MIRA BHAYANDAR MUNICIPAL CORPORATION

Pharmacy Management System Module

Web Application

Report Release Date	February 19, 2026
Type of Audit	Application Security Assessment
Type of Audit Report	First Audit Report
Period	February 17, 2026 to February 18, 2026

Document Control

Document Preparation	
Document Title	VAPT Report of Pharmacy Management System Module Web Application
Document ID	A3S/MBMC/ Pharmacy Management System Module /2526/00014
Document Version	1.0
Prepared by	Jasmeet Singh
Reviewed by	Sagar Gupta
Approved by	Sagar Gupta
Released by	Jasmeet Singh
Release date	February 19, 2026

Document Change History

Version	Date	Remarks / Reason of change
1.0	February 19, 2026	New Report

Document Distribution List

Name	Organization	Designation	Email Id
Mr. Raj Gharat	Mira Bhayandar Municipal Corporation	System Manager	it@mbmc.gov.in

SAGAR GUPTA

Digitally signed by SAGAR GUPTA
Date: 2026.02.20 14:50:43 +05'30'

Contents

Table of Contents

1. Introduction

A3S Tech & Co. (A3S) was engaged by Mira Bhayandar Municipal Corporation to perform VAPT, for Pharmacy Management System Module Web Application. The report highlights gaps identified during the review and recommendations to remediate the gaps.

The objective of Web Application VAPT was to provide independent evaluation of the vulnerabilities in scope to fulfil the objectives of confidentiality, integrity, and availability and to perform controlled attack to assess the immunity level, to assess the overall level of security, discover weak links and provide recommendations and compliance status to vulnerable entities discovered. The report highlights gaps identified during the VAPT review, recommendations, risk ratings and impact of the vulnerabilities.

2. Engagement Scope

Below are the details of assets covered in the scope:

S. No.	Asset Description	Criticality of Asset	Internal IP Address	URL	Public IP Address	Location	Hash Value (in case of applications)	Version (in case of applications)	Other details such as make and model in case of network devices or security devices.
1.	Web Application – Pharmacy Management System Module	Not available	Not Available	Hmisdev.mbmconline.in	Not Available	MUMBAI	Not available	Not available	Not Applicable

3. Details of the Auditing team

S. no.	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshot information published on CERT-In's website (Yes/No)
1.	Jasmeet Singh	Senior IS Consultant	jasmeet@a3stech.co.in	CEH	Yes

4. Audit Activities and Timelines

The audit was conducted in the following phases:

S. no.	Audit Activity	Timeline
1.	Information Gathering	February 17, 2026
2.	Scanning	February 18, 2026
3.	Information Analysis	February 18, 2026
4.	Vulnerability Assessment	February 18, 2026
5.	Penetration Testing	February 18, 2026
6.	Revalidation Testing	NA

5. Audit Methodology and Criteria / Standard referred for audit

The Audit Approach and Methodology was a Risk based Audit Approach. In a risk-based audit approach, IS auditors are not just relying on risk; they also are also relying on internal and operational controls as well as knowledge of the organization and its business. The audit was conducted based on combination of tools and manual testing. The audit methodology and approach are based on global best practice framework such as OWASP Top 10 Vulnerabilities, OSSTMM, SANS 25, CIS benchmarks. These are globally accepted standard and a benchmark for IT security across a large number of organizations.

List of OWASP vulnerabilities (Web Application) is:

S. no	Attack Type	Description
1.	A1- Broken Access Control	Improperly configured or missing restrictions on authenticated users allow them to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive documents, and modifying data and access rights
2.	A2- Cryptographic Failures	Applications and APIs that don't properly protect sensitive data such as financial data, usernames and passwords, or health information, could enable attackers to access such information to commit fraud or steal identities.
3.	A3- Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data
4.	A4- Insecure Design	Insecure design is a broad category representing different weaknesses, expressed as "missing or

S. no	Attack Type	Description
		ineffective control design". An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.
5.	A5- Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application
6.	A6- Vulnerable and Outdated Components	Developers frequently don't know which open source and third-party components are in their applications, making it difficult to update components when new vulnerabilities are discovered. Attackers can exploit an insecure component to take over the server or steal sensitive data.
7.	A7- Identification and Authentication Failures	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities
8.	A8- Software and Data	Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code,

S. no	Attack Type	Description
	Integrity Failures	or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations
9.	A9- Security Logging and Monitoring Failures	The time to detect a breach is frequently measured in weeks or months. Insufficient logging and ineffective integration with security incident response systems allow attackers to pivot to other systems and maintain persistent threats
10.	A10- Server-Side Request Forgery	SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

This document is an exception report highlighting the vulnerabilities and their compliance status.

Our review has been based on the assumption that the information provided to us was accurate and complete, as existing at the time of review, and that all relevant information, system access for review, and supporting documents, as asked for by A3S, were shared with us for the area that was subject of the review.

6. Tools/ Software used

S. no.	Name of Tool/Software used	Version of the tool /Software used	Open Source/Licensed
1.	Burp Suite	2025.12.5	Licensed

7. Executive Summary

The details of the vulnerabilities identified during the testing as mentioned as below:

S. No.	Affected Asset i.e. IP/URL/Application etc.	Observation/Vulnerability title	CVE/CWE	Severity	Recommendation	Reference	New or Repeat observation
1	Hmisdev.mbmconline.in	Missing Security Headers	CWE-693	**Medium**	It is recommended to configure and enable the required HTTP security headers at the web server or application level. At a minimum, implement the following: Content-Security-Policy: default-src 'self'; X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 ; includeSubDomains Referrer-Policy: no-referrer Permissions-Policy:	https://www.invicti.com/blog/web-security/missing-http-security-headers	New

					geolocation=(), camera=(), microphone=() X-Frame-Options: DENY		
2	Hmisdev.mbmconline.in	Out of date (ASP.NET Version)	CWE-200	**Medium**	Upgrade the application to the latest supported and fully patched version of ASP.NET / .NET Framework (4.8.1). Apply all relevant Microsoft security updates. Remove or suppress the X-AspNet-Version and X-Powered-By headers from HTTP responses to prevent version disclosure.	https://cwe.mitre.org/data/definitions/200.html	New
3	Hmisdev.mbmconline.in	Clear Text OTP Transmission in Login Request	CWE-319	**Medium**	It is strongly recommended to: Enforce HTTPS (TLS 1.2 or higher) across the application. Avoid transmitting passwords in clear text. Implement secure encryption mechanisms for data in transit. Ensure passwords are hashed and	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	New

					salted on the server side. Disable login access over HTTP. Use secure authentication frameworks (OAuth, SSO, etc.). Implement short OTP expiration and one-time use validation.		
4	Hmisdev.mbmconline.in	Out of Date (BootStrap Version)	CWE-200	**Medium**	Upgrade Bootstrap to the latest stable and supported version (Bootstrap 5.3.8). Remove deprecated Bootstrap 3 components and ensure all dependent libraries are compatible with the updated version. Regularly update third-party libraries to mitigate known vulnerabilities.	https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/	New
5	Hmisdev.mbmconline.in	Out of Date (jQuery Version)	CWE-200 CWE-937	**Medium**	• Upgrade jQuery to the latest stable version (jQuery 4.0.0). • Review application compatibility before upgrading.	https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/	

					• Implement dependency management and regular vulnerability scanning. • Remove unused or legacy libraries from the application.		
6	Hmisdev.mbmconline.in	Improper Input Validation	CWE-20	**Medium**	Implement strict server-side input validation for all user-supplied fields by applying allow-list based validation. Encode or sanitize special characters before processing or rendering user input. Additionally, implement output encoding, centralized input validation logic, and proper exception handling to prevent script execution and error disclosure.	https://cwe.mitre.org/data/definitions/20.html	New
7	Hmisdev.mbmconline.in	Improper Input Validation (Missing Input Length	CWE-20	**Medium**	Implement strict server-side input validation for all user-supplied fields by applying	https://cwe.mitre.org/data/definitions/20.html	New

		Validation)			allow-list based validation. Encode or sanitize special characters before processing or rendering user input. Additionally, implement output encoding, centralized input validation logic, and proper exception handling to prevent script execution and error disclosure. Implement strict, server-side validation that enforces explicit minimum and maximum lengths for all inputs		
8	Hmisdev.mbmconline.in	Version Disclosure (jQuery)	CWE-200	**Low**	Upgrade to the latest stable jQuery version (4.0.0). Remove unused libraries. Implement dependency management and regular patching. Consider Subresource Integrity (SRI) and Content	https://owasp.org/www-community/attacks/Information_Disclosure	New

					Security Policy (CSP).		
9	Hmisdev.mbmconline.in	Version Disclosure (BootStrap)	CWE-200	**Low**	Remove or obfuscate version comments from client-side files where feasible. Upgrade Bootstrap to the latest supported version (v5.3.8) and ensure outdated components are removed. Regularly review and update third-party libraries to minimize information disclosure and reduce the attack surface.	https://owasp.org/www-community/attacks/Information_Disclosure	New
10	Hmisdev.mbmconline.in	Version Disclosure (ASP.NET)	CWE-200	**Low**	Disable or suppress version disclosure headers by removing X-AspNet-Version and X-Powered-By from HTTP responses. Ensure the application runs on a fully patched and supported version of ASP.NET and regularly apply Microsoft security updates.	https://owasp.org/www-community/attacks/Information_Disclosure	New

11	Hmisdev.mbmconline.in	Server Disclosure	CWE-200	**Low**	It is recommended to remove or obfuscate server identification headers by configuring the web server to suppress detailed version information. Implement secure server hardening practices, ensure unnecessary headers are disabled, and regularly review HTTP response headers to minimize information disclosure.	https://learn.microsoft.com/en-us/archive/blogs/varunm/remove-unwanted-http-response-headers https://www.acunetix.com/vulnerabilities/web/version-disclosure-iis/	New
12	Hmisdev.mbmconline.in	Stack Trace Disclosure (ASP.NET)	CWE-209	**Low**	Disable detailed error messages and stack trace disclosure in production by configuring customErrors in web.config. Ensure that detailed exceptions are logged internally while presenting generic error messages to users. Regularly review error-handling configurations	https://www.acunetix.com/vulnerabilities/web/stack-trace-disclosure-asp-net/	New

