Information Disclosed on own Initiative
DIRECTORATE GENERAL OF SHIPPING
www.dgshipping.gov.in

Date last updated (09.07.2025)

S.No	Item	Details of Disclosure
6.2	Guidelines for Indian Government Websites (GIGW) is followed (released in February, 2009 and included in the Central Secretariat Manual of Office Procedures (CSMOP) by Department of Administrative Reforms and public Grievances, Ministry of Personnel, Public Grievance and pensions, Govt. of India	I. Whether STQC certification obtained and its validity.: No, Process of new website is on going. However Final Web Application Security Audit of Directorate General of Shipping has been done and the CERT In report for the New DGS Website has been received which is attached here with. II. Does the Website show the certificate on the Website?: No **E. Guidelines for Indian Government Websites (GIGW) is followed:** **No**. The existing DGS website is currently undergoing a complete revamp to ensure full compliance with the GIGW (Guidelines for Indian Government Websites) framework, which prescribes accessibility, usability, transparency, and security. The New DGS Website is expected to go live by end of July 2025.

DR CBS CYBER SECURITY SERVICES LLP

LLP Id No. AAK-4058

CERT-In Empanelled Information Security Auditing Organization (2020-2027)
Certified ISO 9001:2015 (No. IAS0508Q2286), ISO/IEC 27001,
Certified ISO/IEC 27001:2022 (No. IN/26314557/3260)

Saturday, 05th July 2025

To,

Shri Deependra Singh Bisen,
Deputy Director General of Shipping,
Director General of Shipping
9th Floor Beta Building, i-Think Techno Campus, Kanjurmarg East,
Mumbai, Maharashtra 400042

Sub: Final Web Application Security Audit Report of Directorate General of Shipping.

Ref No. ITPL/25-26/SW/PO/06 dated 05/06/2025 and link working on 05/06/2025.

Dear Sir,

With above reference, in continuation to the Level-1 security audit report forwarded on **13th June 2025.** and compliance received on **02nd July 2025**.

After compliance verification, the executive summary of Vulnerabilities identified on 04th July 2025 as under :

S.No	Vulnerabilities Discovered in Level-1 Report	Severity	CWE/ CVE	Final Status
1.	Reflected Cross Site Scripting	High	CWE-79	Patched & Closed
2.	Authentication Bypass	High	CWE-306	Patched & Closed
3.	Unrestricted File Upload	High	CWE-434	Patched & Closed
4.	Sensitive Information Disclosure	Medium	CWE-200	Patched & Closed
5.	Unprotected Admin Panel	Medium	CWE-285	Patched & Closed
6.	Clear Text Transmission of Sensitive Information	Medium	CWE-319	Closed
7.	Vulnerable & Outdated Components	Medium	CWE-1104	Patched & Closed
8.	Improper Input Validation	Medium	CWE-20	Patched & Closed
9.	Content Security Policy Bypass	Medium	CWE-693	Patched & Closed
10.	Missing Security Headers	Medium	CWE-693	Patched & Closed
11.	HTTP Methods Allowed	Low	CWE-650	Patched & Closed
12.	Improper Cache Control Header	Low	CWE-525	Patched & Closed
13.	Insecure Transportation Layer Security Version 1.2 Supported	Low	CWE-326	Closed
14.	Cookies without HTTPOnly Flag	Low	CWE-1004	Closed
15.	Cookies without Secure Flag	Low	CWE-614	Patched & Closed

The Hash Value and Path of the audited application is mentioned below:

S.No.	Website/ Portal Name	Test URL	Location	Hash Value provided by auditee	Date & Time of hash value taken / Version
1.	Directorate General of Shipping	https://beta-immortal.com/ https://beta-immortal.com/admin/login	/var/www/dgs	e1c0491b49d0ffe32fc5b872a39a96d1	04th July 2025 & 05:14 PM

Verified By:
DRCBS-22-017

Audited & Documented By:
DRCBS-23-023

The detailed Final Web Security Audit Report of **Directorate General of Shipping**, dated **05th July 2025** prepared by the Audit team is authenticated and attached for your perusal & needful action. Organization must comply with the directions issued by CERT-In vide notification No. 20(3) 2022-CERT-In dated 28.04.2022. The Developer Team of auditee must also follow the Technical Guidelines on Software Bill Of Materials (SBOM) version 1.0 issued by CERT-In dated 03.10.2024.

Thanks & Regards,

CHATUR BHUJ SHARMA
Digitally signed by CHATUR BHUJ SHARMA
Date: 2025.07.05 11:29:16 +05'30'

Dr. CB Sharma IPS (R)
Certified Lead Auditor ISMS (ISO/IEC 27001: 2013)
Founder & CEO

Enclosed: Web Application Security Audit Report of Directorate General of Shipping-Final-Ver2.0

Final Web Application Security Audit Report of Directorate General of Shipping

For

Directorate General of Shipping

Audited By:

DR CBS CYBER SECURITY SERVICES LLP
CERT-In Empanelled Information Security Auditing Organization (2020-2027)
Certified ISO 9001:2015 (No. IN/24614556/4628),
Certified ISO/IEC 27001:2022 (No. IN/26314557/3260)

Saturday, 05th July 2025

Final Security Audit Report

Report Release Date	05th July 2025
Type of Audit	Web Application Audit
Type of Audit Report	Final Audit Report
Period	01st July to 04th July 2025

