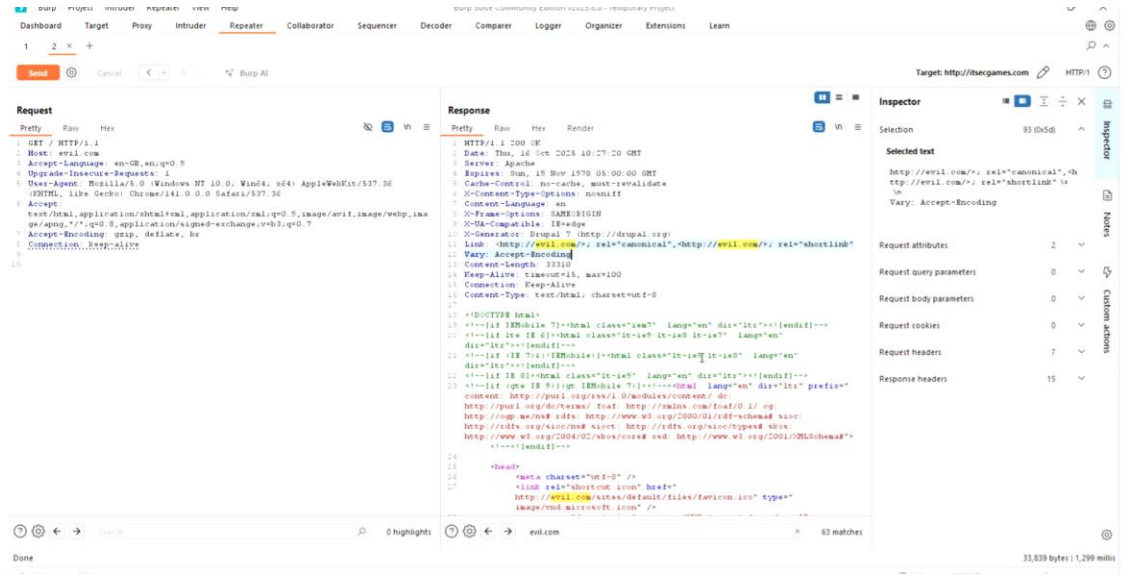
2. Use Application-Configured Base URLs**.**

