MIRA BHAYANDAR MUNICIPAL CORPORATION

Water Connection Approval System

Web Application

Report Release Date	February 12, 2026
Type of Audit	Application Security Assessment
Type of Audit Report	First Audit Report
Period	February 05, 2026 to February 07, 2026

Document Control

Document Preparation	
Document Title	VAPT Report of Water Connection Approval System Web Application
Document ID	A3S/MBMC/ Water Connection Approval System /2526/00013
Document Version	1.0
Prepared by	Jasmeet Singh
Reviewed by	Sagar Gupta
Approved by	Sagar Gupta
Released by	Jasmeet Singh
Release date	February 12, 2026

Document Change History		
Version	**Date**	**Remarks / Reason of change**
1.0	February 12, 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: 2026.02.12
14:07:08 +05'30'

Contents

Table of Contents

1. Introduction

A3S Tech & Co. (A3S) was engaged by Mira Bhayandar Municipal Corporation to perform VAPT, for Water Connection Approval System 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 – Water Connection Approval System	Not available	Not Available	devwater.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 5, 2026
2.	Scanning	February 5, 2026
3.	Information Analysis	February 5, 2026
4.	Vulnerability Assessment	February 6, 2026
5.	Penetration Testing	February 6, 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	devwater.mbmconline.in	Brute Force Attack – Improper Restriction of Authentication Attempts	CWE-307	**High**	To mitigate this vulnerability, it is recommended to Implement account lockout after 5–10 failed login attempts. Apply rate limiting on authentication endpoints. Introduce CAPTCHA after multiple failed attempts. Add progressive delay between login attempts. Monitor and log suspicious login	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/	New

					behavior. Enforce strong password policies		
2	devwater.mbmconline.in	Missing Rate Limiting on Authentication (Password) Functionality	CWE-307	**Medium**	It is recommended to implement the following controls. Apply rate limiting on login endpoints (e.g., 5–10 attempts per minute). Enforce temporary IP blocking after threshold breach. Introduce CAPTCHA after multiple failed attempts. Implement progressive delay (exponential backoff). Monitor and alert on abnormal login behavior.	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/	New
3	devwater.mbmconline.in	Improper Input Validation	CWE-20	**Medium**	Implement strict server-side input validation for all user inputs. Use allow-lists (whitelisting) instead of block-lists. Validate input	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	New

					length, type, format, and range. Encode or sanitize input before processing or displaying it. Implement centralized validation mechanisms.		
4	devwater.mbmconline.in	Missing Length Validation in Phone Numbers	CWE-20	**Medium**	Enforce strict length validation for phone number inputs (e.g., exactly 10 digits for Indian mobile numbers). Validate input on both client-side and server-side. Allow only numeric characters and reject special characters. Implement proper error messages for invalid input.	https://techdocs.akamai.com/identity-cloud/docs/the-minimum-length-validation	New
5	devwater.mbmconline.in	Clear Text Password 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	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	New

					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.)		
6	devwater.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-Frame-Options: DENY X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000; includeSubDomains Referrer-Policy: no-referrer Permissions-Policy: geolocation=(),	https://www.invicti.com/blog/web-security/missing-http-security-headers	New

					camera=(), microphone=()		
7	devwater.mbmconline.in	Captcha Not Implemented	CWE-307	**Medium**	Implement CAPTCHA on authentication and sensitive transaction pages. Apply CAPTCHA after multiple failed login or OTP attempts. Use advanced bot detection mechanisms such as Google reCAPTCHA or equivalent solutions. Implement rate limiting along with CAPTCHA protection.	https://stackoverflow.com/questions/34016388/trying-to-implement-the-new-google-captcha	New
8	devwater.mbmconline.in	Out of date (jQuery Version)	CWE-1104	**Medium**	Upgrade jQuery to the latest stable version (v3.7.1 or above). Remove unused or legacy jQuery functions. Regularly review third-party libraries for security updates. Implement dependency monitoring as part of the SDLC.	https://github.com/jquery/jquery/security/advisories	New
9	devwater.mbmconline.in	Out of Date (Bootstrap Version)	CWE-1104	**Medium**	Upgrade Bootstrap to the latest stable and supported version. Remove	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities	New

					unused or deprecated Bootstrap components. Regularly monitor third-party libraries for security updates. Implement a dependency management and patching process.	/out-of-date-version-bootstrap	
10	devwater.mbmconline.in	Out of Date (X-Asp.Net)	CWE-1104	**Medium**	Upgrade the application to the latest supported ASP.NET / .NET Framework version. Apply the latest security patches from Microsoft. Disable version disclosure headers (X-AspNet-Version, X-Powered-By). Regularly monitor and update application frameworks and dependencies.	https://stackoverflow.com/questions/12561370/how-to-expire-a-link	New
11	devwater.mbmconline.in	Weak Ciphers	CWE-326	**Medium**	Disable all weak and legacy cipher suites. Remove CBC-based and RSA key exchange cipher suites.	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	New

					Allow only strong modern cipher suites such as: AES-GCM, CHACHA20-POLY1305. Enforce TLS 1.2 (secure ciphers only) and TLS 1.3. Regularly review SSL/TLS configurations Recommended Cipher Examples: TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256		
12	devwater.mbmconline.in	Version Disclosure (jQuery)	CWE-200	**Low**	Avoid exposing exact jQuery version details in production environments. Minify and bundle JavaScript files. Remove version comments and banners from client-side resources. Keep jQuery updated to the latest stable version.	https://owasp.org/www-community/attacks/Information_Disclosure	New
13		Version Disclosure	CWE-200	**Low**	Remove or obfuscate version	https://owasp.org/www-	New

		(Bootstrap)			comments and metadata from HTML/JS files. Upgrade to the latest Bootstrap version. Avoid exposing framework versions in client-side responses.	community/attacks/Information_Disclosure	
14		Version Disclosure (X-Asp.Net)	CWE-200	**Low**	Remove or disable the X-AspNet-Version HTTP header. Remove the X-Powered-By header if enabled. Ensure server and framework configurations do not expose internal version details.	https://stackoverflow.com/questions/12561370/how-to-expire-a-link	New
15		Server Version Disclosure	CWE-200	**Low**	Remove or obfuscate the Server HTTP response header. Apply latest security patches to the web server. Implement secure header configurations.	https://serverfault.com/questions/991045/remove-modify-iis-10-server-header-which-discloses-iis-version	New
16		Stack Disclosure	CWE-200	**Low**	Disable the X-Powered-By HTTP	https://learn.microsoft.com/en-	New

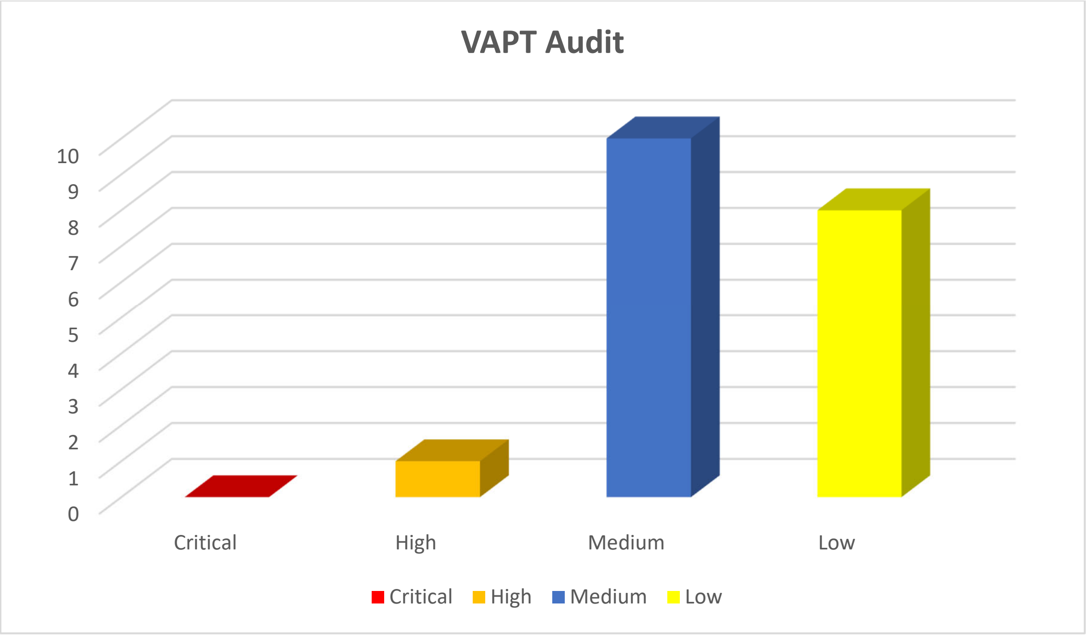
					response header. Avoid exposing internal technology details in HTTP responses. Apply secure server hardening and header management.	us/aspnet/core/security/headers	
17		Clickjacking	CWE-1021	**Low**	Implement X-Frame-Options header (DENY or SAMEORIGIN). Configure Content-Security-Policy with frame-ancestors 'self'. Validate frame usage only for trusted domains if framing is required.	https://learn.microsoft.com/en-us/aspnet/core/security/headers	New
18	devwater.mbmconline.in	Cookies Not Marked Secure	CWE-614	**Low**	Set the Secure flag on all cookies, especially session and authentication cookies. Ensure cookies are transmitted only over HTTPS. Additionally, enable HttpOnly and SameSite attributes for	https://owasp.org/www-community/controls/SecureCookieAttribute	New

					better protection. Set-Cookie: sessionid=abc123; Secure; HttpOnly; SameSite=Strict		
19		Internal Server Error	CWE-209	**Low**	Implement proper exception handling and return generic error messages to users. Disable detailed error messages and stack traces in production environments. Log detailed errors securely on the server side for debugging. Validate and sanitize all user inputs to prevent unexpected errors.	https://stackoverflow.com/questions/5385714/deploying-website-500-internal-server-error	New

Tabular Representation of the vulnerabilities:

Risk Rating	**Count of Observations**
Critical	**-**
High	**1**
Medium	**10**
Low	**8**