Document Control

Document Title	Web Application Security Report of Directorate General of Shipping's website -Final-Ver2.0
Document ID	148/25-26/1601-Final
Document Version	2.0
Prepared by	DRCBS-23-023
Verified by	DRCBS-22-017
Approved by	DRCBS-17-001
Released by	DRCBS-17-004
Release date	05th July 2025

Document Distribution List			
Name	**Organization**	**Designation**	**Email ID**
Shri Deependra Singh Bisen	Directorate General of Shipping	Deputy Director General of Shipping	singh.deependra@gov.in

Content

Introduction

The Audit Team conducted a comprehensive web-based vulnerability assessment and penetration testing (VAPT) of **Directorate General of Shipping.**

The reference of the work order given to us is **Ref No.: ITPL/25-26/SW/PO/06 dated 05/06/2025 and link working on 05/06/2025.**

The objective of this testing was to conduct Vulnerability assessment and penetration testing as per various security standards and Guidelines, Vulnerability Notes, Advisories and White Papers issued by Computer Emergency Response Team (CERT-In).

Following are the details of the application:

S.No	Website/ Portal Name	Production URL
1.	Directorate General of Shipping	https://beta-immortal.com/
		https://beta-immortal.com/admin/login

Engagement Scope

S.No	Website/ Portal Name	Production URL	Location	Hash Value provided by auditee	Date & Time of hash value taken / Version
1.	Directorate General of Shipping	https://beta-immortal.com/ https://beta-immortal.com/admin/login	/var/www/dgs	e1c0491b49d0ffe32fc5b872a39a96d1	04th July 2025 & 05:14 PM

Details of the Auditing team

S.No.	Name/Employee Code	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.	DRCBS-22-017	Associate Cyber Security Analyst	contact@drcbscyber.com	• BCA • M.Sc. Digital Forensic & Information Security (NFSU) • Certified Lead Auditor ISMS(ISO/IEC 27001:2022) from Indian Institute of Quality Management (IIQM) • Various Cyber Security Certificates from Code Red [EC-Council]	Yes
2.	DRCBS-23-023	Asst. Cyber Security Analyst	contact@drcbscyber.com	• B.Tech (CSE) • CEH v12	Yes

Audit Activities and Timelines

Audit Activities	Time Period
Work Order Received	05th June 2025
URL Working	05th June 2025
Audit conducted (From-To)	09th June 2025 to 04th July 2025
Level 1 Report Submitted	13th June 2025
Final Report Submitted	05th July 2025

Audit Methodology and Criteria/Standard referred for audit

The audit team conducted manual as well as tool based audit to identify maximum of vulnerabilities. In tool based method, we were used industry standard tools as mentioned in the tool list supplemented by In house scripts and payloads to achieve optimum results. Sometimes, tools provide false positive results. For it, the auditor team verified the locations of the vulnerabilities through manual methods. Software arithmetic errors and validations related issues are also verified through Manual method.

A comprehensive IT security audit of the web application was performed as per legal mandate and based on web application security Standards of Open Web Application Security Project (OWASP) Comprehensive Framework, Directions by CERT-In under Section 70B, Information Technology Act 2000, Guidelines for Secure Application Design, Development, Implementation & Operations, SANS Top 25 Software Errors, Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE) Guidelines for Secure Application, Design, Development, Implementation & Operations and The Open Source Security Testing Methodology Manual (OSSTMM) etc.

Tools/ Software Used

S.No.	Name of Tool/Software used	Version of the tool /Software used	Open Source/Licensed
1	BurpSuite	2024.3.1	Licensed
2	OWASP ZAP	2.14.0	Open Source
3	Kali Linux	2024.1	Open Source
4	NMAP Scripts Engine	-	Open Source
5	Harvestor	-	Open Source
6	MetaSploit	-	Open Source
7	W3af	-	Open Source
8	Dirbuster	-	Open Source
9	Curl	-	Open Source
10	Wapiti	-	Open Source

Software Components & Dependencies

The following software components and dependencies were identified during the audit:

S.No.	Name of Software Components & Dependencies used	Version of the Software Components & Dependencies used
1	jQuery	3.7.1
2	jQueryUi	1.14.1

Limitations/Exceptions

Predefined Scope: Testing is limited to the predefined scope agreed upon, such as specific domains, subdomains, or applications. Any assets outside the scope will not be assessed.

Zero-Day Vulnerabilities: VAPT cannot identify zero-day vulnerabilities or exploits unknown to the security community at the time of testing.

Risk/Vulnerability Rating Criteria

The risk/ vulnerability of an audit finding is determined by assessing the potential negative impact and the probability that it materializes. Audit findings are classified into three risk/ vulnerability classifications. These risk/ vulnerability categories assist the Management in identification, prioritization and implementation of Audit recommendations.

The three risk/ vulnerability ratings are as under:-

High	These risks/ vulnerabilities are so significant that the Management should determine any exposure to date and effect an agreed program for their immediate and permanent resolution in order to provide assurance that they will not recur in the future. These are weaknesses that have compromised control or security, and should therefore be addressed immediately.
Medium	These risks/ vulnerabilities are important and the Management should quickly develop action plans that will ensure timely and permanent resolution of the weaknesses noted. Typically, these are weaknesses in control or security, which could develop into a potential exposure. This should be addressed at the earliest opportunity.
Low	These risks/ vulnerabilities are not material in the context of current levels of activity but the Management should be aware of them and ensure that they are resolved as soon as possible as they may become material if activities increase. These risks, even though not a direct threat to control or security, should be addressed in the interest of efficiency.