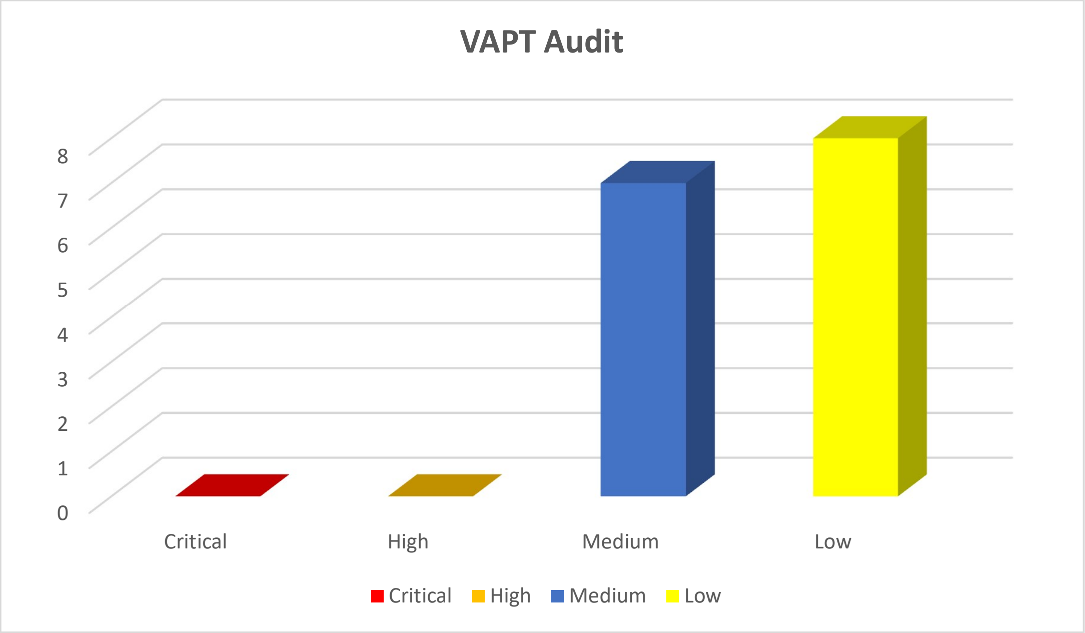
					to prevent leakage of sensitive debugging information.		
13	Hmisdev.mbmconline.in	Cookie not marked as securesite attribute	CWE-614	**Low**	Configure the application to set the Secure flag on all sensitive cookies to ensure they are transmitted only over HTTPS connections. Additionally, enforce HTTPS across the application and review cookie attributes such as HttpOnly and SameSite for improved session security.	https://cwe.mitre.org/data/definitions/614.html	New
14	Hmisdev.mbmconline.in	Clickjacking	CWE-1021 CWE-693	**Low**	Implement the X-Frame-Options header with the value DENY or SAMEORIGIN. Additionally, configure a Content-Security-Policy with the frame-ancestors directive to explicitly restrict which domains are allowed to embed the application. These controls	https://cwe.mitre.org/data/definitions/693.html https://cwe.mitre.org/data/definitions/1021.html	New

					will prevent unauthorized framing and mitigate clickjacking attacks.		
15	Hmisdev.mbmconline.in	Concurrent Login	CWE-613	**Low**	Restrict the number of active sessions per user account. When a new login occurs, invalidate any previous active sessions. Implement session timeout and logout mechanisms. Provide users with visibility of active sessions and the ability to terminate other sessions if required.	https://owasp.org/Top10/2021/A07_2021-Identification_and_Authentication_Failures/	New

Tabular Representation of the vulnerabilities:

Risk Rating	Count of Observations
Critical	**-**
High	**-**
Medium	**7**
Low	**8**

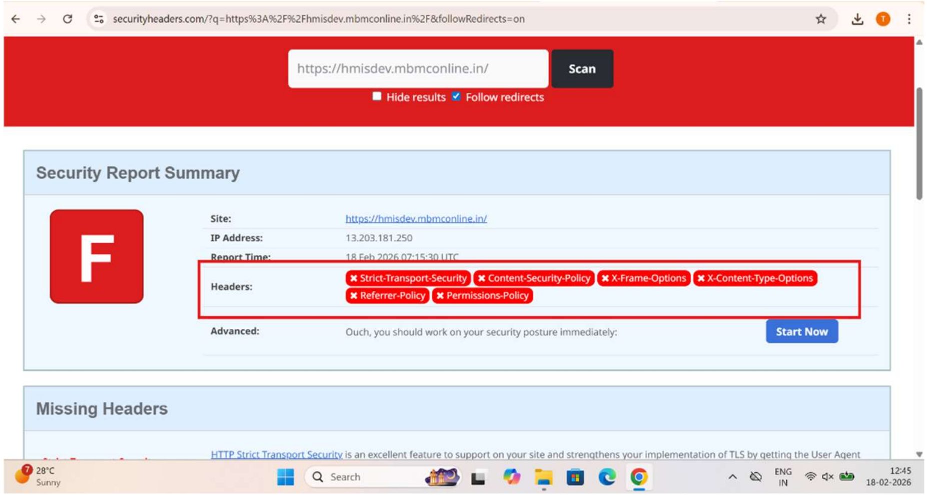
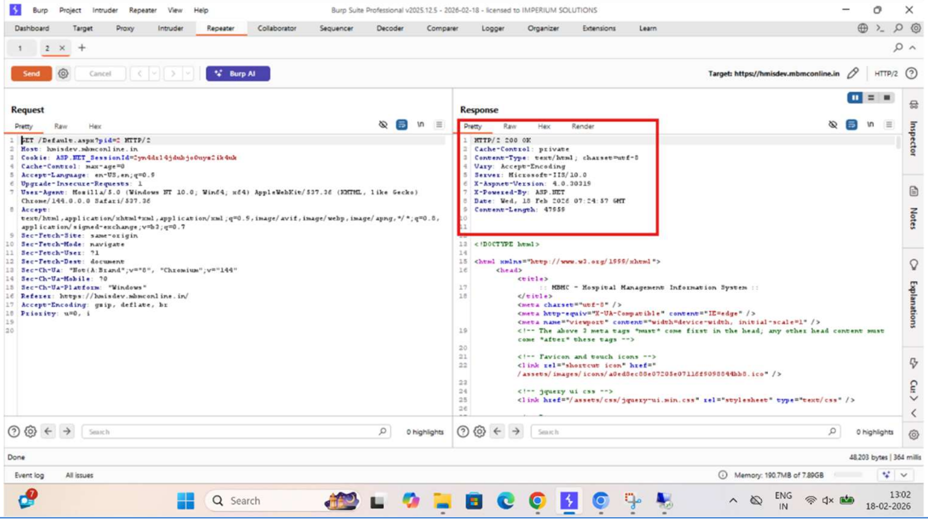
Graphical Representation of vulnerabilities



8. Detailed Observations

1. Missing Security Headers

Vulnerability Title	***Affected URLs/IP***
Missing Security Headers	Hmisdev.mbmconline.in
Detailed Observation	The application response does not include important HTTP security headers such as Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. Absence of these headers may expose the application to attacks like Clickjacking, MIME-sniffing, Cross-Site Scripting (XSS), information leakage, and protocol downgrade attacks. This indicates improper security configuration at the web server or application level.
Vulnerability Reference (CWE/CVE)	CWE-693
Severity	**Medium**
Recommendation	It is recommended to configure and enable the required HTTP security headers at the web server or application level. At a minimum, implement the following: Content-Security-Policy: default-src 'self'; X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000; includeSubDomains Referrer-Policy: no-referrer Permissions-Policy: geolocation=(), camera=(), microphone=() X-Frame-Options: DENY
Reference	https://www.invicti.com/blog/web-security/missing-http-security-headers
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)	 

securityheaders.com/?q=https%3A%2F%2Fhmisdev.mbmconline.in%2F&followRedirects=on

https://hmisdev.mbmconline.in/ Scan

□ Hide results ☑ Follow redirects

Security Report Summary

Site:	https://hmisdev.mbmconline.in/
IP Address:	13.203.181.250
Report Time:	18 Feb 2026 07:15:30 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Advanced:	Ouch, you should work on your security posture immediately:

Missing Headers

HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent

Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS

Target: https://hmisdev.mbmconline.in HTTP/2

Request

```
GET /Default.aspx?pid=2 HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dzl4jdubjo0uyz2ik4uk
Cache-Control: max-age=0
Accept-Language: en-US,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/144.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://hmisdev.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

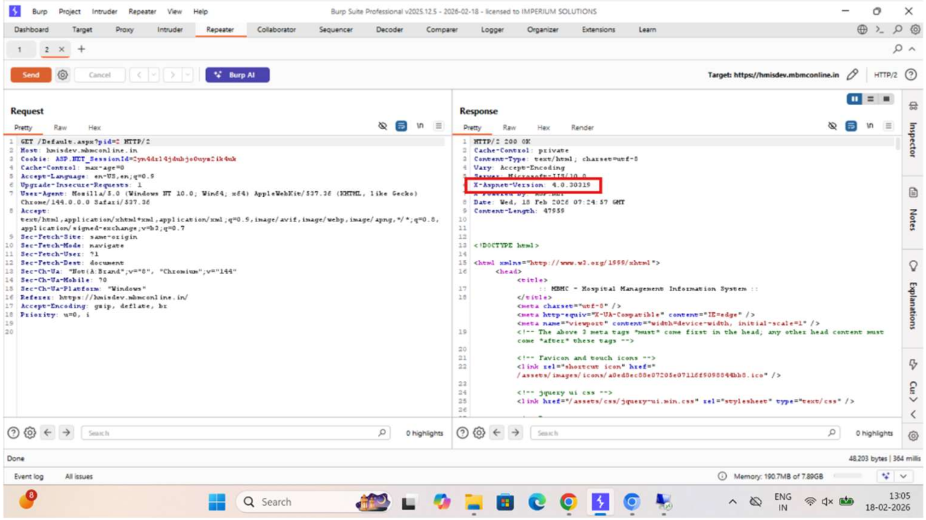
Response

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:24:57 GMT
Content-Length: 47959


<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <title>
            :: MBMC - Hospital Management Information System ::
        </title>
        <meta charset="utf-8" />
        <meta http-equiv="X-UA-Compatible" content="IE=edge" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />
        <!-- The above 3 meta tags *must* come first in the head; any other head content must
        come *after* these tags -->

        <!-- Favicon and touch icons -->
        <link rel="shortcut icon" href="
        /assets/images/icons/a0ed8ec08e07205e07116f9098844bb8.ico" />

        <!-- jquery ui css -->
        <link href="/assets/css/jquery-ui.min.css" rel="stylesheet" type="text/css" />
```