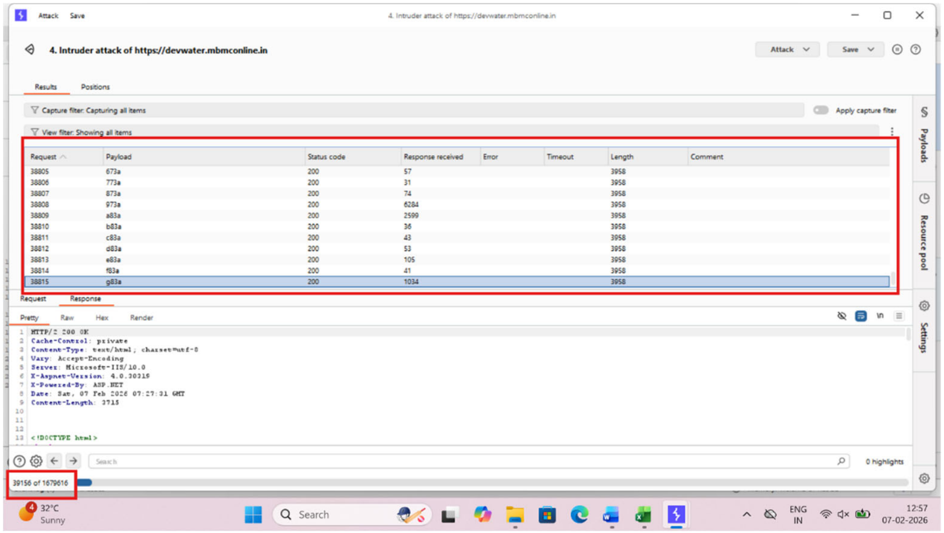
Graphical Representation of vulnerabilities



8. Detailed Observations

1. Brute Force Attack – Improper Restriction of Authentication Attempts

Vulnerability Title	***Affected URLs/IP***
Brute Force Attack – Improper Restriction of Authentication Attempts	devwater.mbmconline.in
Detailed Observation	Multiple login requests were sent with different payloads. The application returned HTTP 200 OK responses for all attempts. No account lockout mechanism was triggered. No CAPTCHA challenge was enforced. No request rate-limiting was observed. Response length and behavior remained consistent across attempts. This confirms that the application allows unlimited authentication attempts.
Vulnerability Reference (CWE/CVE)	CWE-307
Severity	**High**
Recommendation	To mitigate this vulnerability, it is recommended to Implement account lockout after 5–10 failed login attempts. Apply rate limiting on authentication endpoints. Introduce CAPTCHA after multiple failed attempts. Add progressive delay between login attempts. Monitor and log suspicious login behavior. Enforce strong password policies
Reference	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)	

4. Intruder attack of https://devwater.mbmconline.in

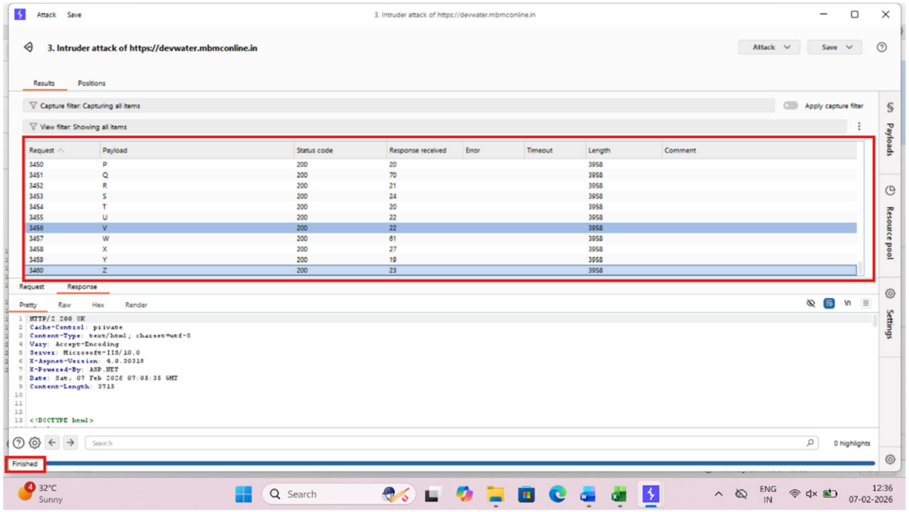
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
38805	673a	200	57			3958	
38806	773a	200	31			3958	
38807	873a	200	74			3958	
38808	973a	200	6284			3958	
38809	a83a	200	2599			3958	
38810	b83a	200	36			3958	
38811	c83a	200	43			3958	
38812	d83a	200	53			3958	
38813	e83a	200	105			3958	
38814	f83a	200	41			3958	
38815	g83a	200	1034			3958	

```
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: Sat, 07 Feb 2026 07:27:31 GMT
Content-Length: 3715



<!DOCTYPE html>
```

39156 of 1679616

2. Missing Rate Limiting on Authentication (Password) Functionality

Vulnerability Title	***Affected URLs/IP***
Missing Rate Limiting on Authentication (Password) Functionality	devwater.mbmconline.in
Detailed Observation	Rate limiting is a security control used to restrict the number of requests a user or IP address can make within a specific time period. During the security assessment, it was observed that the application does not enforce rate limiting on the login/password endpoint, allowing an attacker to send multiple authentication requests continuously.
Vulnerability Reference (CWE/CVE)	CWE-307
Severity	**Medium**
Recommendation	It is recommended to implement the following controls. Apply rate limiting on login endpoints (e.g., 5–10 attempts per minute). Enforce temporary IP blocking after threshold breach. Introduce CAPTCHA after multiple failed attempts. Implement progressive delay (exponential backoff). Monitor and alert on abnormal login behavior.
Reference	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

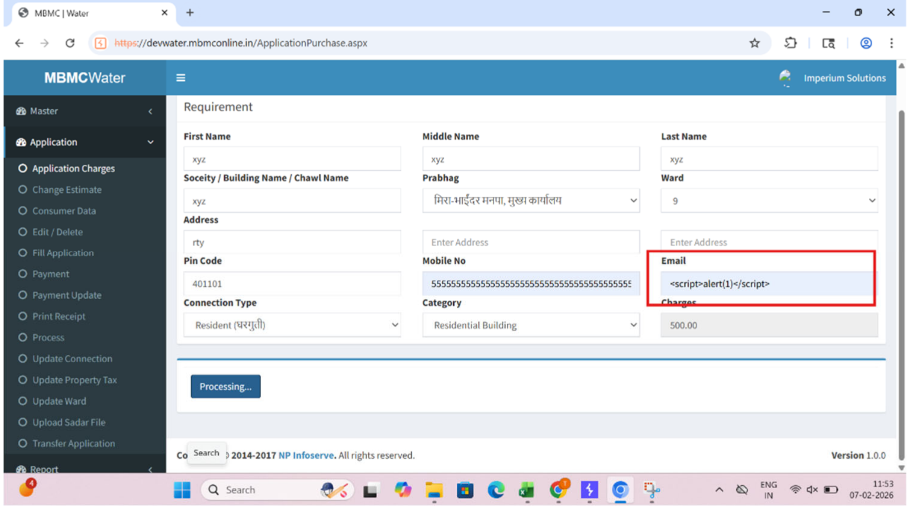
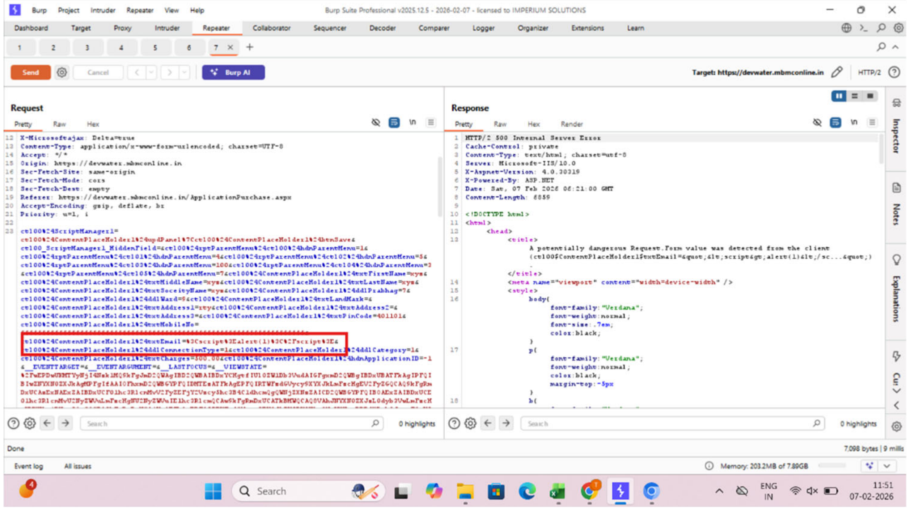
3. Intruder attack of https://devwater.mbmconline.in

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
3450	P	200	20			3958	
3451	Q	200	70			3958	
3452	R	200	21			3958	
3453	S	200	24			3958	
3454	T	200	20			3958	
3455	U	200	22			3958	
3456	V	200	22			3958	
3457	W	200	61			3958	
3458	X	200	27			3958	
3459	Y	200	19			3958	
3460	Z	200	23			3958	

```
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: Sat, 07 Feb 2026 07:05:35 GMT
Content-Length: 3715



<!DOCTYPE html>
```

3. Improper Input Validation

Vulnerability Title	***Affected URLs/IP***
Improper Input Validation	devwater.mbmconline.in
Detailed Observation	The application does not properly validate user-supplied input before processing it. As a result, malicious or unexpected input can be accepted and handled by the application, potentially leading to security vulnerabilities such as injection attacks, application errors, or unauthorized behavior.
Vulnerability Reference (CWE/CVE)	CWE-20
Severity	**Medium**
Recommendation	Implement strict server-side input validation for all user inputs. Use allow-lists (whitelisting) instead of block-lists. Validate input length, type, format, and range. Encode or sanitize input before processing or displaying it. Implement centralized validation mechanisms.
Reference	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

MBMC | Water

https://devwater.mbmconline.in/ApplicationPurchase.aspx

MBMCWater — Imperium Solutions

Requirement

First Name: xyz
Middle Name: xyz
Last Name: xyz
Soceity / Building Name / Chawl Name: xyz
Prabhag: मिरा-भाईंदर मनपा, मुख्य कार्यालय
Ward: 9
Address: rty
Enter Address
Enter Address
Pin Code: 401101
Mobile No: 555555555555555555555555555555555555555555
Email: <script>alert(1)</script>
Connection Type: Resident (घरगुती)
Category: Residential Building
Charges: 500.00

Processing...