Executive Summary

The summary of Vulnerabilities/Non-conformities identified during the audit is mentioned below:

S. No	Severity of Vulnerabilities/Non-Conformities	Count
1.	High	00
2.	Medium	01
3.	Low	02
	Total	**03**

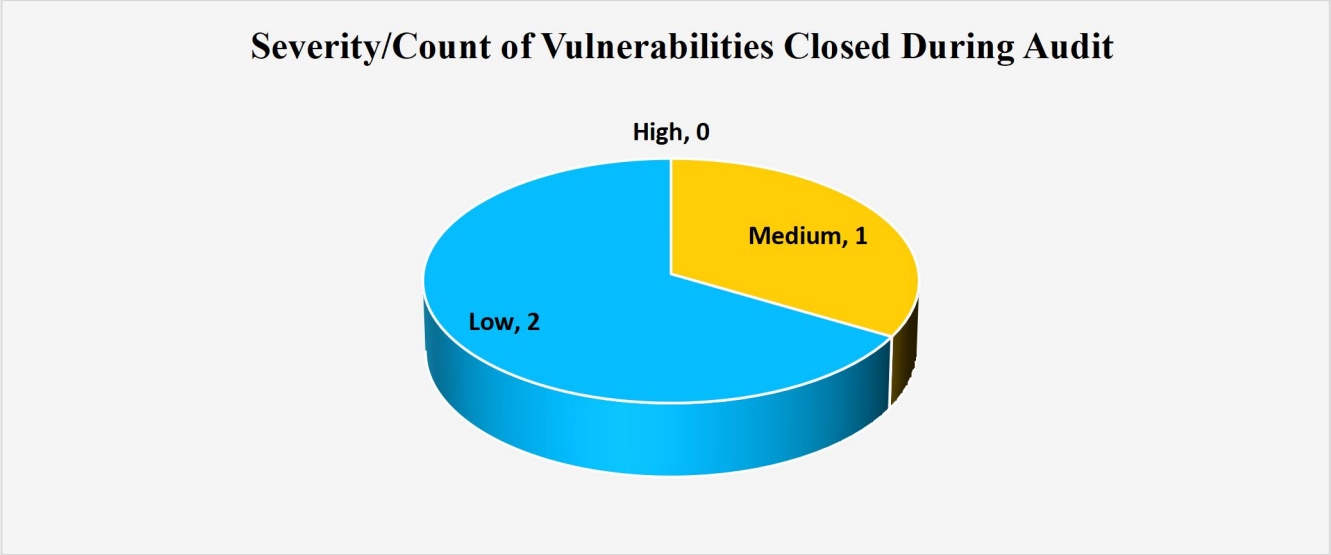
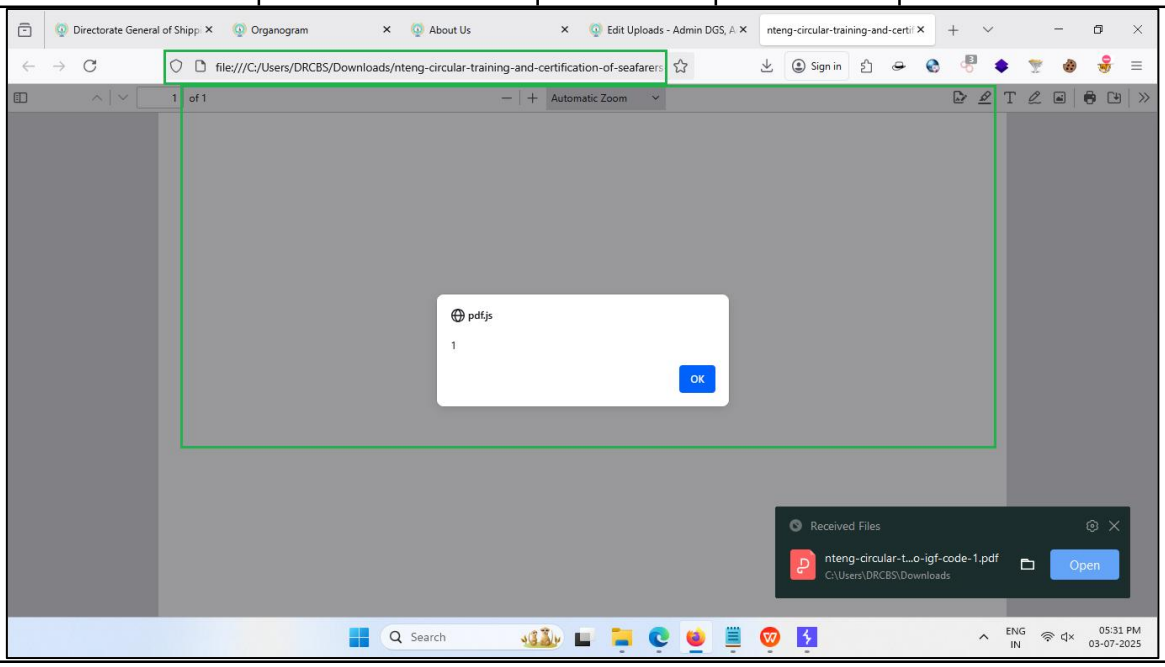