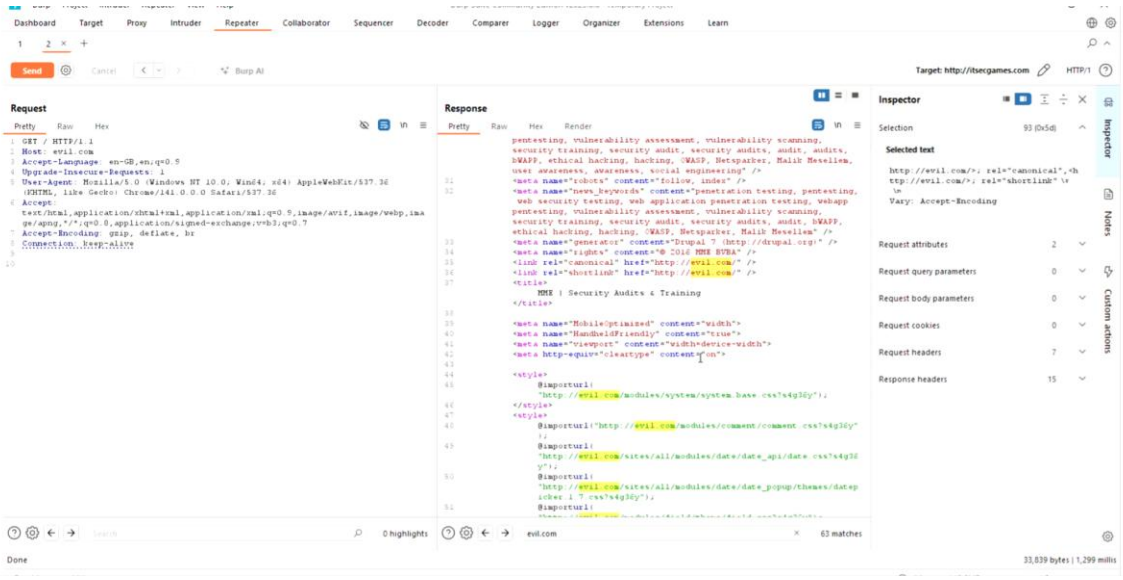
3. Sanitize and Canonicalize Input**.**

4. Secure Reverse Proxies and CDNs**.**

5. Monitor and Log Suspicious Requests.

6. Test and Verify Remediation.


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Send
Cancel
Burp AI
Target: http://itsecgames.com
HTTP/1
Request
Pretty
Raw
Hex
GET / HTTP/1.1
Host: evil.com
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Response
Render
HTTP/1.1 200 OK
Date: Thu, 16 Oct 2025 10:27:20 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <http://evil.com/>; rel="canonical",<http://evil.com/>; rel="shortlink"
Vary: Accept-Encoding
Content-Length: 33310
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
<!DOCTYPE html>
<!--[if IEMobile 7]><html class="iem7" lang="en" dir="ltr"><![endif]-->
<!--[if lte IE 6]><html class="lt-ie9 lt-ie8 lt-ie7" lang="en"
dir="ltr"><![endif]-->
<!--[if (IE 7)&(!IEMobile)]><html class="lt-ie9 lt-ie8" lang="en"
dir="ltr"><![endif]-->
<!--[if IE 8]><html class="lt-ie9" lang="en" dir="ltr"><![endif]-->
<!--[if (gte IE 9)|(gt IEMobile 7)]><!--><html lang="en" dir="ltr" prefix="
content: http://purl.org/rss/1.0/modules/content/ dc:
http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og:
http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc:
http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos:
http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#">
<!--<![endif]-->
<head>
<meta charset="utf-8" />
<link rel="shortcut icon" href="
http://evil.com/sites/default/files/favicon.ico" type="
image/vnd.microsoft.icon" />
Inspector
Selection
93 (0x5d)
Selected text
http://evil.com/>; rel="canonical",<h
ttp://evil.com/>; rel="shortlink" \r
\n
Vary: Accept-Encoding
Request attributes
2
Request query parameters
0
Request body parameters
0
Request cookies
0
Request headers
7
Response headers
15
Inspector
Notes
Custom actions
0 highlights
evil.com
63 matches
Done
33,839 bytes | 1,299 millis


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Send
Cancel
Burp AI
Target: http://itsecgames.com
HTTP/1
Request
Pretty
Raw
Hex
GET / HTTP/1.1
Host: evil.com
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Response
Render
pentesting, vulnerability assessment, vulnerability scanning,
security training, security audit, security audits, audit, audits,
bWAPP, ethical hacking, hacking, OWASP, Netsparker, Malik Mesellem,
user awareness, awareness, social engineering" />
<meta name="robots" content="follow, index" />
<meta name="news_keywords" content="penetration testing, pentesting,
web security testing, web application penetration testing, webapp
pentesting, vulnerability assessment, vulnerability scanning,
security training, security audit, security audits, audit, bWAPP,
ethical hacking, hacking, OWASP, Netsparker, Malik Mesellem" />
<meta name="generator" content="Drupal 7 (http://drupal.org)" />
<meta name="rights" content="© 2018 MME BVBA" />
<link rel="canonical" href="http://evil.com/" />
<link rel="shortlink" href="http://evil.com/" />
<title>
MME | Security Audits & Training
</title>
<meta name="MobileOptimized" content="width">
<meta name="HandheldFriendly" content="true">
<meta name="viewport" content="width=device-width">
<meta http-equiv="cleartype" content="on">
<style>
@import url(
"http://evil.com/modules/system/system.base.css?s4g36y");
</style>
<style>
@import url("http://evil.com/modules/comment/comment.css?s4g36y"
);
@import url(
"http://evil.com/sites/all/modules/date/date_api/date.css?s4g36
y");
@import url(
"http://evil.com/sites/all/modules/date/date_popup/themes/datep
icker.1.7.css?s4g36y");
@import url(
Inspector
Selection
93 (0x5d)
Selected text
http://evil.com/>; rel="canonical",<h
ttp://evil.com/>; rel="shortlink" \r
\n
Vary: Accept-Encoding
Request attributes
2
Request query parameters
0
Request body parameters
0
Request cookies
0
Request headers
7
Response headers
15
Inspector
Notes
Custom actions
0 highlights
evil.com
63 matches
Done
33,839 bytes | 1,299 millis