Co 2014-2017 NP Infoserve. All rights reserved. Version 1.0.0

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

Request

```
X-Microsoftajax: Delta=true
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: https://devwater.mbmconline.in
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://devwater.mbmconline.in/ApplicationPurchase.aspx
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

ctl00%24ScriptManager1=
ctl00%24ContentPlaceHolder1%24updPanel%7Cctl00%24ContentPlaceHolder1%24btnSave&
ctl00_ScriptManager1_HiddenField=&ctl00%24rptParentMenu%24ctl00%24hdnParentMenu=1&
ctl00%24rptParentMenu%24ctl01%24hdnParentMenu=4&ctl00%24rptParentMenu%24ctl02%24hdnParentMenu=5&
ctl00%24rptParentMenu%24ctl03%24hdnParentMenu=10&ctl00%24rptParentMenu%24ctl04%24hdnParentMenu=3
&ctl00%24rptParentMenu%24ctl05%24hdnParentMenu=7&ctl00%24ContentPlaceHolder1%24txtFirstName=xyz&
ctl00%24ContentPlaceHolder1%24txtMiddleName=xyz&ctl00%24ContentPlaceHolder1%24txtLastName=xyz&
ctl00%24ContentPlaceHolder1%24txtSoceityName=xyz&ctl00%24ContentPlaceHolder1%24ddlPrabhag=7&
ctl00%24ContentPlaceHolder1%24ddlWard=9&ctl00%24ContentPlaceHolder1%24txtLandMark=&
ctl00%24ContentPlaceHolder1%24txtAddress1=rty&ctl00%24ContentPlaceHolder1%24txtAddress2=&
ctl00%24ContentPlaceHolder1%24txtAddress3=&ctl00%24ContentPlaceHolder1%24txtPinCode=401101&
ctl00%24ContentPlaceHolder1%24txtMobileNo=
ctl00%24ContentPlaceHolder1%24txtEmail=%3Cscript%3Ealert(1)%3C%2Fscript%3E&
ctl00%24ContentPlaceHolder1%24ddlConnectionType=1&ctl00%24ContentPlaceHolder1%24ddlCategory=1&
ctl00%24ContentPlaceHolder1%24txtCharges=500.00&ctl00%24ContentPlaceHolder1%24hdnApplicationID=-1
&__EVENTTARGET=&__EVENTARGUMENT=&__LASTFOCUS=&__VIEWSTATE=
```

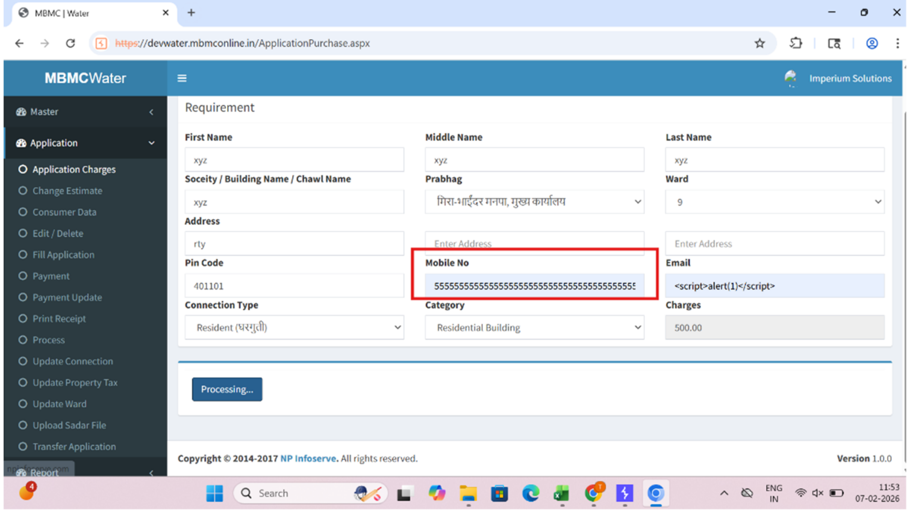
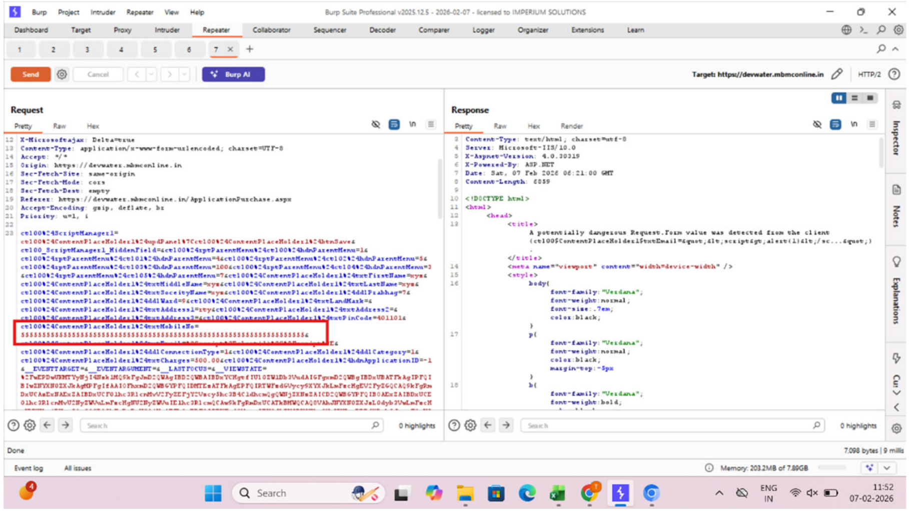
Response

```
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: Sat, 07 Feb 2026 06:21:00 GMT
Content-Length: 6859

<!DOCTYPE html>
<html>
        <head>
              <title>
                    A potentially dangerous Request.Form value was detected from the client
                    (ctl00$ContentPlaceHolder1$txtEmail=&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{
```

4. Missing Length Validation in Phone Numbers

Vulnerability Title	***Affected URLs/IP***
Missing Length Validation in Phone Numbers	devwater.mbmconline.in

Detailed Observation	The application does not enforce proper length validation on phone number input fields. As a result, users can submit phone numbers with invalid or excessive lengths, which may lead to improper input handling and increase the risk of injection, logic bypass, or application errors.

Vulnerability Reference (CWE/CVE)	CWE-20
Severity	**Medium**
Recommendation	Enforce strict length validation for phone number inputs (e.g., exactly 10 digits for Indian mobile numbers). Validate input on both client-side and server-side. Allow only numeric characters and reject special characters. Implement proper error messages for invalid input.
Reference	https://techdocs.akamai.com/identity-cloud/docs/the-minimum-length-validation
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

MBMC | Water

https://devwater.mbmconline.in/ApplicationPurchase.aspx

MBMCWater

Imperium Solutions

Requirement

First Name: xyz

Middle Name: xyz

Last Name: xyz

Soceity / Building Name / Chawl Name: xyz

Prabhag: मिरा-भाईंदर मनपा, मुख्य कार्यालय

Ward: 9

Address: rty

Enter Address

Enter Address

Pin Code: 401101

Mobile No: 5555555555555555555555555555555555555555

Email: <script>alert(1)</script>

Connection Type: Resident (घरगुती)

Category: Residential Building

Charges: 500.00

Processing...

Copyright © 2014-2017 NP Infoserve. All rights reserved.

Version 1.0.0

Burp Suite Professional v2025.12.5 - 2026-02-07 - licensed to IMPERIUM SOLUTIONS

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

Request

```
X-Microsoftajax: Delta=true
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: https://devwater.mbmconline.in
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://devwater.mbmconline.in/ApplicationPurchase.aspx
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

ctl00%24ScriptManager1=
ctl00%24ContentPlaceHolder1%24updPanel1%7Cctl00%24ContentPlaceHolder1%24btnSave&
ctl00_ScriptManager1_HiddenField=&ctl00%24rptParentMenu%24ctl00%24hdnParentMenu=1&
ctl00%24rptParentMenu%24ctl01%24hdnParentMenu=4&ctl00%24rptParentMenu%24ctl02%24hdnParentMenu=5&
ctl00%24rptParentMenu%24ctl03%24hdnParentMenu=100&ctl00%24rptParentMenu%24ctl04%24hdnParentMenu=3
&ctl00%24rptParentMenu%24ctl05%24hdnParentMenu=7&ctl00%24ContentPlaceHolder1%24txtFirstName=xyz&
ctl00%24ContentPlaceHolder1%24txtMiddleName=xyz&ctl00%24ContentPlaceHolder1%24txtLastName=xyz&
ctl00%24ContentPlaceHolder1%24txtSoceityName=xyz&ctl00%24ContentPlaceHolder1%24ddlPrabhag=7&
ctl00%24ContentPlaceHolder1%24ddlWard=9&ctl00%24ContentPlaceHolder1%24txtLandMark=&
ctl00%24ContentPlaceHolder1%24txtAddress1=rty&ctl00%24ContentPlaceHolder1%24txtAddress2=&
ctl00%24ContentPlaceHolder1%24txtAddress3=&ctl00%24ContentPlaceHolder1%24txtPinCode=401101&
ctl00%24ContentPlaceHolder1%24txtMobileNo=
5555555555555555555555555555555555555555555555555555555555555555&
ctl00%24ContentPlaceHolder1%24ddlConnectionType=1&ctl00%24ContentPlaceHolder1%24ddlCategory=1&
ctl00%24ContentPlaceHolder1%24txtCharges=500.00&ctl00%24ContentPlaceHolder1%24hdnApplicationID=-1
&__EVENTTARGET=&__EVENTARGUMENT=&__LASTFOCUS=&__VIEWSTATE=
```

Response

```
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 06:21:00 GMT
Content-Length: 6859

<!DOCTYPE html>
<html>
    <head>
        <title>
            A potentially dangerous Request.Form value was detected from the client
            (ctl00$ContentPlaceHolder1$txtEmail="&lt;script&gt;alert(1)&lt;/sc...").
        </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{
                font-family:"Verdana";
                font-weight:bold;
```