Figure 1. Vulnerabilities Chart

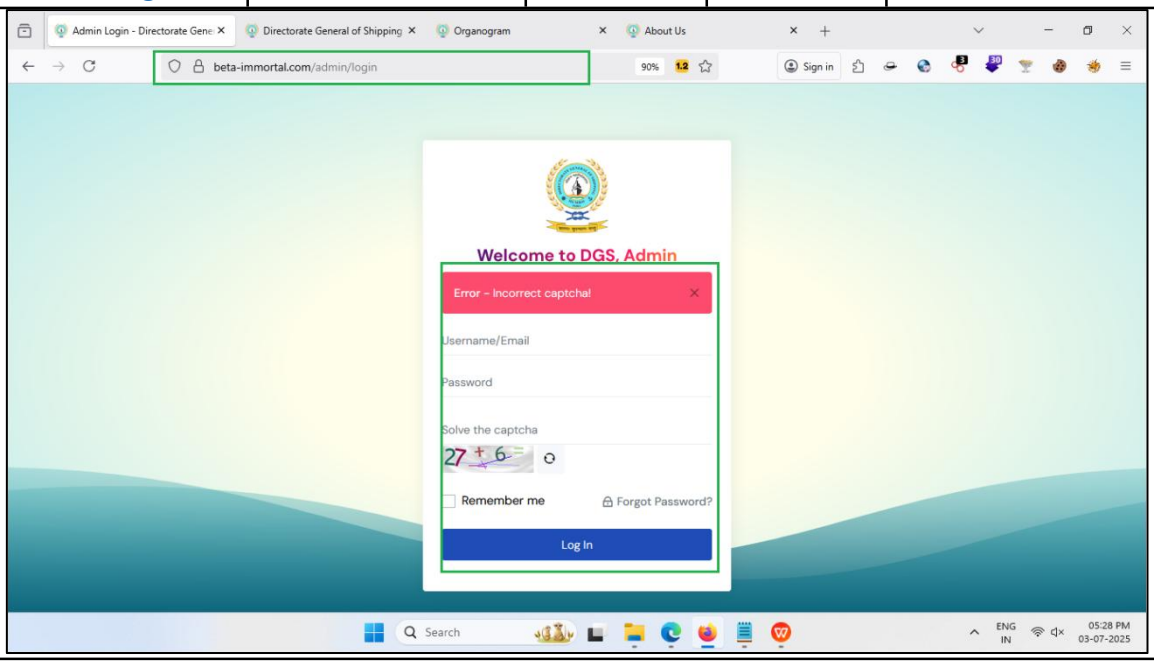
List of Vulnerable Points				
S.No	Vulnerabilities Discovered in Level-1 Report	Severity	CWE/ CVE	Final Status
1.	Reflected Cross Site Scripting	High	CWE-79	Patched & Closed
2.	Authentication Bypass	High	CWE-306	Patched & Closed
3.	Unrestricted File Upload	High	CWE-434	Patched & Closed
4.	Sensitive Information Disclosure	Medium	CWE-200	Patched & Closed
5.	Unprotected Admin Panel	Medium	CWE-285	Patched & Closed
6.	Clear Text Transmission of Sensitive Information	Medium	CWE-319	Closed
7.	Vulnerable & Outdated Components	Medium	CWE-1104	Patched & Closed
8.	Improper Input Validation	Medium	CWE-20	Patched & Closed
9.	Content Security Policy Bypass	Medium	CWE-693	Patched & Closed
10.	Missing Security Headers	Medium	CWE-693	Patched & Closed
11.	HTTP Methods Allowed	Low	CWE-650	Patched & Closed
12.	Improper Cache Control Header	Low	CWE-525	Patched & Closed
13.	Insecure Transportation Layer Security Version 1.2 Supported	Low	CWE-326	Closed
14.	Cookies without HTTPOnly Flag	Low	CWE-1004	Closed
15.	Cookies without Secure Flag	Low	CWE-614	Patched & Closed