2. Out of date (ASP.NET Version)

Vulnerability Title	***Affected URLs/IP***
Out of date (ASP.NET Version)	Hmisdev.mbmconline.in

Detailed Observation	The HTTP response header reveals the ASP.NET framework version via X-AspNet-Version: 4.0.30319. Disclosure of framework version information allows attackers to identify outdated or vulnerable ASP.NET versions and target known exploits. Exposing technology stack details increases the risk of targeted attacks and reconnaissance activities.
Vulnerability Reference (CWE/CVE)	CWE-200

Severity	**Medium**
Recommendation	Upgrade the application to the latest supported and fully patched version of ASP.NET / .NET Framework (4.8.1). Apply all relevant Microsoft security updates. Remove or suppress the X-AspNet-Version and X-Powered-By headers from HTTP responses to prevent version disclosure.
Reference	https://cwe.mitre.org/data/definitions/200.html
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

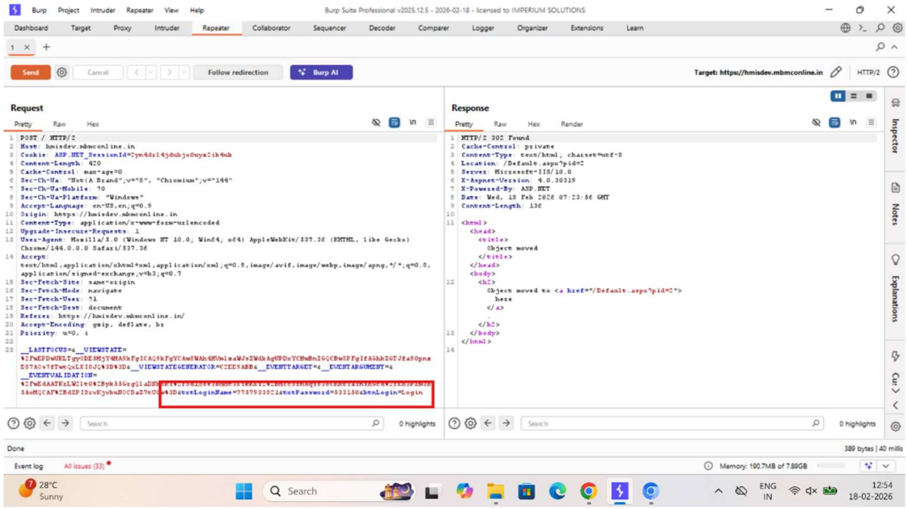
Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Burp AI
Target: https://hmisdev.mbmconline.in
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Explanations
0 highlights
Done
48,203 bytes | 364 millis
Event log All issues
Memory: 190.7MB of 7.89GB
Search
ENG IN
13:05
18-02-2026

```
GET /Default.aspx?pid=2 HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4drl4jdubjo0uyz2ik4uk
Cache-Control: max-age=0
Accept-Language: en-US,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/144.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://hmisdev.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:24:57 GMT
Content-Length: 47959



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <title>
                  :: MBMC - Hospital Management Information System ::
            </title>
            <meta charset="utf-8" />
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <meta name="viewport" content="width=device-width, initial-scale=1" />
            <!-- The above 3 meta tags *must* come first in the head; any other head content must
            come *after* these tags -->

            <!-- Favicon and touch icons -->
            <link rel="shortcut icon" href="
            /assets/images/icons/a0ed8ec08e07205e07116f9098844bb8.ico" />

            <!-- jquery ui css -->
            <link href="/assets/css/jquery-ui.min.css" rel="stylesheet" type="text/css" />
```

3. Clear Text OTP Transmission in Login Request

Vulnerability Title	***Affected URLs/IP***
Clear Text OTP Transmission in Login Request	Hmisdev.mbmconline.in
Detailed Observation	The login request transmits sensitive authentication data (OTP) in clear text within the HTTP request body. If transport encryption is weak, improperly configured, or intercepted (e.g., via MITM attack, proxy logging, or network sniffing), the OTP can be captured and reused by an attacker. OTP values should never be exposed in plaintext during transmission or logging. This increases the risk of account takeover.

Vulnerability Reference (CWE/CVE)	CWE-319
Severity	**Medium**
Recommendation	It is strongly recommended to: Enforce HTTPS (TLS 1.2 or higher) across the application. Avoid transmitting passwords in clear text. Implement secure encryption mechanisms for data in transit. Ensure passwords are hashed and salted on the server side. Disable login access over HTTP. Use secure authentication frameworks (OAuth, SSO, etc.). Implement short OTP expiration and one-time use validation.
Reference	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

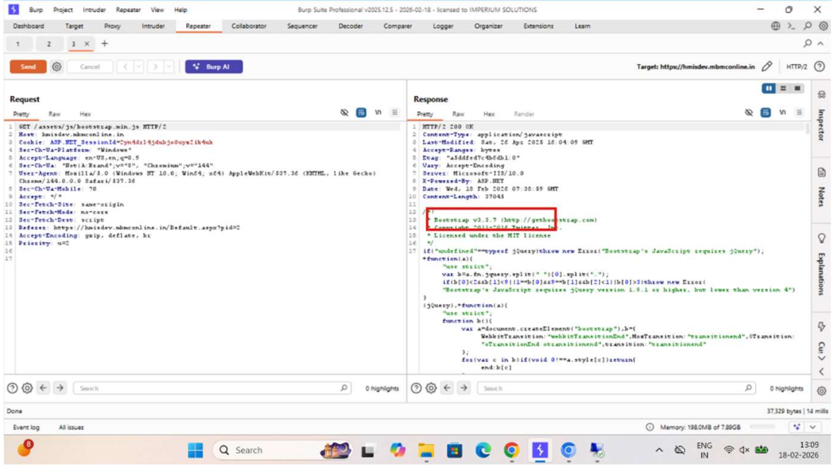
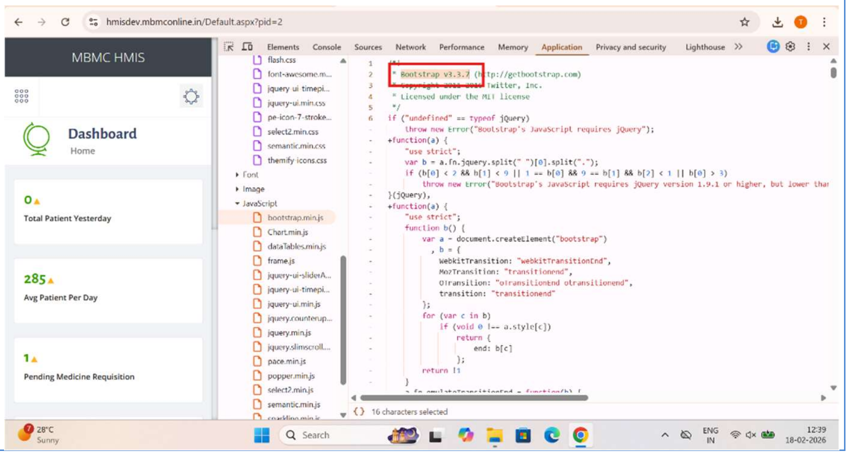
Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Follow redirection Burp AI
Target: https://hmisdev.mbmconline.in HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector Notes Explanations
0 highlights
Done
Event log All issues (33)
Memory: 190.7MB of 7.89GB
389 bytes | 40 millis
28°C Sunny
Search
ENG IN
12:54 18-02-2026

```
POST / HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dz14jdubjo0uys2ik4uk
Content-Length: 420
Cache-Control: max-age=0
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://hmisdev.mbmconline.in
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://hmisdev.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

__LASTFOCUS=&__VIEWSTATE=
%2FwEPDwUKLTgyODE5MjY4MA9kFgICAQ9kFgYCAw8WAh4HVmlzaWJsZWdkAgUPDxYCHwBnZGQCBw8PFgIfAGhkZGTJfa90pns
E07A0s7fTwtQxLXI8JQ%3D%3D&__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTTARGET=&__EVENTARGUMENT=&
__EVENTVALIDATION=
%2FwEdAATKzLW21t0%2Byk55GzgQ1aDH[illegible]
5AoMQCAF%2BdZPISzvKjvbuN0CDaZ7tUCw%3D&txtLoginName=7757933821&txtPassword=523150&btnLogin=Login
```

```
HTTP/2 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Default.aspx?pid=2
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:23:56 GMT
Content-Length: 136

<html>
  <head>
    <title>
      Object moved
    </title>
  </head>
  <body>
    <h2>
      Object moved to <a href="/Default.aspx?pid=2">
        here
      </a>
      .
    </h2>
  </body>
</html>
```

4. Out of Date (Bootstrap Version)

Vulnerability Title	***Affected URLs/IP***
Out of Date (Bootstrap Version)	Hmisdev.mbmconline.in
Detailed Observation	The application was found to be using Bootstrap version 3.3.7. Bootstrap 3.3.7 is an outdated version and is no longer actively maintained. Older versions of Bootstrap may contain

	known security vulnerabilities and compatibility issues, increasing the risk of client-side attacks.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Medium**
Recommendation	Upgrade Bootstrap to the latest stable and supported version (Bootstrap 5.3.8). Remove deprecated Bootstrap 3 components and ensure all dependent libraries are compatible with the updated version. Regularly update third-party libraries to mitigate known vulnerabilities.
Reference	https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

Target: https://hmisdev.mbmconline.in

Request

```
GET /assets/js/bootstrap.min.js HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dz14jdubjo0uyw2ik4uk
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://hmisdev.mbmconline.in/Default.aspx?pid=2
Accept-Encoding: gzip, deflate, br
Priority: u=2
```