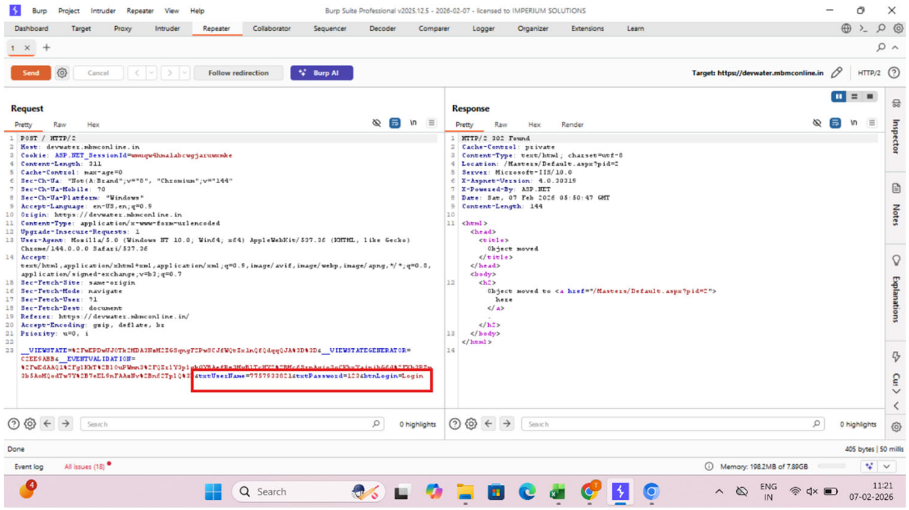
Done

7,098 bytes | 9 millis

Memory: 203.2MB of 7.89GB

5. Clear Text Password Transmission in Login Request

Vulnerability Title		***Affected URLs/IP***
Clear Text Password Transmission in Login Request		devwater.mbmconline.in
Detailed Observation	Clear text password transmission occurs when user credentials are sent from the client to the server without proper encryption or protection. This allows attackers to view sensitive information such as usernames and passwords in readable format. During the security assessment, it was observed that the application transmits the password parameter in plain readable text within the HTTP request.	
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.)	
Reference	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	
New/ Repeat Observation	New Observation	

References to evidences / Proof of Concept (POCs)	

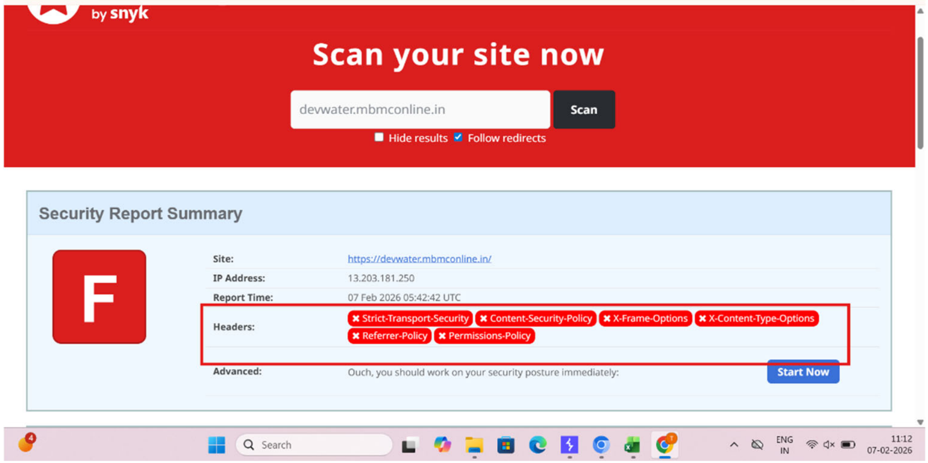
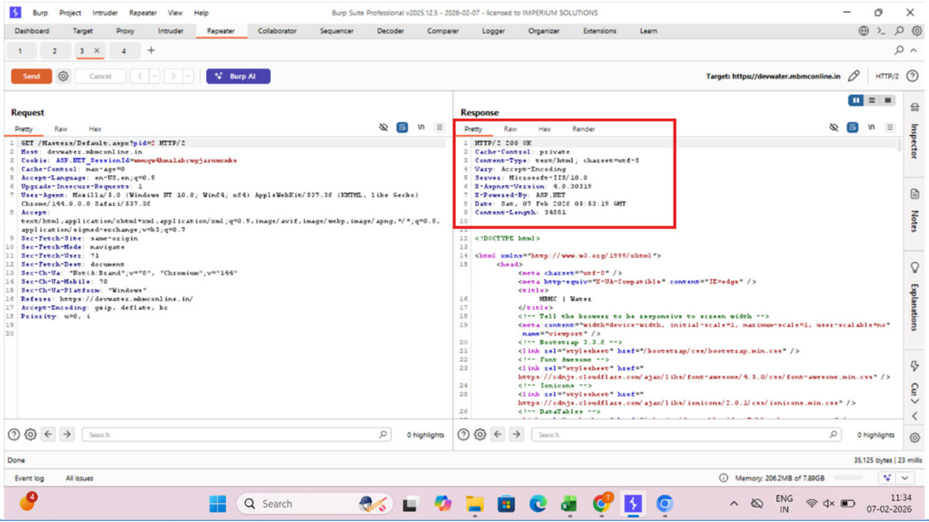
Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.12.5 - 2026-02-07 - licensed to IMPERIUM SOLUTIONS
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Follow redirection Burp AI
Target: https://devwater.mbmconline.in HTTP/2
Request Pretty Raw Hex
Response Pretty Raw Hex Render
Inspector Notes Explanations
0 highlights
Done
405 bytes | 50 millis
Event log All issues (18)
Memory: 198.2MB of 7.89GB
ENG IN 11:21 07-02-2026

```
POST / HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hmalabcwgjaruwxmke
Content-Length: 311
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://devwater.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://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

__VIEWSTATE=%2FwEPDwUJOTk2MDA3NzM2ZGSqngF2Pw8CJfWQtZx1nQfQdqqQJA%3D%3D&__VIEWSTATEGENERATOR=
C2EE9ABB&__EVENTVALIDATION=
%2FwEdAAQ1%2Fg1EkT%2B1OuPWmn3%2FQZz1Y3pl
3b5AoMQodTw7Y%2B7eEL9nFAAaNv%2Bn62Tp1Q%3&txtUserName=7757933821&txtPassword=123&btnLogin=Login
```

```
HTTP/2 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Masters/Default.aspx?pid=2
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 05:50:47 GMT
Content-Length: 144

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

6. Missing Security Headers

Vulnerability Title	***Affected URLs/IP***
Missing Security Headers	devwater.mbmconline.in
Detailed Observation	The application does not implement one or more recommended HTTP security headers. Security headers help browsers enforce security controls that reduce the risk of common web attacks such as Cross-Site Scripting (XSS), Clickjacking, MIME-type sniffing, and information disclosure. Absence of these headers weakens the overall security posture of the application.
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=()

Reference	https://www.invicti.com/blog/web-security/missing-http-security-headers
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

Security Report Summary

F

Site:	https://devwater.mbmconline.in/
IP Address:	13.203.181.250
Report Time:	07 Feb 2026 05:42:42 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:

Request

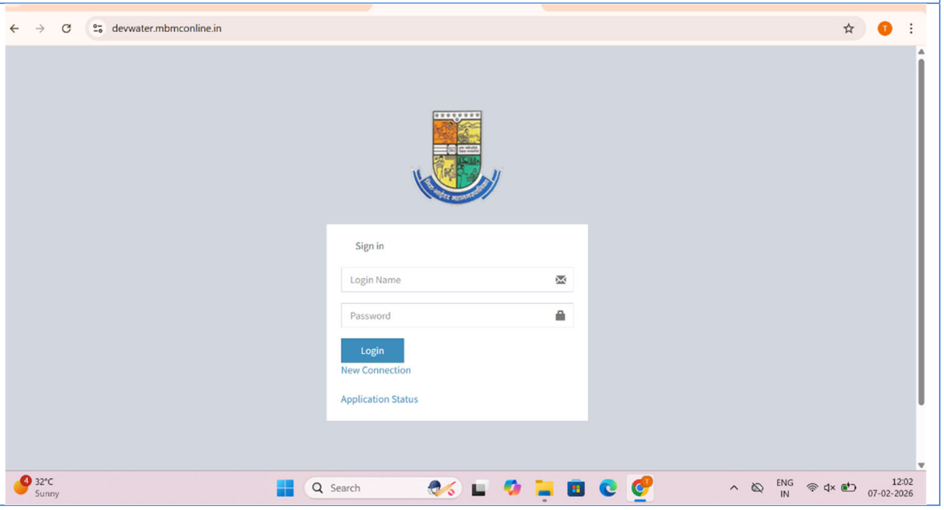
```
GET /Masters/Default.aspx?pid=2 HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hwalabcwgjaruwxske
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
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://devwater.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: Sat, 07 Feb 2026 05:53:19 GMT
Content-Length: 34881