Detailed Observations

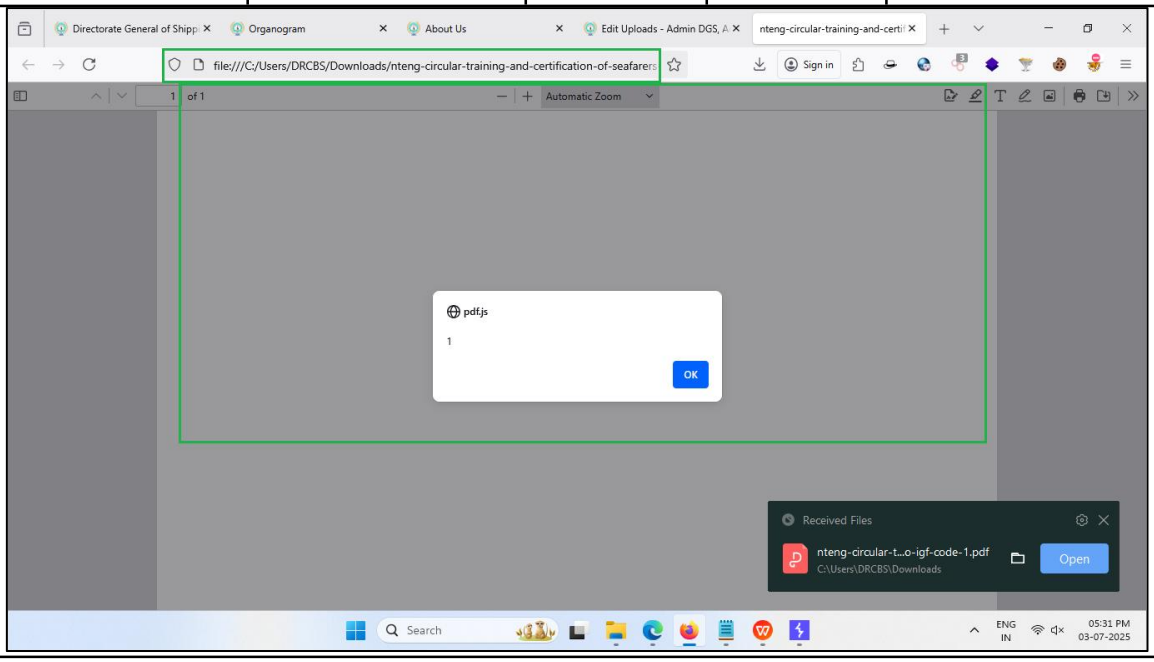
Final Report						
S No	Vulnerable Point / Location	Vulnerability	Manually/ Tool Based	Comments/ Review of flaw / Reference	Auditee Remark	Auditor Remark
1	2	3	4	5	6	7
1. Reflected Cross Site Scripting (High)						
1.1.	https://beta-immortal.com/admin/uploads	Reflected Cross Site Scripting	Manual	CWE-79	This issue is resolved.	Patched & Closed



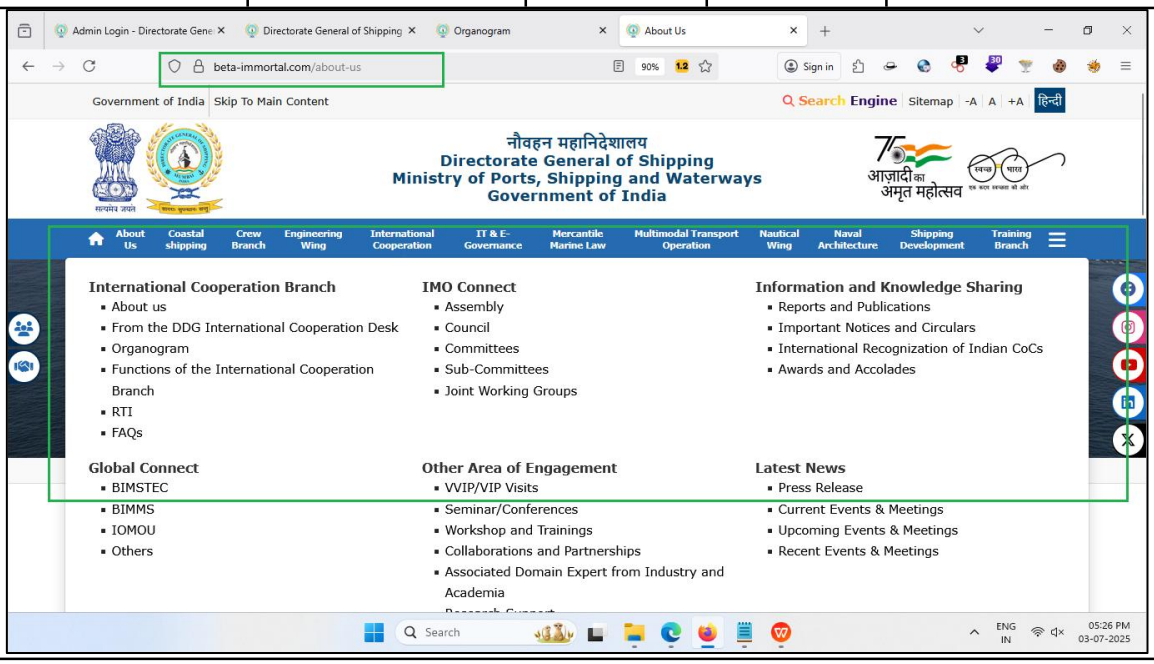
2. Authentication Bypass (High)						
2.1.	https://beta-immortal.com/admin/login	Authentication Bypass	Manual	CWE-306	This issue is resolved.	Patched & Closed