Response

```
HTTP/2 200 OK
Content-Type: application/javascript
Last-Modified: Sat, 26 Apr 2025 16:04:05 GMT
Accept-Ranges: bytes
Etag: "a5ddfed7c4b6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:38:59 GMT
Content-Length: 37045

/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");
+function(a){
    "use strict";
    var b=a.fn.jquery.split(" ")[0].split(".");
    if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error(
    "Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")
}
(jQuery),+function(a){
    "use strict";
    function b(){
        var a=document.createElement("bootstrap"),b={
            WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:
            "oTransitionEnd otransitionend",transition:"transitionend"
        };
        for(var c in b)if(void 0!==a.style[c])return{
            end:b[c]
```

37,329 bytes | 14 millis

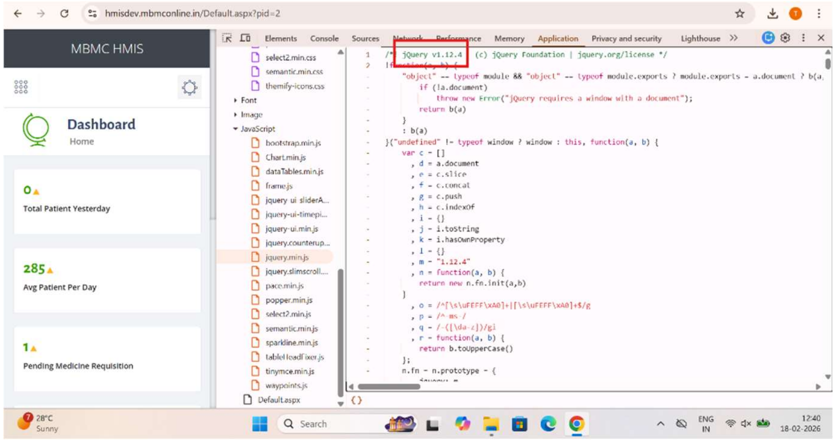
hmisdev.mbmconline.in/Default.aspx?pid=2

```
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if ("undefined" == typeof jQuery)
    throw new Error("Bootstrap's JavaScript requires jQuery");
+function(a) {
    "use strict";
    var b = a.fn.jquery.split(" ")[0].split(".");
    if (b[0] < 2 && b[1] < 9 || 1 == b[0] && 9 == b[1] && b[2] < 1 || b[0] > 3)
        throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than
}(jQuery),
+function(a) {
    "use strict";
    function b() {
        var a = document.createElement("bootstrap")
          , b = {
            WebkitTransition: "webkitTransitionEnd",
            MozTransition: "transitionend",
            OTransition: "oTransitionEnd otransitionend",
            transition: "transitionend"
        };
        for (var c in b)
            if (void 0 !== a.style[c])
                return {
                    end: b[c]
                };
        return !1
    }
```

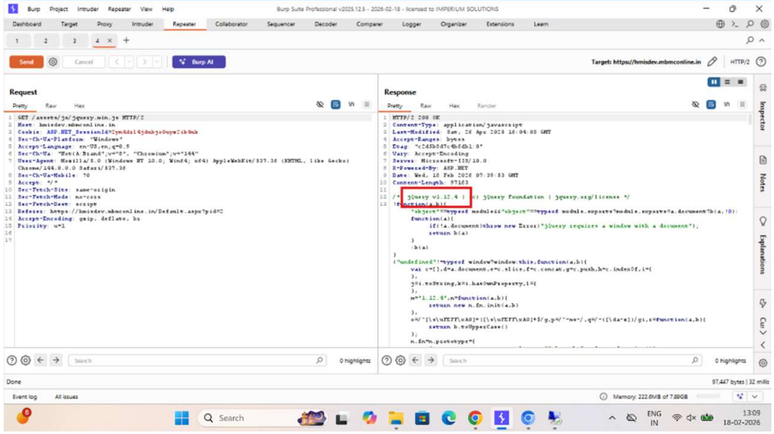
16 characters selected

5. Out of Date (jQuery Version)

Vulnerability Title	***Affected URLs/IP***

Out of Date (jQuery Version)	Hmisdev.mbmconline.in
Detailed Observation	The application is using jQuery v1.12.4, which is an outdated and unsupported version. Older jQuery versions are affected by multiple known vulnerabilities, including Cross-Site Scripting (XSS) issues. Using outdated JavaScript libraries increases the risk of exploitation through publicly available attack techniques.
Vulnerability Reference (CWE/CVE)	CWE-200 CWE-937
Severity	**Medium**
Recommendation	• Upgrade jQuery to the latest stable version (jQuery 4.0.0). • Review application compatibility before upgrading. • Implement dependency management and regular vulnerability scanning. • Remove unused or legacy libraries from the application.
Reference	https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

```
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
!function(a, b) {
    "object" == typeof module && "object" == typeof module.exports ? module.exports = a.document ? b(a,
        if (!a.document)
            throw new Error("jQuery requires a window with a document");
        return b(a)
    }
    : b(a)
}("undefined" != typeof window ? window : this, function(a, b) {
    var c = []
      , d = a.document
      , e = c.slice
      , f = c.concat
      , g = c.push
      , h = c.indexOf
      , i = {}
      , j = i.toString
      , k = i.hasOwnProperty
      , l = {}
      , m = "1.12.4"
      , n = function(a, b) {
        return new n.fn.init(a,b)
    }
      , o = /^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g
      , p = /^-ms-/
      , q = /-([\da-z])/gi
      , r = function(a, b) {
        return b.toUpperCase()
    };
    n.fn = n.prototype = {
```

```
GET /assets/js/jquery.min.js HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2ym4dzl4jdubjz0uym2ik0uk
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://hmisdev.mbmconline.in/Default.aspx?pid=2
Accept-Encoding: gzip, deflate, br
Priority: u=1
```

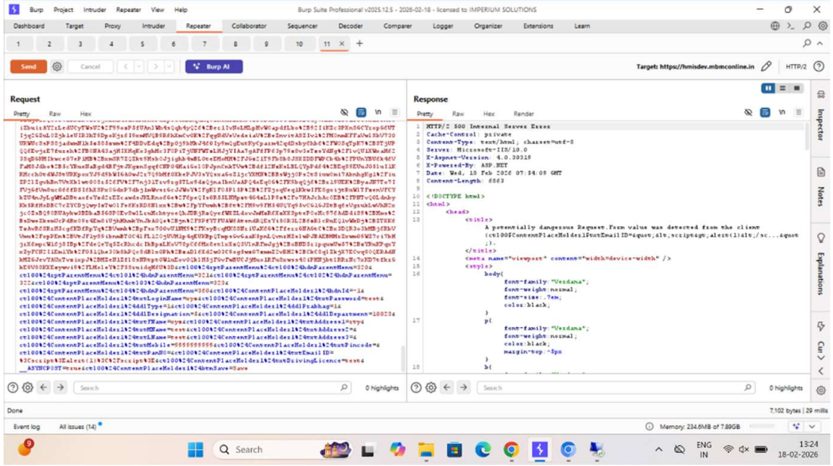
```
HTTP/2 200 OK
Content-Type: application/javascript
Last-Modified: Sat, 26 Apr 2025 16:04:08 GMT
Accept-Ranges: bytes
Etag: "c2d5b0d7c4b6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:39:53 GMT
Content-Length: 97163

/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){
    "object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):
    function(a){
        if(!a.document)throw new Error("jQuery requires a window with a document");
        return b(a)
    }
    :b(a)
}
("undefined"!=typeof window?window:this,function(a,b){
    var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={
    },
    j=i.toString,k=i.hasOwnProperty,l={
    },
    m="1.12.4",n=function(a,b){
        return new n.fn.init(a,b)
    },
    o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){
        return b.toUpperCase()
    };
    n.fn=n.prototype={
```

Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3 4 +
Send Cancel Burp AI
Target: https://hmisdev.mbmconline.in HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector Notes Explanations
0 highlights
Done
97,447 bytes | 32 millis
Event log All issues
Memory: 222.6MB of 7.89GB
ENG IN 13:09 18-02-2026

6. Improper Input Validation

Vulnerability Title	***Affected URLs/IP***
Improper Input Validation	Hmisdev.mbmconline.in
Detailed Observation	The application does not properly validate user-supplied input. During testing, script payload (<script>alert(1)</script>) was submitted in input field like Email-ID, which triggered a server-side validation error (HTTP 500 – Potentially dangerous Request. Form value detected). This indicates insufficient input validation and improper error handling. Lack of proper validation may lead to Cross-Site Scripting (XSS), injection attacks, or application crashes.
Vulnerability Reference (CWE/CVE)	CWE-20
Severity	**Medium**
Recommendation	Implement strict server-side input validation for all user-supplied fields by applying allow-list based validation. Encode or sanitize special characters before processing or rendering user input. Additionally, implement output encoding, centralized input validation logic, and proper exception handling to prevent script execution and error disclosure.
Reference	https://cwe.mitre.org/data/definitions/20.html
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)