<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <meta charset="utf-8" />
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <title>
                  MBMC | Water
            </title>
            <!-- Tell the browser to be responsive to screen width -->
            <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"
             name="viewport" />
            <!-- Bootstrap 3.3.6 -->
            <link rel="stylesheet" href="/bootstrap/css/bootstrap.min.css" />
            <!-- Font Awesome -->
            <link rel="stylesheet" href="
            https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.5.0/css/font-awesome.min.css" />
            <!-- Ionicons -->
            <link rel="stylesheet" href="
            https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css" />
            <!-- DataTables -->
```

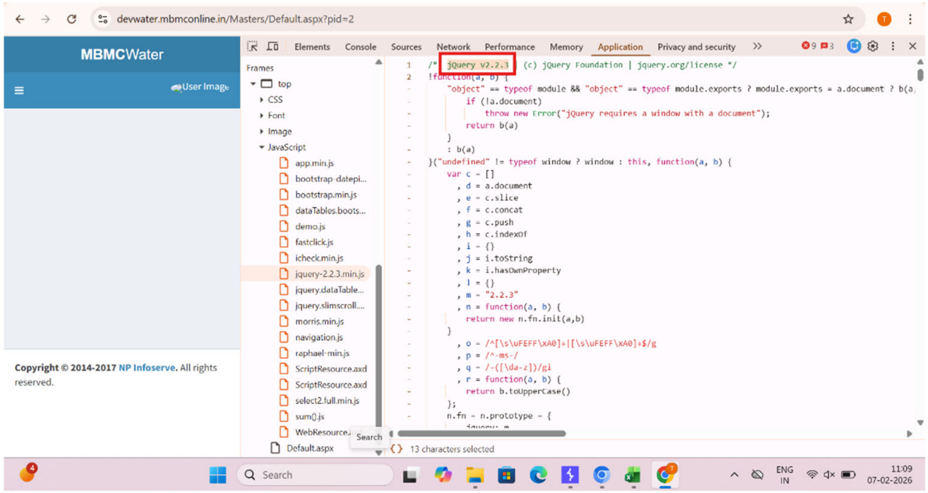
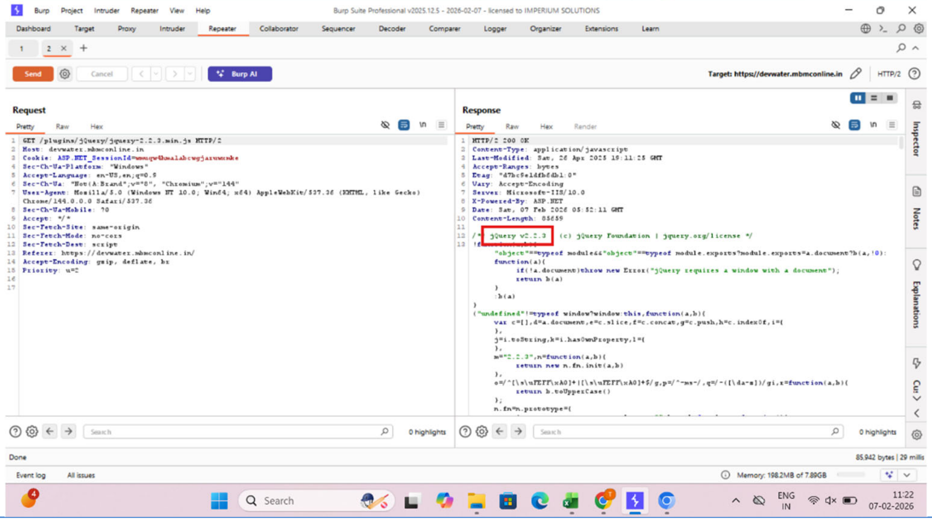
7. Captcha Not Implemented

Vulnerability Title	***Affected URLs/IP***
Captcha Not Implemented	devwater.mbmconline.in
Detailed Observation	The application does not implement CAPTCHA protection on sensitive functionalities such as login, registration, password reset, or OTP requests. The absence of CAPTCHA increases the risk of automated bot attacks and brute-force attempts.
Vulnerability Reference (CWE/CVE)	CWE-307

Severity	**Medium**
Recommendation	Implement CAPTCHA on authentication and sensitive transaction pages. Apply CAPTCHA after multiple failed login or OTP attempts. Use advanced bot detection mechanisms such as Google reCAPTCHA or equivalent solutions. Implement rate limiting along with CAPTCHA protection.
Reference	https://stackoverflow.com/questions/34016388/trying-to-implement-the-new-google-captcha
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

8. Out of Date (jQuery Version)

Vulnerability Title	***Affected URLs/IP***
Out of date (jQuery Version)	devwater.mbmconline.in
Detailed Observation	The web application is using jQuery version 2.2.3, which is an outdated JavaScript library. This version is affected by known security vulnerabilities, including issues related to Cross-Site Scripting (XSS), which have been addressed in later releases. Use of outdated client-side libraries may allow attackers to exploit known weaknesses in the application's front-end components.
Vulnerability Reference (CWE/CVE)	CWE-1104
Severity	**Medium**

Recommendation	Upgrade jQuery to the latest stable version (v3.7.1 or above). Remove unused or legacy jQuery functions. Regularly review third-party libraries for security updates. Implement dependency monitoring as part of the SDLC.
Reference	https://github.com/jquery/jquery/security/advisories
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

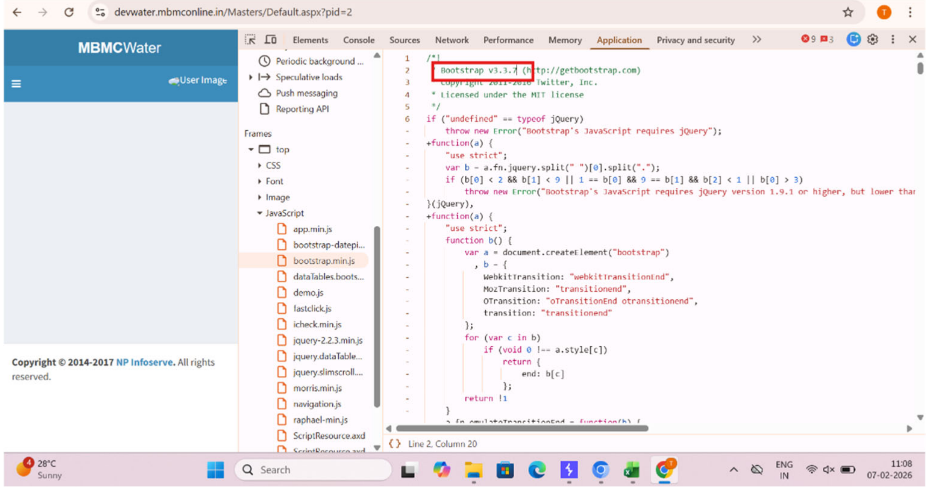
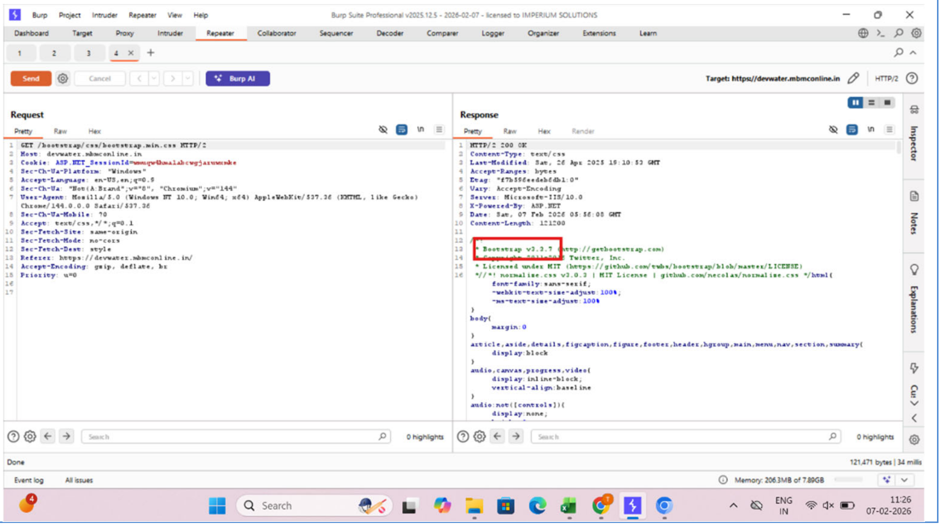
```
/* jQuery v2.2.3 | (c) jQuery Foundation | jquery.org/license */
!function(a, b) {
    "object" == typeof module && "object" == typeof module.exports ? module.exports = a.document ? b(a,
        if (!a.document)
            throw new Error("jQuery requires a window with a document");
        return 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 = "2.2.3"
      , 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 /plugins/jQuery/jquery-2.2.3.min.js HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wwuqw4hwalabcwgjaruwmke
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://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=2
```

```
HTTP/2 200 OK
Content-Type: application/javascript
Last-Modified: Sat, 26 Apr 2025 19:11:25 GMT
Accept-Ranges: bytes
Etag: "d7bc9e1dfb6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 05:52:11 GMT
Content-Length: 85659

/*! jQuery v2.2.3 | (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="2.2.3",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. Out of Date (Bootstrap Version)

Vulnerability Title	***Affected URLs/IP***
Out of date (Bootstrap Version)	devwater.mbmconline.in

Detailed Observation	The application is using an outdated version of the Bootstrap framework. Older Bootstrap versions contain known security vulnerabilities and bugs that have been publicly disclosed. Attackers may exploit these weaknesses to perform client-side attacks such as Cross-Site Scripting (XSS), UI manipulation, or denial of service.
Vulnerability Reference (CWE/CVE)	CWE-1104
Severity	**Medium**
Recommendation	Upgrade Bootstrap to the latest stable and supported version. Remove unused or deprecated Bootstrap components. Regularly monitor third-party libraries for security updates. Implement a dependency management and patching process.
Reference	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/out-of-date-version-bootstrap
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 

devwater.mbmconline.in/Masters/Default.aspx?pid=2

Copyright © 2014-2017 NP Infoserve. All rights reserved.

```
/*!
 * 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
    }
```

Line 2, Column 20

Burp Suite Professional v2025.12.5 - 2026-02-07 - licensed to IMPERIUM SOLUTIONS

Target: https://devwater.mbmconline.in

Request

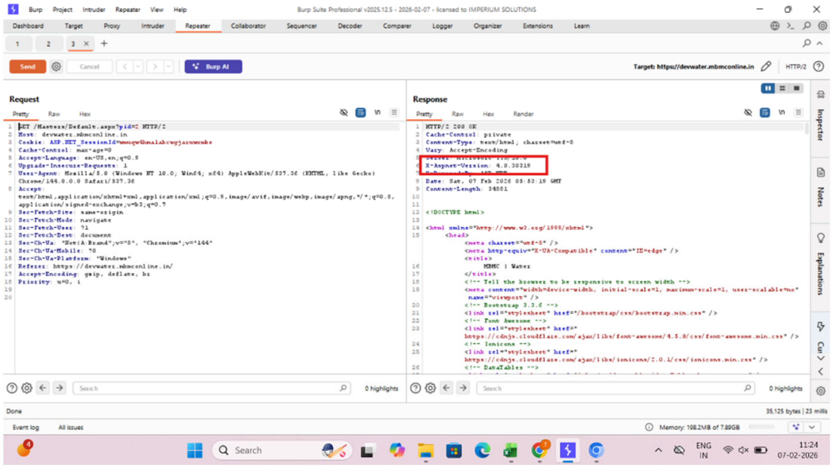
```
GET /bootstrap/css/bootstrap.min.css HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hwalabcwgjaruwmke
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/144.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

Response

```
HTTP/2 200 OK
Content-Type: text/css
Last-Modified: Sat, 26 Apr 2025 19:10:53 GMT
Accept-Ranges: bytes
Etag: "f7b596eedeb6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 05:56:08 GMT
Content-Length: 121200