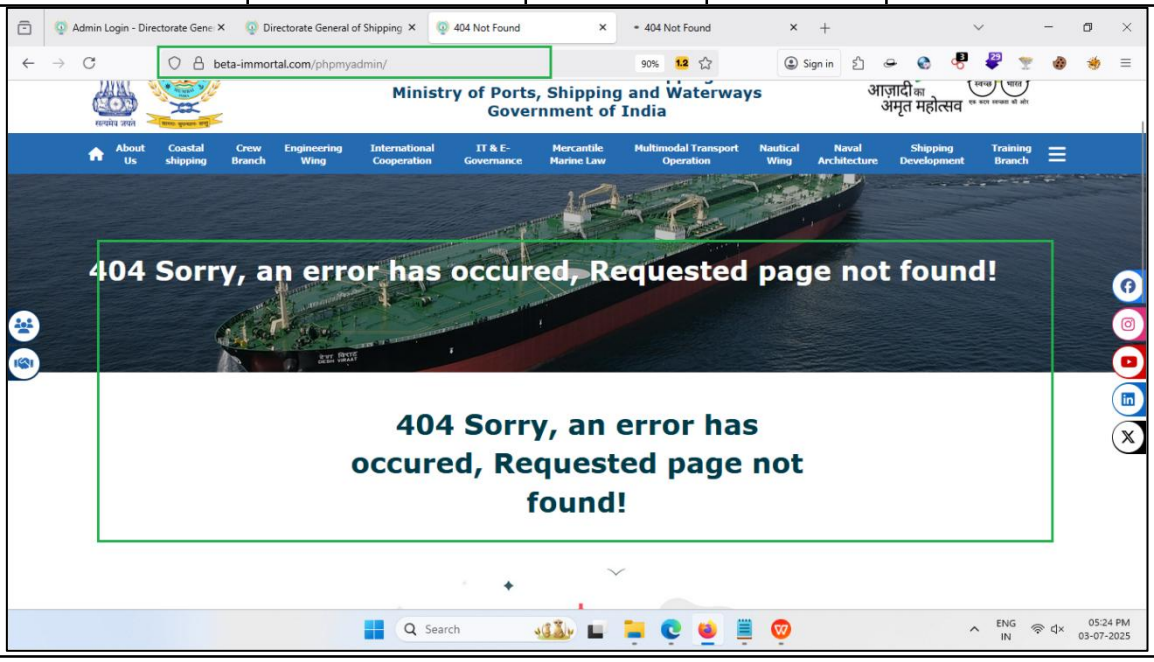
3. Unrestricted File Upload (High)						
3.1.	https://beta-immortal.com/admin/uploads	Unrestricted File Upload	Manual	CWE-434	This issue is resolved.	Patched & Closed

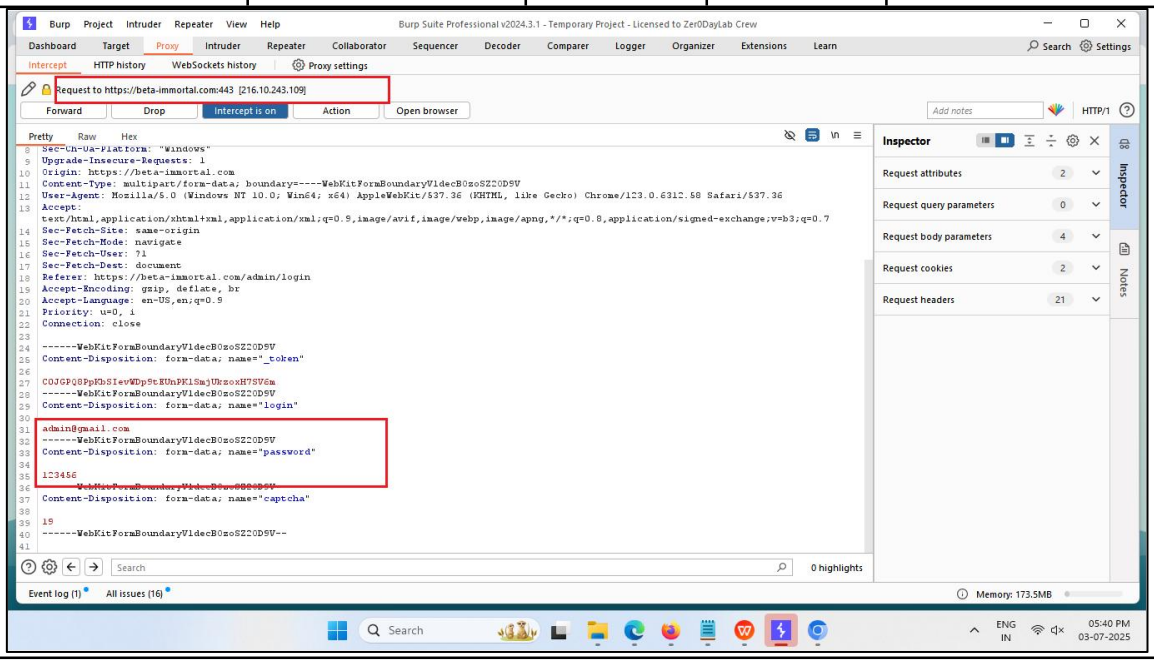


4. Sensitive Information Disclosure (Medium)						
4.1.	https://beta-immortal.com/about-us	Sensitive Information Disclosure	Manual	CWE-200	This issue is resolved.	Patched & Closed