Target: https://hmisdev.mbmconline.in HTTP/2

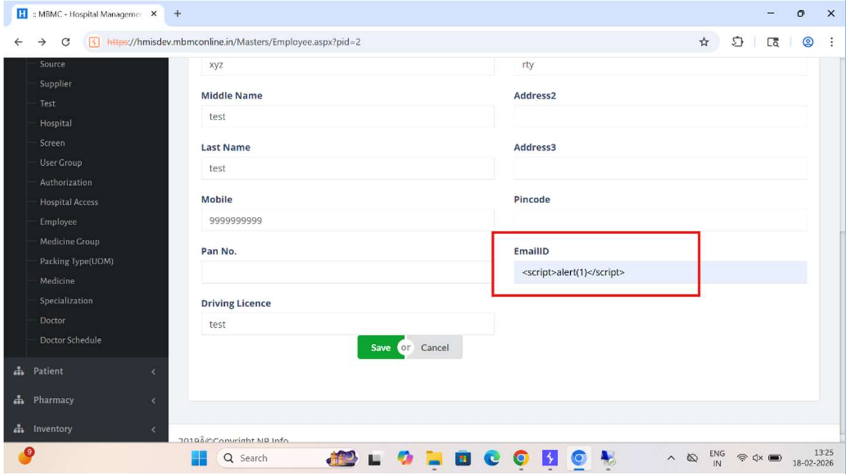
Request:

```
ctl00%24rptParentMenu%24ctl01%24hdnParentMenu=321&ctl00%24rptParentMenu%24ctl02%24hdnParentMenu=
322&ctl00%24rptParentMenu%24ctl03%24hdnParentMenu=323&
ctl00%24rptParentMenu%24ctl04%24hdnParentMenu=360&ctl00%24ContentPlaceHolder1%24hdnId=-1&
ctl00%24ContentPlaceHolder1%24txtLoginName=xyz&ctl00%24ContentPlaceHolder1%24txtPassword=test&
ctl00%24ContentPlaceHolder1%24ddlType=1&ctl00%24ContentPlaceHolder1%24ddlPrabhag=1&
ctl00%24ContentPlaceHolder1%24ddlDesignation=5&ctl00%24ContentPlaceHolder1%24ddlDepartment=10023&
ctl00%24ContentPlaceHolder1%24txtFName=xyz&ctl00%24ContentPlaceHolder1%24txtAddress1=rty&
ctl00%24ContentPlaceHolder1%24txtMName=test&ctl00%24ContentPlaceHolder1%24txtAddress2=&
ctl00%24ContentPlaceHolder1%24txtLName=test&ctl00%24ContentPlaceHolder1%24txtAddress3=&
ctl00%24ContentPlaceHolder1%24txtMobile=9999999999&ctl00%24ContentPlaceHolder1%24txtPincode=&
ctl00%24ContentPlaceHolder1%24txtPanNO=&ctl00%24ContentPlaceHolder1%24txtEmailID=
%3Cscript%3Ealert(1)%3C%2Fscript%3E&ctl00%24ContentPlaceHolder1%24txtDrivingLicence=test&
__ASYNCPOST=true&ctl00%24ContentPlaceHolder1%24btnSave=Save
```

Response:

```
HTTP/2 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:54:05 GMT
Content-Length: 6863

<!DOCTYPE html>
<html>
    <head>
        <title>
            A potentially dangerous Request.Form value was detected from the client
            (ctl00$ContentPlaceHolder1$txtEmailID=&quot;&lt;script&gt;alert(1)&lt;/sc...&quot;
            ).
        </title>
        <meta name="viewport" content="width=device-width" />
        <style>
            body{
                font-family:"Verdana";
                font-weight:normal;
                font-size: .7em;
                color:black;
            }
            p{
                font-family:"Verdana";
                font-weight:normal;
                color:black;
                margin-top: -5px
            }
            b{
```

Done 7,102 bytes | 29 millis



xyz	rty
Middle Name	Address2
test	
Last Name	Address3
test	
Mobile	Pincode
9999999999	
Pan No.	EmailID
	<script>alert(1)</script>
Driving Licence	
test	

7. Improper Input Validation (Missing Input Length Validation)

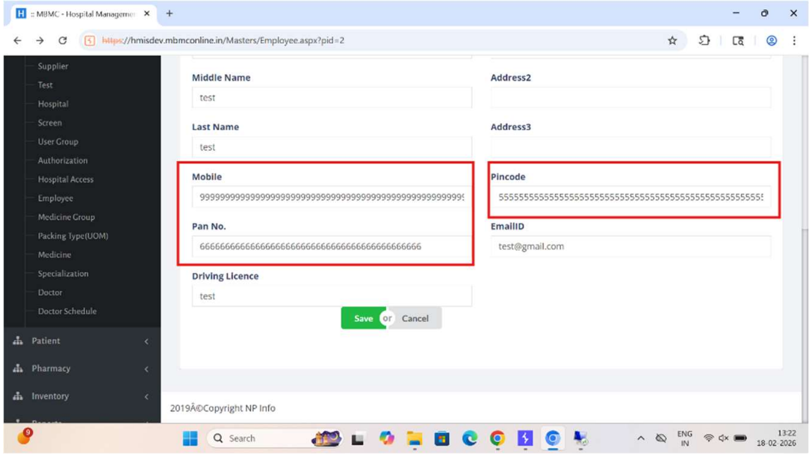
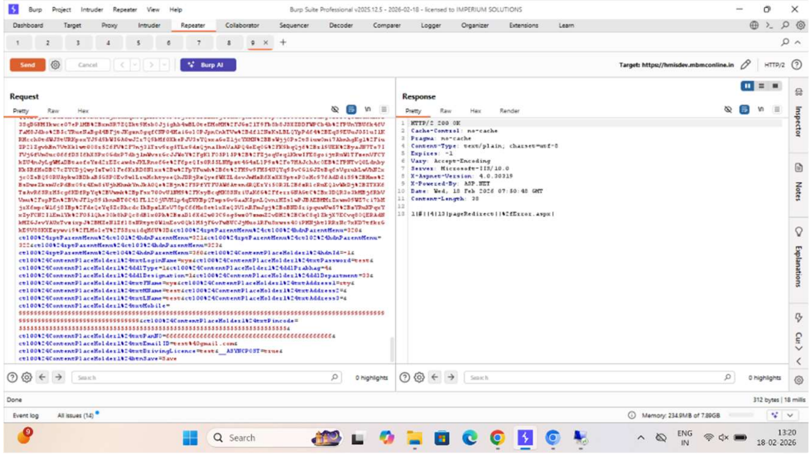
Vulnerability Title	***Affected URLs/IP***
Improper Input Validation (Missing Input Length Validation)	Hmisdev.mbmconline.in

Detailed Observation

During testing of the Employee Management module, it was observed that the application accepts excessively long numeric input in the following fields:

- Mobile
- Pin code
- PAN Number

The application does not enforce server-side input length validation. Extremely large values (hundreds of characters) were accepted and processed.

	This indicates missing backend validation controls and insufficient input sanitization.
Vulnerability Reference (CWE/CVE)	CWE-20
Severity	**Medium**
Recommendation	Implement strict server-side input validation for all user-supplied fields by applying allow-list based validation. Encode or sanitize special characters before processing or rendering user input. Additionally, implement output encoding, centralized input validation logic, and proper exception handling to prevent script execution and error disclosure. Implement strict, server-side validation that enforces explicit minimum and maximum lengths for all inputs
Reference	https://cwe.mitre.org/data/definitions/20.html
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

:: MBMC - Hospital Manageme

https://hmisdev.mbmconline.in/Masters/Employee.aspx?pid=2

Middle Name: test

Address2:

Last Name: test

Address3:

Mobile: 99999999999999999999999999999999999999999999999999

Pincode: 55555555555555555555555555555555555555555555555555

Pan No.: 6666666666666666666666666666666666666666666

EmailID: test@gmail.com

Driving Licence: test

2019Â©Copyright NP Info

Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS

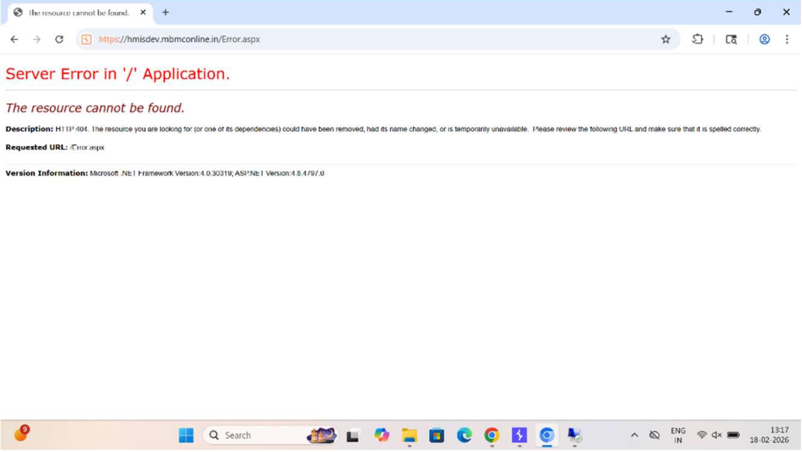
Target: https://hmisdev.mbmconline.in HTTP/2

Request

```
[illegible]
hE9V08XXEsywvi9%2FLMoleT%2F5SzuidqM6U%3D&ctl00%24rptParentMenu%24ctl00%24hdnParentMenu=320&
ctl00%24rptParentMenu%24ctl01%24hdnParentMenu=321&ctl00%24rptParentMenu%24ctl02%24hdnParentMenu=
322&ctl00%24rptParentMenu%24ctl03%24hdnParentMenu=323&
ctl00%24rptParentMenu%24ctl04%24hdnParentMenu=360&ctl00%24ContentPlaceHolder1%24hdnId=-1&
ctl00%24ContentPlaceHolder1%24txtLoginName=xyz&ctl00%24ContentPlaceHolder1%24txtPassword=test&
ctl00%24ContentPlaceHolder1%24ddlType=1&ctl00%24ContentPlaceHolder1%24ddlPrabhag=4&
ctl00%24ContentPlaceHolder1%24ddlDesignation=1&ctl00%24ContentPlaceHolder1%24ddlDepartment=33&
ctl00%24ContentPlaceHolder1%24txtFName=xyz&ctl00%24ContentPlaceHolder1%24txtAddress1=xty&
ctl00%24ContentPlaceHolder1%24txtMName=test&ctl00%24ContentPlaceHolder1%24txtAddress2=&
ctl00%24ContentPlaceHolder1%24txtLName=test&ctl00%24ContentPlaceHolder1%24txtAddress3=&
ctl00%24ContentPlaceHolder1%24txtMobile=
9999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999&ctl00%24ContentPlaceHolder1%24txtPincode=
5555555555555555555555555555555555555555555555555555555555555555555555555555555&
ctl00%24ContentPlaceHolder1%24txtPanNO=666666666666666666666666666666666666666666666666666&
ctl00%24ContentPlaceHolder1%24txtEmailID=test%40gmail.com&
ctl00%24ContentPlaceHolder1%24txtDrivingLicence=test&__ASYNCPOST=true&
ctl00%24ContentPlaceHolder1%24btnSave=Save
```