NMAP Vulnerability Scan Report — itsecgames.com

Executive summary:

A network-level assessment identified several service exposures and misconfigurations: Critical: Exposed database service (MySQL/MariaDB) on TCP/3306. Medium: Weak TLS/SSL configuration and support for outdated ciphers/protocols on HTTPS. Low/Medium: Server version disclosure (Apache 2.4.x) visible in headers. Other: Open/filtered SSH and general exposure of HTTP/HTTPS.

Methodology (recommended commands)-

Host & port discovery: nmap -sS -Pn -p- itsecgames.com – Service/version and default scripts: nmap -sV -sC -p 22,80,443,3306 itsecgames.com - TLS/SSL enumeration: nmap--script ssl-enum-ciphers -p 443 itsecgames.com - MySQL checks: nmap --script mysql info,mysql-empty-password -p 3306

Findings

Finding A — Exposed database service (TCP/3306): Severity: Critical/High Description: TCP port 3306 reported open and serving MySQL/MariaDB. Internet-accessible DB servers risk data theft and exploitation. Recommended remediation: • Block port 3306 at the perimeter; restrict access to management hosts or VPN only. • Use bastion hosts/SSH tunnels or VPN for remote DB access. • Update DB engine, enforce strong passwords, disable remote root, audit accounts.

Finding B — Weak TLS/SSL ciphers (HTTPS / 443): Severity: Medium Description: TLS service may allow weak ciphers or older protocol versions (TLS1.0) as reported by ssl-enum ciphers. Recommended remediation: • Support TLS 1.2 and TLS 1.3 only; remove weak ciphers (3DES, RC4). • Use ECDHE key exchange and AEAD ciphers; enable HSTS. • Test with SSL Labs or testssl.sh.

Finding C — Server version disclosure (Apache 2.4.x): Severity: Low/Medium Description: HTTP headers reveal server and likely Apache 2.4.x; this aids attacker fingerprinting. Recommended remediation: • Hide/generalize Server header (ServerTokens Prod; ServerSignature Off), or strip via proxy/WAF. • Patch Apache and OS packages.

Finding D — SSH open/filtered (22): Severity: Medium Description: SSH reachable or filtered; remote management service must be hardened. Recommended remediation: • Restrict SSH to management IPs or use bastion/VPN. • Enforce key-based auth, disable password auth and root login; use fail2ban

Risk prioritization & remediation roadmap Immediate (24–72h): • Block inbound 3306; enforce strong DB credentials. Short-term (1–2 weeks): • Harden TLS, remove weak ciphers, enable HSTS; hide server headers; restrict SSH. Medium-term (2–6 weeks): • Patch/upgrade Apache, MySQL, OS; run full authenticated scans. Long-term (1–3 months):

```
└─$ nmap -sV -sC -p 22,80,443,3306 itsecgames.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 09:21 IST
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.060s latency).
rDNS record for 31.3.96.40: web.mmebvba.com

PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 6.7p1 (protocol 2.0)
| ssh-hostkey:
|   1024 cc:27:db:28:f4:85:35:8d:b9:a6:5f:81:93:3e:ef:5a (DSA)
|   2048 ba:84:0f:0a:52:7e:e8:59:6f:e7:5c:d6:e2:b1:b8:c6 (RSA)
|   256 9e:d1:3d:1f:19:26:ea:5d:44:2d:56:58:86:58:89:5a (ECDSA)
|_  256 5e:12:90:7b:68:ac:e2:e2:53:37:d1:b5:ac:3c:de:af (ED25519)
80/tcp   open     http     Apache httpd
|_http-title: bWAPP, a buggy web application!
443/tcp  open     ssl/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
| ssl-cert: Subject: commonName=web.mmebvba.com
| Not valid before: 2015-05-25T09:07:54
|_Not valid after:  2025-05-22T09:07:54
3306/tcp filtered mysql

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.78 seconds
```