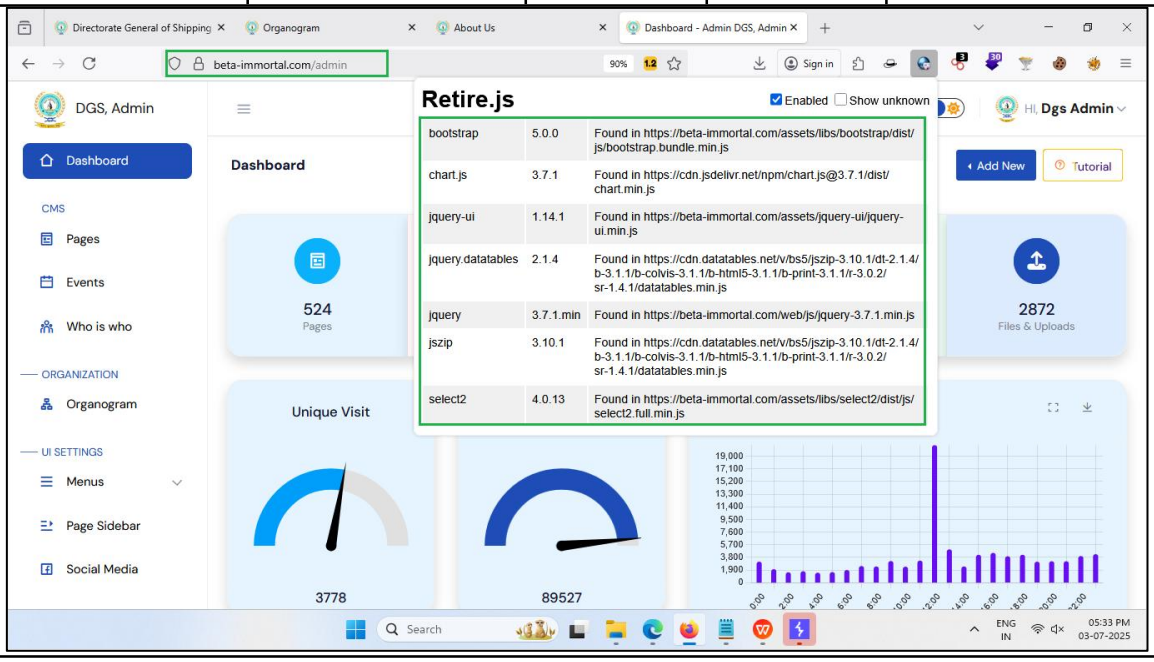


5. Unprotected Admin Panel (Medium)						
5.1.	https://beta-immortal.com/phpmyadmin/	Unprotected Admin Panel	Manual	CWE-285	This issue is resolved.	Patched & Closed

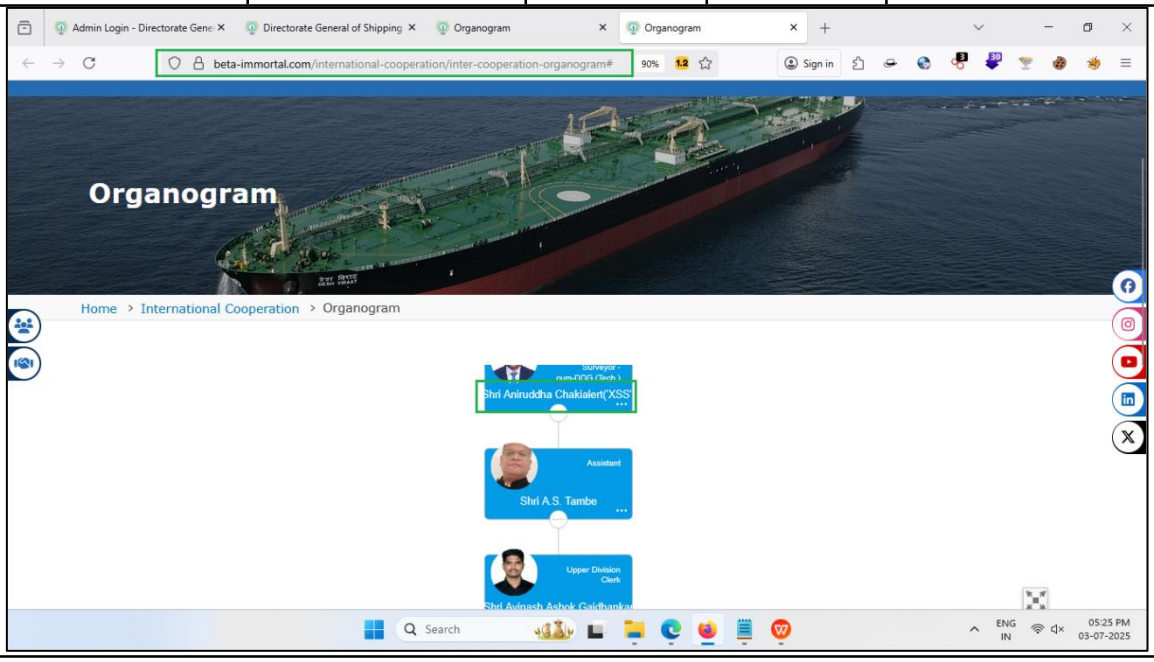


6. Clear Text Transmission of Sensitive Information (Medium)						
	https://beta-immortal.com/admin/login	Clear Text Transmission of Sensitive Information	Manual	CWE-319	This issue has been acknowledged and is considered non-risk, as the portal in question is an internal admin interface used solely for managing the website.	
6.1.						Closed

7. Vulnerable & Outdated Components (Medium)						
7.1.	https://beta-immortal.com/admin/login	Vulnerable & Outdated Components	Manual	CWE-1104	This issue is resolved.	Patched & Closed