/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{
    font-family:sans-serif;
    -webkit-text-size-adjust:100%;
    -ms-text-size-adjust:100%
}
body{
    margin:0
}
article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{
    display:block
}
audio,canvas,progress,video{
    display:inline-block;
    vertical-align:baseline
}
audio:not([controls]){
    display:none;
```

121,471 bytes | 34 millis

10. Out of Date (X-Asp.Net)

Vulnerability Title	***Affected URLs/IP***
Out of Date (X-Asp.Net)	devwater.mbmconline.in
Detailed Observation	The application discloses and uses an outdated version of the ASP.NET framework (X-AspNet-Version: 4.0.30319). Older ASP.NET versions contain publicly known security vulnerabilities that may be exploited by attackers to compromise the application.
Vulnerability Reference (CWE/CVE)	CWE-1104
Severity	**Low**
Recommendation	Upgrade the application to the latest supported ASP.NET / .NET Framework version. Apply the latest security patches from Microsoft. Disable version disclosure headers (X-AspNet-Version, X-Powered-By). Regularly monitor and update application frameworks and dependencies.
Reference	https://stackoverflow.com/questions/12561370/how-to-expire-a-link
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

Target: https://devwater.mbmconline.in

Request

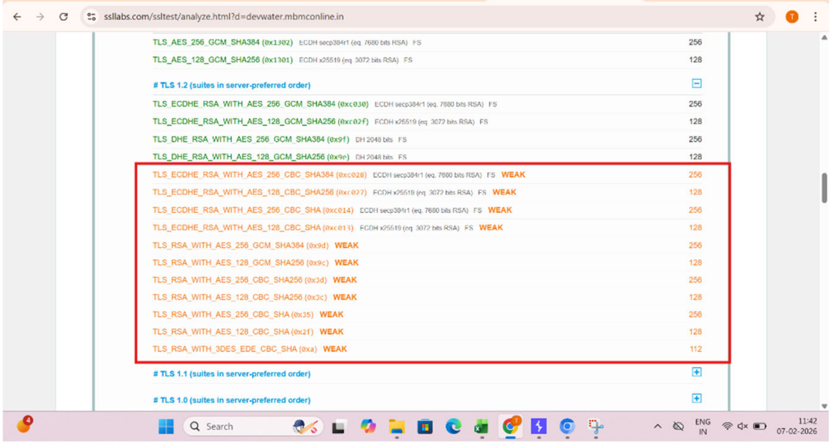
```
GET /Masters/Default.aspx?pid=2 HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hmalabcwgjaruwmke
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
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://devwater.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: Sat, 07 Feb 2026 05:53:19 GMT
Content-Length: 34881


<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <meta charset="utf-8" />
        <meta http-equiv="X-UA-Compatible" content="IE=edge" />
        <title>
            MBMC | Water
        </title>
        <!-- Tell the browser to be responsive to screen width -->
        <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"
         name="viewport" />
        <!-- Bootstrap 3.3.6 -->
        <link rel="stylesheet" href="/bootstrap/css/bootstrap.min.css" />
        <!-- Font Awesome -->
        <link rel="stylesheet" href="
        https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.5.0/css/font-awesome.min.css" />
        <!-- Ionicons -->
        <link rel="stylesheet" href="
        https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css" />
        <!-- DataTables -->
```

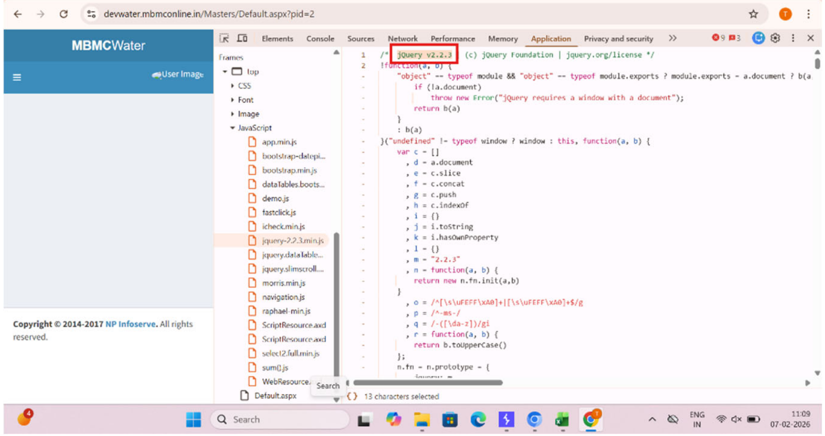
35,125 bytes | 23 millis

11. Weak Ciphers

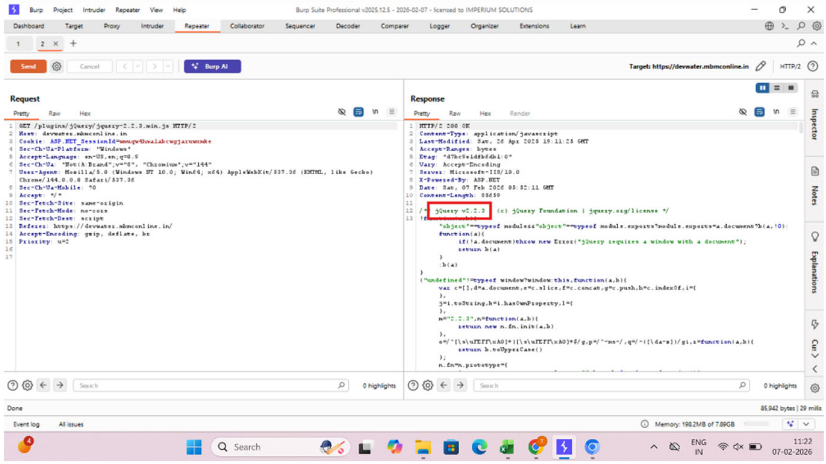
Vulnerability Title	***Affected URLs/IP***
Weak Ciphers	devwater.mbmconline.in
Detailed Observation	The application server is configured to support multiple weak SSL/TLS cipher suites under TLS 1.2. These cipher suites rely on outdated cryptographic mechanisms such as CBC mode encryption and RSA key exchange, which are vulnerable to known cryptographic attacks. The presence of these weak cipher suites may allow an attacker to downgrade the encryption strength and potentially compromise the confidentiality and integrity of data transmitted between the client and the server.
Vulnerability Reference (CWE/CVE)	CWE-326
Severity	**Medium**
Recommendation	Disable all weak and legacy cipher suites. Remove CBC-based and RSA key exchange cipher suites. Allow only strong modern cipher suites such as: AES-GCM, CHACHA20-POLY1305. Enforce TLS 1.2 (secure ciphers only) and TLS 1.3. Regularly review SSL/TLS configurations Recommended Cipher Examples: TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256
Reference	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	 ssllabs.com/ssltest/analyze.html?d=devwater.mbmconline.in TLS_AES_256_GCM_SHA384 (0x1302) ECDH secp384r1 (eq. 7680 bits RSA) FS 256 TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS 128 # TLS 1.2 (suites in server-preferred order) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp384r1 (eq. 7680 bits RSA) FS 256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS 128 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS 256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS 128 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp384r1 (eq. 7680 bits RSA) FS WEAK 256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp384r1 (eq. 7680 bits RSA) FS WEAK 256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128 TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK 256 TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 128 TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK 256 TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 128 TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK 256 TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 128 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK 112 # TLS 1.1 (suites in server-preferred order) # TLS 1.0 (suites in server-preferred order)

12. Version Disclosure (jQuery)

Vulnerability Title	***Affected URLs/IP***
Version Disclosure (jQuery)	devwater.mbmconline.in

Detailed Observation	it was observed that the application discloses the jQuery library version information within client-side JavaScript files or page source code. Exposing the exact jQuery version allows attackers to fingerprint the application technology stack and identify known vulnerabilities associated with that specific version, which may aid in targeted attacks.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	Avoid exposing exact jQuery version details in production environments. Minify and bundle JavaScript files. Remove version comments and banners from client-side resources. Keep jQuery updated to the latest stable version.
Reference	https://owasp.org/www-community/attacks/Information_Disclosure
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

```
/* jQuery v2.2.3 | (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 = "2.2.3"
      , 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 = {
```

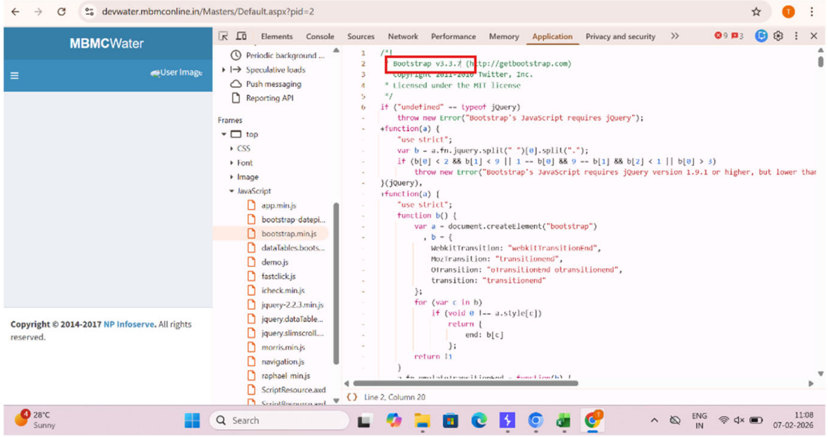
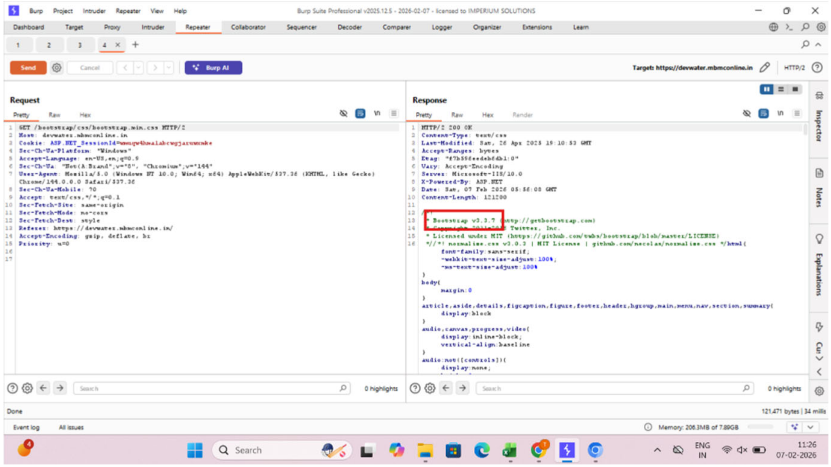
	

```
GET /plugins/jQuery/jquery-2.2.3.min.js HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wwuqw4hwalabcwgjaruwcnke
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (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://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=2
```

```
HTTP/2 200 OK
Content-Type: application/javascript
Last-Modified: Sat, 26 Apr 2025 19:11:25 GMT
Accept-Ranges: bytes
Etag: "d7bc9e1dfb6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 05:52:11 GMT
Content-Length: 85659