Response

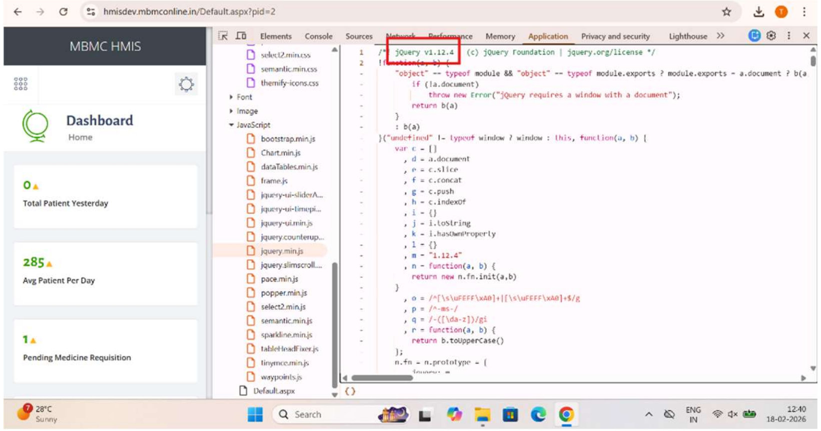
```
HTTP/2 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/plain; charset=utf-8
Expires: -1
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:50:48 GMT
Content-Length: 38

1|#||4|13|pageRedirect||%2fError.aspx|
```

	 The resource cannot be found. https://hmisdev.mbmconline.in/Error.aspx Server Error in '/' Application. *The resource cannot be found.* **Description:** HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly. **Requested URL:** /Error.aspx **Version Information:** Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4797.0

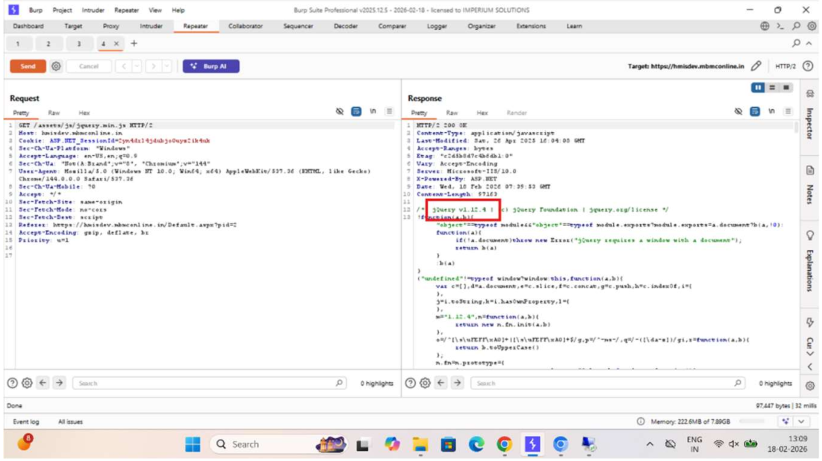
8. Version Disclosure (jQuery)

Vulnerability Title	***Affected URLs/IP***
Version Disclosure (jQuery)	Hmisdev.mbmconline.in
Detailed Observation	The application is using jQuery version 1.12.4, which is publicly disclosed via client-side source code. This version is outdated and contains known security vulnerabilities. Public version disclosure allows attackers to target known exploits associated with this version.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	Upgrade to the latest stable jQuery version (4.0.0). Remove unused libraries. Implement dependency management and regular patching. Consider Sub resource Integrity (SRI) and Content Security Policy (CSP).
Reference	https://owasp.org/www-community/attacks/Information_Disclosure
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)



```
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
!function(a, b) {
    "object" == typeof module && "object" == typeof module.exports ? module.exports = a.document ? b(a
        if (!a.document)
            throw new Error("jQuery requires a window with a document");
        return b(a)
    }
    : b(a)
}("undefined" != typeof window ? window : this, function(a, b) {
    var c = []
      , d = a.document
      , e = c.slice
      , f = c.concat
      , g = c.push
      , h = c.indexOf
      , i = {}
      , j = i.toString
      , k = i.hasOwnProperty
      , l = {}
      , m = "1.12.4"
      , n = function(a, b) {
        return new n.fn.init(a,b)
    }
      , o = /^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g
      , p = /^-ms-/
      , q = /-([\da-z])/gi
      , r = function(a, b) {
        return b.toUpperCase()
    };
    n.fn = n.prototype = {
```



Request

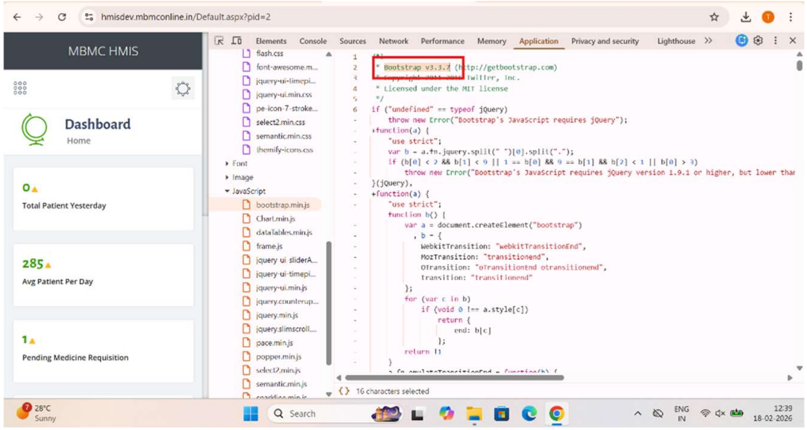
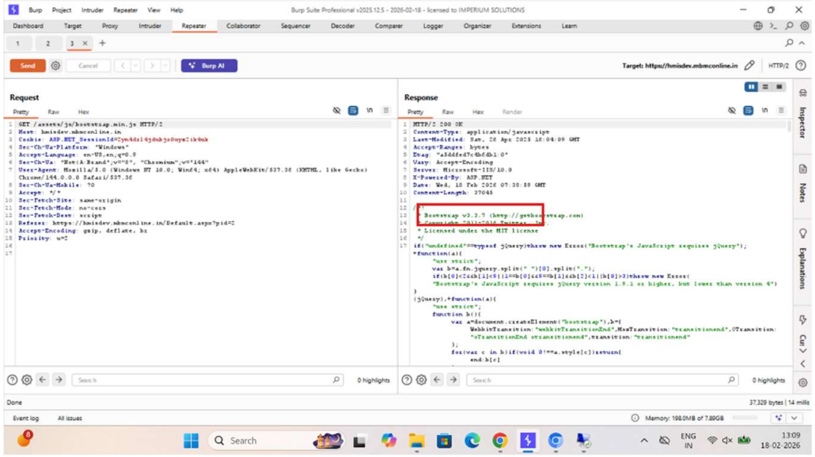
```
GET /assets/js/jquery.min.js HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dzl4jdubjo0uym2ik4uk
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://hmisdev.mbmconline.in/Default.aspx?pid=2
Accept-Encoding: gzip, deflate, br
Priority: u=1
```

Response

```
HTTP/2 200 OK
Content-Type: application/javascript
Last-Modified: Sat, 26 Apr 2025 16:04:08 GMT
Accept-Ranges: bytes
Etag: "c2d5b8d7c4b6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:39:53 GMT
Content-Length: 97163

/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){
    "object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):
    function(a){
        if(!a.document)throw new Error("jQuery requires a window with a document");
        return b(a)
    }
    :b(a)
}
("undefined"!=typeof window?window:this,function(a,b){
    var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={
    },
    j=i.toString,k=i.hasOwnProperty,l={
    },
    m="1.12.4",n=function(a,b){
        return new n.fn.init(a,b)
    },
    o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){
        return b.toUpperCase()
    };
    n.fn=n.prototype={
```

9. Version Disclosure (Bootstrap)

Vulnerability Title	***Affected URLs/IP***
Version Disclosure (Bootstrap)	Hmisdev.mbmconline.in
Detailed Observation	The application discloses the Bootstrap framework version through client-side resources where the version information is explicitly mentioned (e.g., Bootstrap v3.3.7). Disclosure of third-party library versions allows an attacker to identify the exact framework version in use and potentially exploit known vulnerabilities associated with that version.
Vulnerability Reference (CWE/CVE)	CWE-200

Severity	**Low**
Recommendation	Remove or obfuscate version comments from client-side files where feasible. Upgrade Bootstrap to the latest supported version (v5.3.8) and ensure outdated components are removed. Regularly review and update third-party libraries to minimize information disclosure and reduce the attack surface.
Reference	https://owasp.org/www-community/attacks/Information_Disclosure
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

hmisdev.mbmconline.in/Default.aspx?pid=2

```
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if ("undefined" == typeof jQuery)
    throw new Error("Bootstrap's JavaScript requires jQuery");
+function(a) {
    "use strict";
    var b = a.fn.jquery.split(" ")[0].split(".");
    if (b[0] < 2 && b[1] < 9 || 1 == b[0] && 9 == b[1] && b[2] < 1 || b[0] > 3)
        throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower thar
}(jQuery),
+function(a) {
    "use strict";
    function b() {
        var a = document.createElement("bootstrap")
          , b = {
            WebkitTransition: "webkitTransitionEnd",
            MozTransition: "transitionend",
            OTransition: "oTransitionEnd otransitionend",
            transition: "transitionend"
        };
        for (var c in b)
            if (void 0 !== a.style[c])
                return {
                    end: b[c]
                };
        return !1
    }
```

Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS

Target: https://hmisdev.mbmconline.in

Request

```
GET /assets/js/bootstrap.min.js HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2ym4dzl4jdubjo0uym2ik4uk
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://hmisdev.mbmconline.in/Default.aspx?pid=2
Accept-Encoding: gzip, deflate, br
Priority: u=2
```

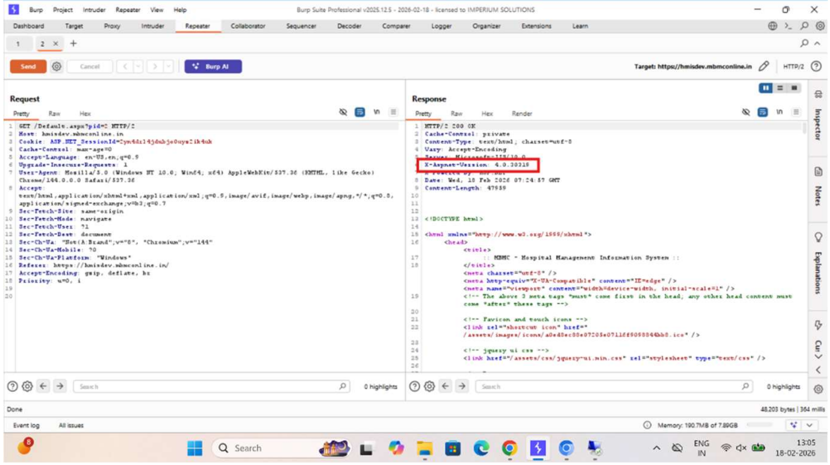
Response

```
HTTP/2 200 OK
Content-Type: application/javascript
Last-Modified: Sat, 26 Apr 2025 16:04:09 GMT
Accept-Ranges: bytes
Etag: "a5ddfed7c4b6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:38:59 GMT
Content-Length: 37045

/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");
+function(a){
      "use strict";
      var b=a.fn.jquery.split(" ")[0].split(".");
      if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error(
      "Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")
}
(jQuery),+function(a){
      "use strict";
      function b(){
            var a=document.createElement("bootstrap"),b={
                  WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:
                  "oTransitionEnd otransitionend",transition:"transitionend"
            };
            for(var c in b)if(void 0!==a.style[c])return{
                  end:b[c]
```

37,329 bytes | 14 millis

10. Version Disclosure (ASP.NET)

Vulnerability Title	***Affected URLs/IP***

Version Disclosure (ASP.NET)	Hmisdev.mbmconline.in
Detailed Observation	The application discloses ASP.NET framework version information through HTTP response headers such as X-AspNet-Version and X-Powered-By. This information reveals the underlying technology and framework version in use, which can assist an attacker in identifying and exploiting known vulnerabilities specific to that ASP.NET version.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	Disable or suppress version disclosure headers by removing X-AspNet-Version and X-Powered-By from HTTP responses. Ensure the application runs on a fully patched and supported version of ASP.NET and regularly apply Microsoft security updates.
Reference	https://owasp.org/www-community/attacks/Information_Disclosure
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Burp AI
Target: https://hmisdev.mbmconline.in HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector Notes Explanations
0 highlights
Done
48,203 bytes | 364 millis
Event log All issues
Memory: 190.7MB of 7.89GB
13:05 18-02-2026

Request

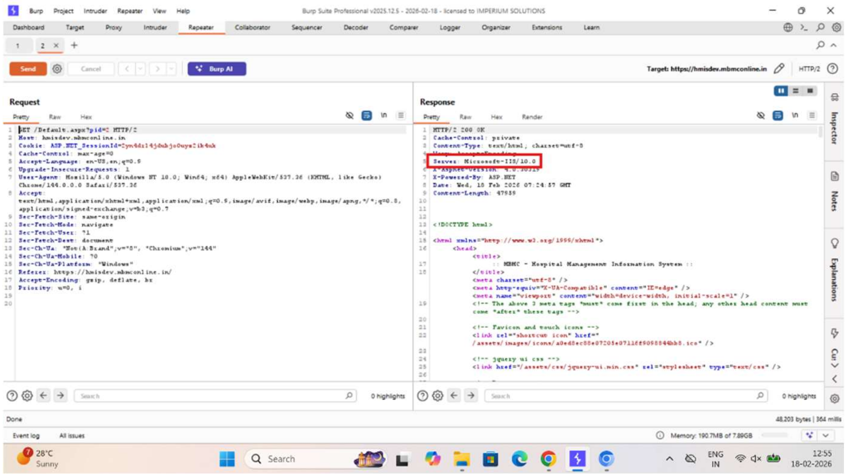
```
GET /Default.aspx?pid=2 HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dz14jdubje0uys2ik4uk
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://hmisdev.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:24:57 GMT
Content-Length: 47939



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <title>
                  :: MBMC - Hospital Management Information System ::
            </title>
            <meta charset="utf-8" />
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <meta name="viewport" content="width=device-width, initial-scale=1" />
            <!-- The above 3 meta tags *must* come first in the head; any other head content must
            come *after* these tags -->

            <!-- Favicon and touch icons -->
            <link rel="shortcut icon" href="
            /assets/images/icons/a0ed8ec88e07205e0711ff9098844bb8.ico" />

            <!-- jquery ui css -->
            <link href="/assets/css/jquery-ui.min.css" rel="stylesheet" type="text/css" />
```

11. Server Disclosure

Vulnerability Title	***Affected URLs/IP***

Server Disclosure	Hmisdev.mbmconline.in
Detailed Observation	It was observed that the application discloses server technology details in the HTTP response headers. The Server header reveals the backend web server and version information (e.g., Microsoft-IIS/10.0). Such disclosures provide attackers with valuable information about the underlying infrastructure, which can be leveraged to identify known vulnerabilities, misconfigurations, or targeted exploits specific to the disclosed server version.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	It is recommended to remove or obfuscate server identification headers by configuring the web server to suppress detailed version information. Implement secure server hardening practices, ensure unnecessary headers are disabled, and regularly review HTTP response headers to minimize information disclosure.
Reference	https://learn.microsoft.com/en-us/archive/blogs/varunm/remove-unwanted-http-response-headers https://www.acunetix.com/vulnerabilities/web/version-disclosure-iis/
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

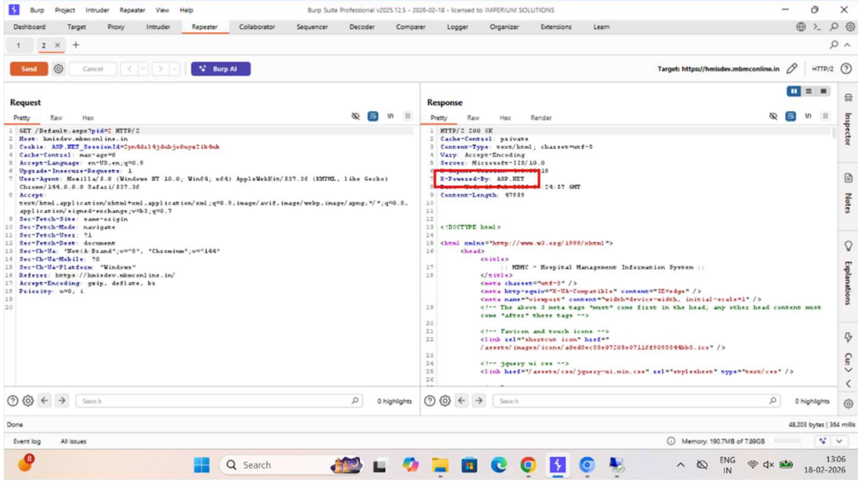
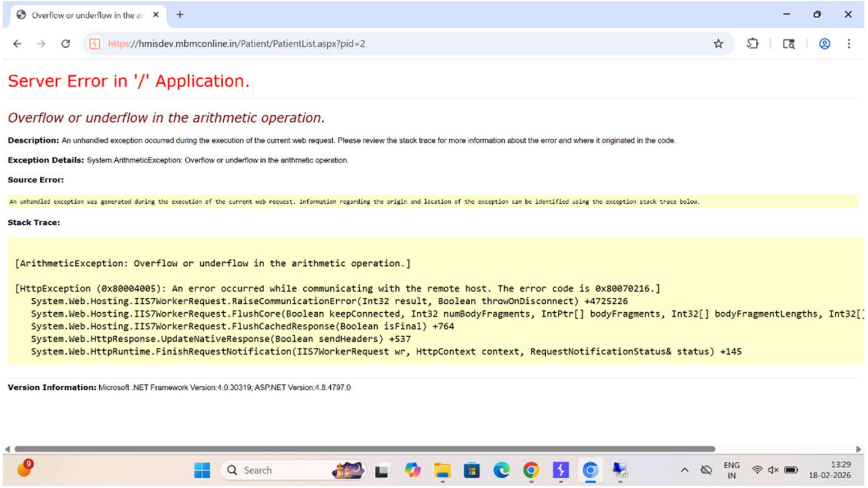
Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Burp AI
Target: https://hmisdev.mbmconline.in
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Explanations
Search
0 highlights
Done
48,203 bytes | 364 millis
Event log All issues
Memory: 190.7MB of 7.89GB
28°C Sunny
Search
ENG IN
12:55 18-02-2026

```
GET /Default.aspx?pid=2 HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dzl4jdubjo0uyx2ik4uk
Cache-Control: max-age=0
Accept-Language: en-US,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/144.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://hmisdev.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 07:24:57 GMT
Content-Length: 47959



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <title>
                  :: MBMC - Hospital Management Information System ::
            </title>
            <meta charset="utf-8" />
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <meta name="viewport" content="width=device-width, initial-scale=1" />
            <!-- The above 3 meta tags *must* come first in the head; any other head content must
            come *after* these tags -->

            <!-- Favicon and touch icons -->
            <link rel="shortcut icon" href="
            /assets/images/icons/a0ed8ec88e07205e0711ff9098844bb8.ico" />

            <!-- jquery ui css -->
            <link href="/assets/css/jquery-ui.min.css" rel="stylesheet" type="text/css" />
```

12. Stack Trace Disclosure (ASP.NET)

Vulnerability Title	***Affected URLs/IP***
Stack Trace Disclosure (ASP.NET)	Hmisdev.mbmconline.in
Detailed Observation	During testing, the application response was found to disclose ASP.NET internal details through HTTP response headers and application behavior. Such disclosures may expose internal application logic, framework details, or error-handling configurations. If stack traces are exposed during error conditions, an attacker could gain insights into application structure, file paths, and underlying technologies, increasing the risk of targeted attacks.
Vulnerability Reference (CWE/CVE)	CWE-209
Severity	**Low**
Recommendation	Disable detailed error messages and stack trace disclosure in production by configuring customErrors in web.config. Ensure that detailed exceptions are logged internally while presenting generic error messages to users. Regularly review error-handling configurations to prevent leakage of sensitive debugging information.
Reference	https://www.acunetix.com/vulnerabilities/web/stack-trace-disclosure-asp-net/
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)	 

Burp Suite Professional v2025.12.5 - 2026-02-18 - licensed to IMPERIUM SOLUTIONS
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Burp AI
Target: https://hmisdev.mbmconline.in
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Explanations
0 highlights
Done
48,203 bytes | 364 millis
Event log All issues
Memory: 190.7MB of 7.89GB
Search
ENG IN
13:06
18-02-2026

Request

```
GET /Default.aspx?pid=2 HTTP/2
Host: hmisdev.mbmconline.in
Cookie: ASP.NET_SessionId=2yn4dz14jdubjo0uya2ik4uk
Cache-Control: max-age=0
Accept-Language: en-US,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/144.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://hmisdev.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 18 Feb 2026 [illegible]:24:57 GMT
Content-Length: 47939



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <title>
                  :: MBMC - Hospital Management Information System ::
            </title>
            <meta charset="utf-8" />
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <meta name="viewport" content="width=device-width, initial-scale=1" />
            <!-- The above 3 meta tags *must* come first in the head; any other head content must
            come *after* these tags -->

            <!-- Favicon and touch icons -->
            <link rel="shortcut icon" href="
            /assets/images/icons/a0ed8ec08e07205e0711f9098844bb8.ico" />

            <!-- jquery ui css -->
            <link href="/assets/css/jquery-ui.min.css" rel="stylesheet" type="text/css" />
```

Overflow or underflow in the a
https://hmisdev.mbmconline.in/Patient/PatientList.aspx?pid=2
Search
ENG IN
13:29
18-02-2026

Server Error in '/' Application.