/*! jQuery v2.2.3 | (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="2.2.3",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={
```

13. Version Disclosure (Bootstrap)

Vulnerability Title	***Affected URLs/IP***
Version Disclosure (Bootstrap)	devwater.mbmconline.in
Detailed Observation	The application discloses the Bootstrap framework version through client-side files or HTML source code. Version disclosure allows attackers to identify the exact library version in use, which can help them target known vulnerabilities associated with that version.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	Remove or obfuscate version comments and metadata from HTML/JS files. Upgrade to the latest Bootstrap version. Avoid exposing framework versions in client-side responses.
Reference	https://owasp.org/www-community/attacks/Information_Disclosure
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)	 

devwater.mbmconline.in/Masters/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
    }
```

Request

```
GET /bootstrap/css/bootstrap.min.css HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hwalabcwgjaruwxnke
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: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

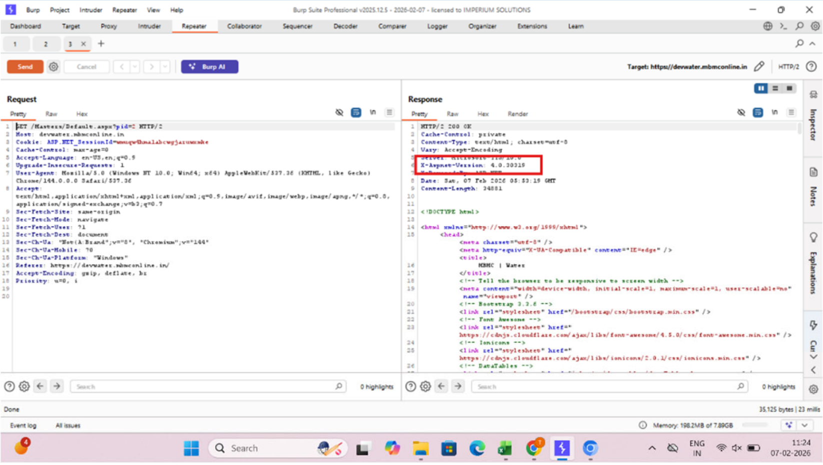
Response

```
HTTP/2 200 OK
Content-Type: text/css
Last-Modified: Sat, 26 Apr 2025 19:10:53 GMT
Accept-Ranges: bytes
Etag: "f7b59deedeb6db1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 05:56:08 GMT
Content-Length: 121200

/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{
     font-family:sans-serif;
     -webkit-text-size-adjust:100%;
     -ms-text-size-adjust:100%
}
body{
     margin:0
}
article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{
     display:block
}
audio,canvas,progress,video{
     display:inline-block;
     vertical-align:baseline
}
audio:not([controls]){
     display:none;
```

14. Version Disclosure (X-Asp.Net)

Vulnerability Title	***Affected URLs/IP***
Version Disclosure (X-Asp.Net)	devwater.mbmconline.in

Detailed Observation	The application discloses the ASP.NET framework version through HTTP response headers. The X-AspNet-Version header reveals internal technology details, which can aid attackers during reconnaissance to identify known vulnerabilities associated with the disclosed version.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**

Recommendation	Remove or disable the X-AspNet-Version HTTP header. Remove the X-Powered-By header if enabled. Ensure server and framework configurations do not expose internal version details.
Reference	https://stackoverflow.com/questions/12561370/how-to-expire-a-link
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.12.5 - 2026-02-07 - licensed to IMPERIUM SOLUTIONS
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3
Send
Cancel
Burp AI
Target: https://devwater.mbmconline.in
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Explanations
Search
0 highlights
Done
35,125 bytes | 23 millis
Event log All issues
Memory: 198.2MB of 7.89GB
Search
ENG IN
11:24 07-02-2026

Request

```
GET /Masters/Default.aspx?pid=2 HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hmalabcwgjaruwxmke
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://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

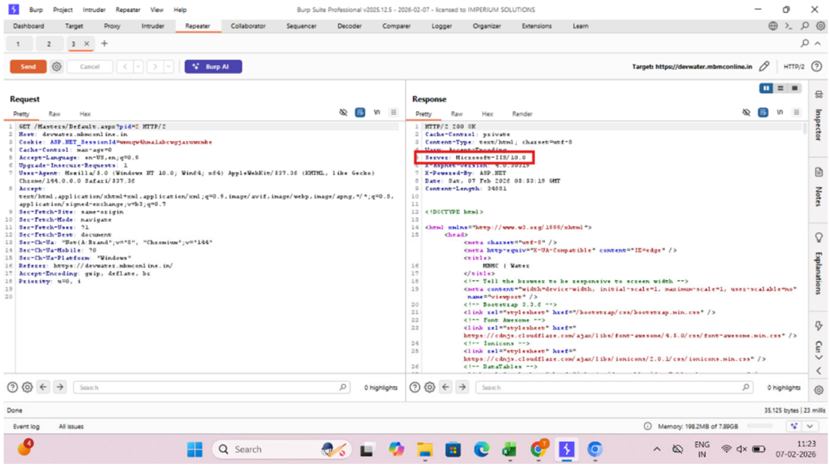
Response

```
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: Sat, 07 Feb 2026 05:53:19 GMT
Content-Length: 24881


<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
      <head>
            <meta charset="utf-8" />
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <title>
                  MBMC | Water
            </title>
            <!-- Tell the browser to be responsive to screen width -->
            <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"
             name="viewport" />
            <!-- Bootstrap 3.3.6 -->
            <link rel="stylesheet" href="/bootstrap/css/bootstrap.min.css" />
            <!-- Font Awesome -->
            <link rel="stylesheet" href="
            https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.5.0/css/font-awesome.min.css" />
            <!-- Ionicons -->
            <link rel="stylesheet" href="
            https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css" />
            <!-- DataTables -->
```

15. Server Version Disclosure

Vulnerability Title	***Affected URLs/IP***
Server Version Disclosure	devwater.mbmconline.in

Detailed Observation	The application discloses the web server type and version in HTTP response headers. The Server header reveals internal infrastructure details (Microsoft-IIS/10.0), which can assist attackers during reconnaissance to identify server-specific vulnerabilities and tailor attacks accordingly.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	Remove or obfuscate the Server HTTP response header. Apply latest security patches to the web server. Implement secure header configurations.

Reference	https://serverfault.com/questions/991045/remove-modify-iis-10-server-header-which-discloses-iis-version
New/ Repeat Observation	New Observation
References to evidences / Proof of Concept (POCs)	

Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.12.5 - 2026-02-07 - licensed to IMPERIUM SOLUTIONS
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3
Send Cancel Burp AI
Target: https://devwater.mbmconline.in HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Explanations
0 highlights
Done
35,125 bytes | 23 millis
Event log All issues
Memory: 198.2MB of 7.89GB
Search
ENG IN
11:23
07-02-2026

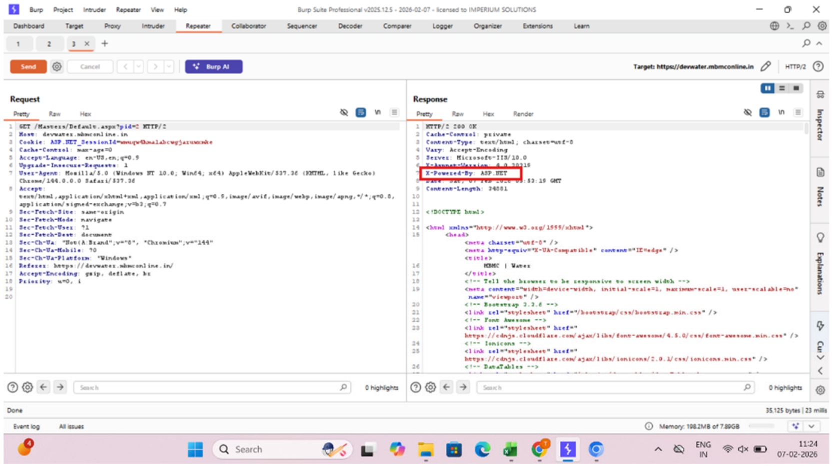
```
GET /Masters/Default.aspx?pid=2 HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wmuqw4hwalabcwgjaruwcnke
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
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://devwater.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: Sat, 07 Feb 2026 05:53:19 GMT
Content-Length: 34881


<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <meta charset="utf-8" />
        <meta http-equiv="X-UA-Compatible" content="IE=edge" />
        <title>
            MBMC | Water
        </title>
        <!-- Tell the browser to be responsive to screen width -->
        <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"
         name="viewport" />
        <!-- Bootstrap 3.3.6 -->
        <link rel="stylesheet" href="/bootstrap/css/bootstrap.min.css" />
        <!-- Font Awesome -->
        <link rel="stylesheet" href="
        https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.5.0/css/font-awesome.min.css" />
        <!-- Ionicons -->
        <link rel="stylesheet" href="
        https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css" />
        <!-- DataTables -->
```

16. Stack Disclosure

Vulnerability Title	***Affected URLs/IP***
Stack Disclosure	devwater.mbmconline.in

Detailed Observation	The application discloses backend technology details through the X-Powered-By HTTP response header. This header reveals that the application is built using ASP.NET, which provides attackers with useful information during reconnaissance to identify framework-specific vulnerabilities.
Vulnerability Reference (CWE/CVE)	CWE-200
Severity	**Low**
Recommendation	Disable the X-Powered-By HTTP response header. Avoid exposing internal technology details in HTTP responses. Apply secure server hardening and header management.
Reference	https://learn.microsoft.com/en-us/aspnet/core/security/headers
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)	

Request

```
GET /Masters/Default.aspx?pid=2 HTTP/2
Host: devwater.mbmconline.in
Cookie: ASP.NET_SessionId=wwuqw4hmalabcwgjaruwmke
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://devwater.mbmconline.in/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

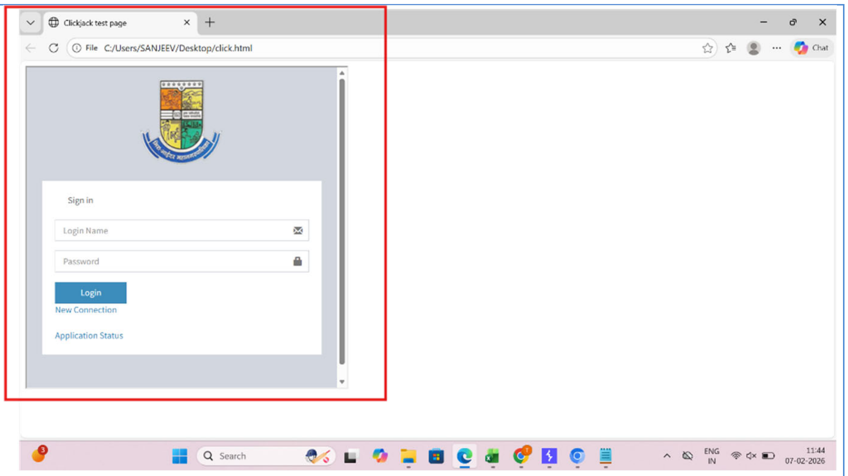
```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 07 Feb 2026 05:53:19 GMT
Content-Length: 34881