Overflow or underflow in the arithmetic operation.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.ArithmeticException: Overflow or underflow in the arithmetic operation.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.
```

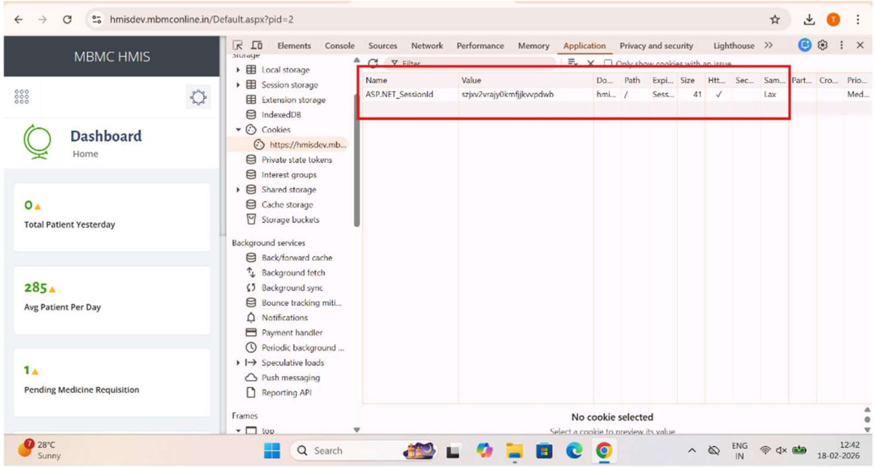
Stack Trace:

```
[ArithmeticException: Overflow or underflow in the arithmetic operation.]

[HttpException (0x80004005): An error occurred while communicating with the remote host. The error code is 0x80070216.]
   System.Web.Hosting.IIS7WorkerRequest.RaiseCommunicationError(Int32 result, Boolean throwOnDisconnect) +4725226
   System.Web.Hosting.IIS7WorkerRequest.FlushCore(Boolean keepConnected, Int32 numBodyFragments, IntPtr[] bodyFragments, Int32[] bodyFragmentLengths, Int32[
   System.Web.Hosting.IIS7WorkerRequest.FlushCachedResponse(Boolean isFinal) +764
   System.Web.HttpResponse.UpdateNativeResponse(Boolean sendHeaders) +537
   System.Web.HttpRuntime.FinishRequestNotification(IIS7WorkerRequest wr, HttpContext context, RequestNotificationStatus& status) +145
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4797.0

13. Cookie not marked as securesite attribute

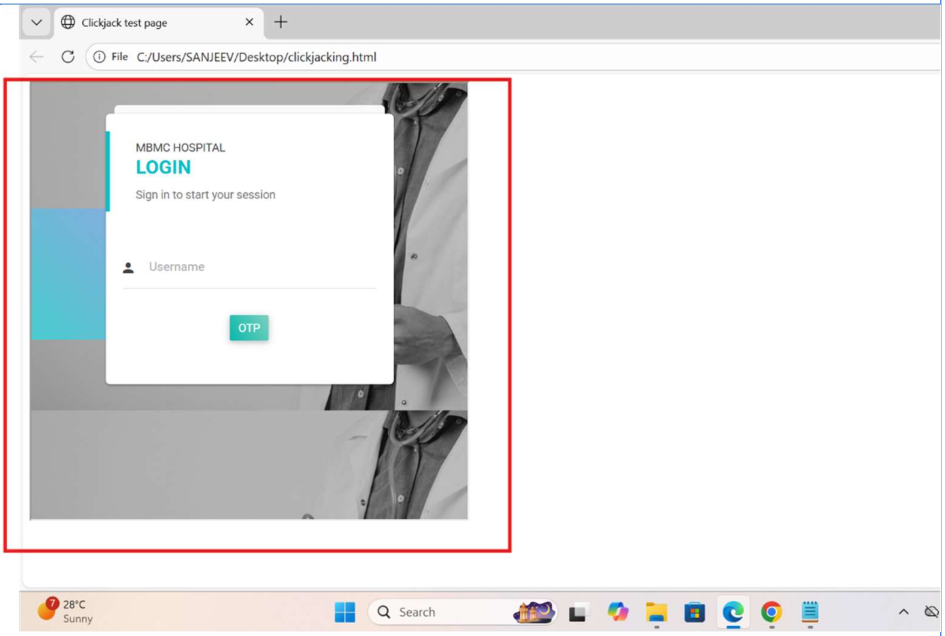
Vulnerability Title	***Affected URLs/IP***
Cookie not marked as securesite attribute	Hmisdev.mbmconline.in
Detailed Observation	During testing, the application was observed setting a session cookie without the Secure attribute. As a result, the cookie may be transmitted over unencrypted HTTP connections if accessed improperly, which could allow an attacker to intercept or hijack the session through man-in-the-middle (MITM) attacks.
Vulnerability Reference (CWE/CVE)	CWE-614

Severity	**Low**
Recommendation	Configure the application to set the Secure flag on all sensitive cookies to ensure they are transmitted only over HTTPS connections. Additionally, enforce HTTPS across the application and review cookie attributes such as HttpOnly and SameSite for improved session security.
Reference	https://cwe.mitre.org/data/definitions/614.html
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

Name	Value	Do...	Path	Expi...	Size	Htt...	Sec...	Sam...	Part...	Cro...	Prio...
ASP.NET_SessionId	szjxv2vrajy0kmfjjkvvpdwb	hmi...	/	Sess...	41	✓		Lax			Med...

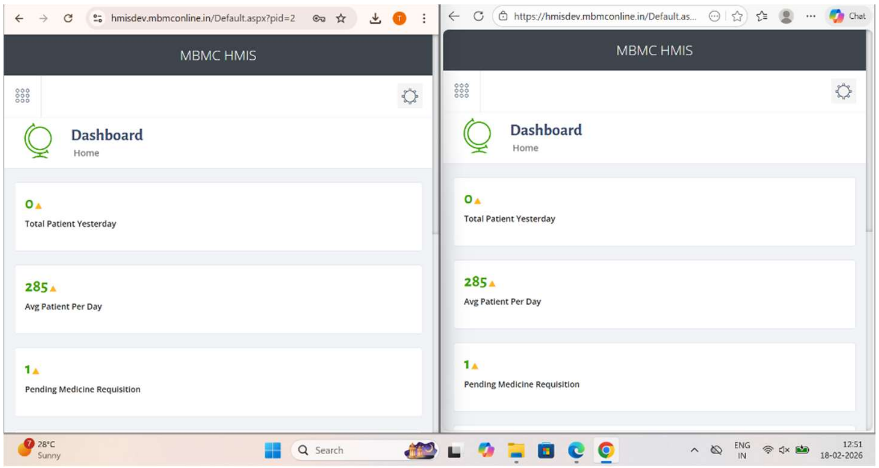
14. Clickjacking

Vulnerability Title	***Affected URLs/IP***
Clickjacking	Hmisdev.mbmconline.in
Detailed Observation	The application was successfully loaded within an HTML <iframe> from an external source, as demonstrated during testing. This indicates that the application does not implement proper anti-clickjacking protections such as the X-Frame-Options header or an appropriate Content-Security-Policy (frame-ancestors) directive. An attacker could exploit this by embedding the application in a malicious page and tricking users into performing unintended actions.

Vulnerability Reference (CWE/CVE)	CWE-1021 CWE-693
Severity	**Low**
Recommendation	Implement the X-Frame-Options header with the value DENY or SAMEORIGIN. Additionally, configure a Content-Security-Policy with the frame-ancestors directive to explicitly restrict which domains are allowed to embed the application. These controls will prevent unauthorized framing and mitigate clickjacking attacks.
Reference	https://cwe.mitre.org/data/definitions/693.html https://cwe.mitre.org/data/definitions/1021.html
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 Clickjack test page File C:/Users/SANJEEV/Desktop/clickjacking.html MBMC HOSPITAL LOGIN Sign in to start your session Username OTP 28°C Sunny Search

15.Concurrent Login

Vulnerability Title	***Affected URLs/IP***
Concurrent Login	Hmisdev.mbmconline.in
Detailed Observation	The application allows the same user credentials to establish multiple active sessions simultaneously across different browsers/devices without invalidating previous sessions,

	enforcing session uniqueness, or notifying the user. Session IDs remain valid in parallel, increasing exposure window if credentials are compromised and enabling unauthorized persistent access to sensitive healthcare data.
Vulnerability Reference (CWE/CVE)	CWE-613
Severity	**Low**
Recommendation	Restrict the number of active sessions per user account. When a new login occurs, invalidate any previous active sessions. Implement session timeout and logout mechanisms. Provide users with visibility of active sessions and the ability to terminate other sessions if required.
Reference	https://owasp.org/Top10/2021/A07_2021-Identification_and_Authentication_Failures/
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 hmisdev.mbmconline.in/Default.aspx?pid=2 https://hmisdev.mbmconline.in/Default.as... MBMC HMIS Dashboard Home 0 Total Patient Yesterday 285 Avg Patient Per Day 1 Pending Medicine Requisition MBMC HMIS Dashboard Home 0 Total Patient Yesterday 285 Avg Patient Per Day 1 Pending Medicine Requisition 28°C Sunny Search ENG IN 12:51 18-02-2026