<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
	<head>
		<meta charset="utf-8" />
		<meta http-equiv="X-UA-Compatible" content="IE=edge" />
		<title>
			MBMC | Water
		</title>
		<!-- Tell the browser to be responsive to screen width -->
		<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"
		 name="viewport" />
		<!-- Bootstrap 3.3.6 -->
		<link rel="stylesheet" href="/bootstrap/css/bootstrap.min.css" />
		<!-- Font Awesome -->
		<link rel="stylesheet" href="
		https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.5.0/css/font-awesome.min.css" />
		<!-- Ionicons -->
		<link rel="stylesheet" href="
		https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/css/ionicons.min.css" />
		<!-- DataTables -->
```

Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.12.5 - 2026-02-07 - licensed to IMPERIUM SOLUTIONS
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3
Send Cancel Burp AI
Target: https://devwater.mbmconline.in HTTP/2
Pretty Raw Hex Render
Search 0 highlights
Inspector Notes Explanations
Done
35,125 bytes | 23 millis
Event log All issues
Memory: 198.2MB of 7.89GB
Search
ENG IN
11:24
07-02-2026

17. Clickjacking

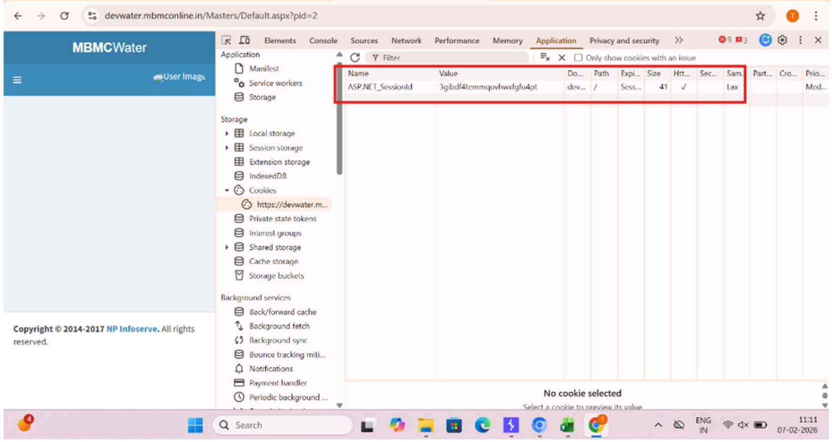
Vulnerability Title	***Affected URLs/IP***
Clickjacking	devwater.mbmconline.in

Detailed Observation	The application does not implement proper frame-busting protections, allowing it to be embedded within an iframe on a malicious website. This could enable clickjacking attacks, where users are tricked into clicking on hidden or disguised elements, potentially leading to unauthorized actions.
Vulnerability Reference (CWE/CVE)	CWE-1021
Severity	**Low**
Recommendation	Implement X-Frame-Options header (DENY or SAMEORIGIN). Configure Content-Security-Policy with frame-ancestors 'self'. Validate frame usage only for trusted domains if framing is required.
Reference	https://learn.microsoft.com/en-us/aspnet/core/security/headers
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)	 Clickjack test page File C:/Users/SANJEEV/Desktop/click.html Chat Sign in Login Name Password Login New Connection Application Status Search ENG IN 11:44 07-02-2026

18. Cookies Not Marked Secure

Vulnerability Title	***Affected URLs/IP***
Cookies Not Marked Secure	devwater.mbmconline.in
Detailed Observation	The application sets cookies without the Secure attribute. Cookies missing this flag may be transmitted over unencrypted HTTP connections, making them vulnerable to interception by attackers through man-in-the-middle (MITM) attacks.
Vulnerability Reference (CWE/CVE)	CWE-614
Severity	**Low**
Recommendation	Set the Secure flag on all cookies, especially session and authentication cookies. Ensure cookies are transmitted only over HTTPS. Additionally, enable HttpOnly and SameSite attributes for better protection. Set-Cookie: sessionid=abc123; Secure; HttpOnly; SameSite=Strict
Reference	https://owasp.org/www-community/controls/SecureCookieAttribute
New/ Repeat Observation	New Observation

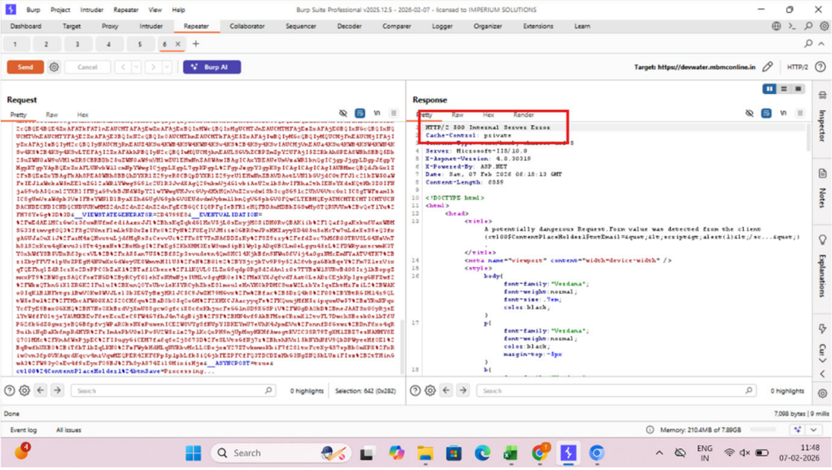
References to evidences / Proof of Concept (POCs)	 devwater.mbmconline.in/Masters/Default.aspx?pid=2 MBMCWater Name: ASP.NET_SessionId · Value: 3gibdf4temmqovhwxfgfu4pt · Do...: dev... · Path: / · Expi...: Sess... · Size: 41 · Htt...: ✓ · Sam...: Lax · Prio...: Med... No cookie selected Select a cookie to preview its value Copyright © 2014-2017 NP Infoserve. All rights reserved.

19. Internal Server Error

Vulnerability Title	***Affected URLs/IP***
Internal Server Error	devwater.mbmconline.in

Detailed Observation	The application returns HTTP 500 Internal Server Error responses when unexpected or malformed input is provided. This indicates improper exception handling and may expose internal application behavior, increasing the risk of information leakage and further exploitation.
Vulnerability Reference (CWE/CVE)	CWE-209
Severity	**Low**
Recommendation	Implement proper exception handling and return generic error messages to users. Disable detailed error messages and stack traces in production environments. Log detailed errors securely on the server side for debugging. Validate and sanitize all user inputs to prevent unexpected errors.
Reference	https://stackoverflow.com/questions/5385714/deploying-website-500-internal-server-error
New/ Repeat Observation	New Observation

References to evidences / Proof of Concept (POCs)

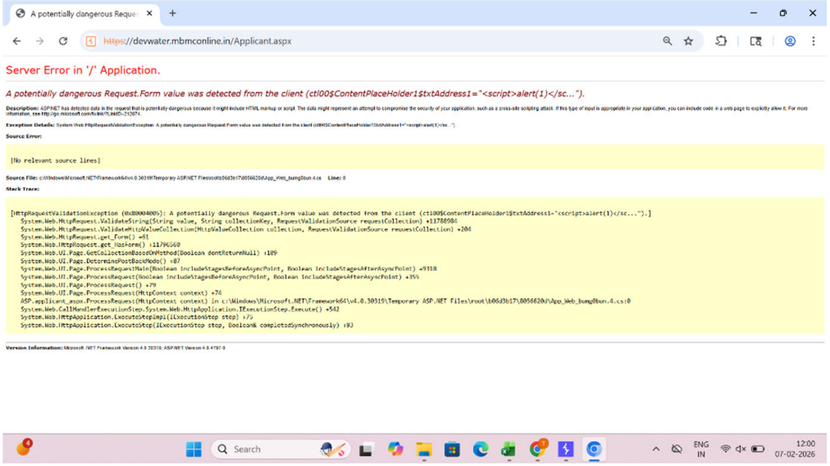


Target: https://devwater.mbmconline.in

```
[illegible]
__VIEWSTATEGENERATOR=CD4758E8&__EVENTVALIDATION=
[illegible]
__ASYNCPOST=true&
ctl00%24ContentPlaceHolder1%24btnSave=Processing...
```

```
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: Sat, 07 Feb 2026 06:18:13 GMT
Content-Length: 6859

<!DOCTYPE html>
<html>
    <head>
        <title>
            A potentially dangerous Request.Form value was detected from the client
            (ctl00$ContentPlaceHolder1$txtEmail=&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{
```

Burp Suite Professional v2025.12.5 - 2026-02-07 - 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
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector Notes Explanations
0 highlights Selection: 642 (0x282)
0 highlights
Done
7,098 bytes | 9 millis
Event log All issues
Memory: 210.4MB of 7.89GB
Search
ENG IN
11:48
07-02-2026



https://devwater.mbmconline.in/Applicant.aspx

Server Error in '/' Application.

A potentially dangerous Request.Form value was detected from the client (ctl00$ContentPlaceHolder1$txtAddress1="<script>alert(1)</sc...").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkID=212874.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.Form value was detected from the client (ctl00$ContentPlaceHolder1$txtAddress1="<script>alert(1)</sc...").

Source Error:

```
[No relevant source lines]
```

Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\b06d3b17\8056620d\App_Web_bumg0bun.4.cs   **Line:** 0

Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (ctl00$ContentPlaceHolder1$txtAddress1="<script>alert(1)</sc...").]
   System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11788984
   System.Web.HttpRequest.ValidateHttpValueCollection(HttpValueCollection collection, RequestValidationSource requestCollection) +204
   System.Web.HttpRequest.get_Form() +61
   System.Web.HttpRequest.get_HasForm() +11796560
   System.Web.UI.Page.GetCollectionBasedOnMethod(Boolean dontReturnNull) +109
   System.Web.UI.Page.DeterminePostBackMode() +87
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9318
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +355
   System.Web.UI.Page.ProcessRequest() +79
   System.Web.UI.Page.ProcessRequest(HttpContext context) +74
   ASP.applicant_aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\b06d3b17\8056620d\App_Web_bumg0bun.4.cs:0
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +542
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +75
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +93
```

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