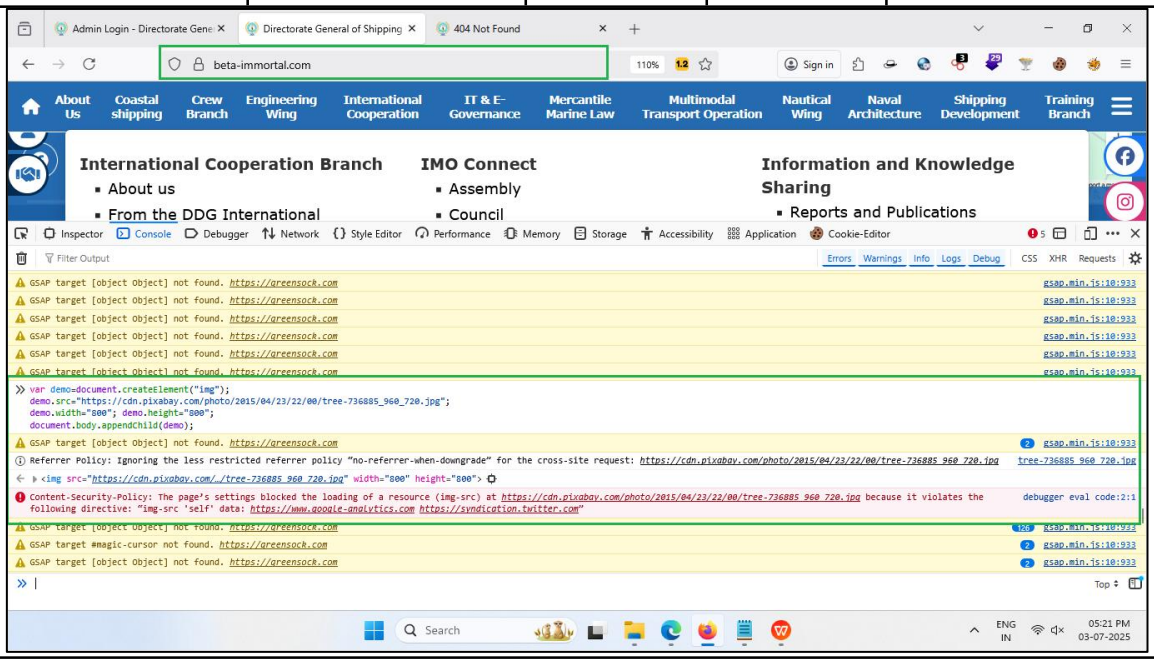


8. Improper Input Validation (Medium)						
8.1.	https://beta-immortal.com/ew-organogram	Improper Input Validation	Manual	CWE-20	This issue is resolved.	Patched & Closed



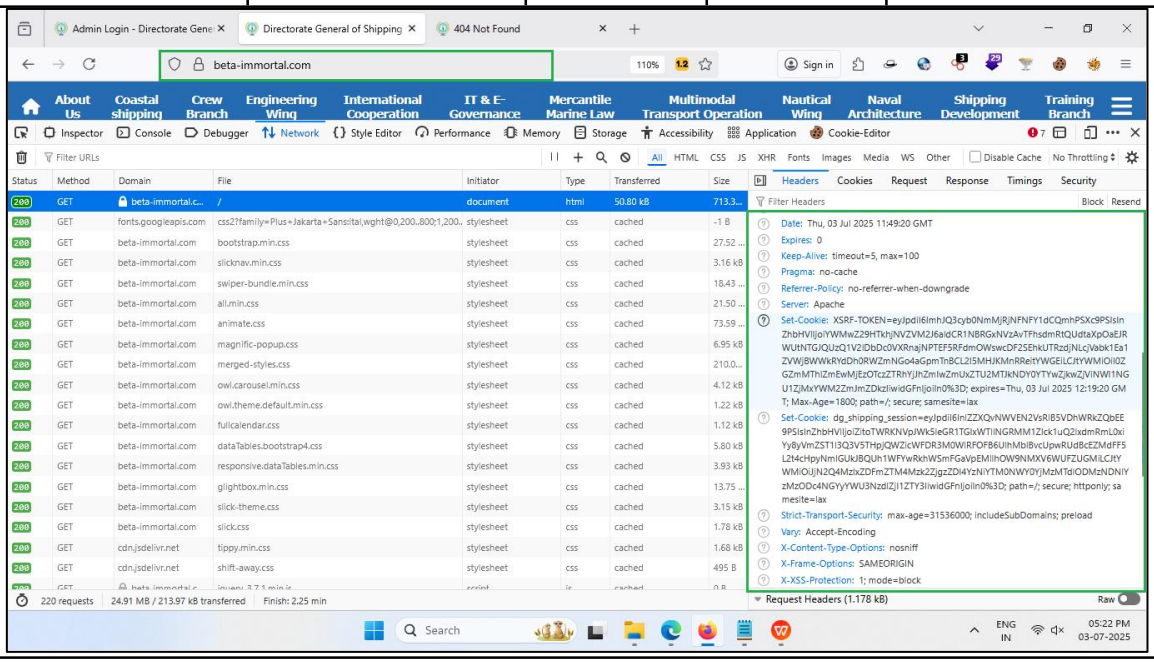
9. Content Security Policy Bypass (Medium)

9.1.	https://beta-immortal.com/	Improper Input Validation	Manual	CWE-693	This issue is resolved.	Patched & Closed



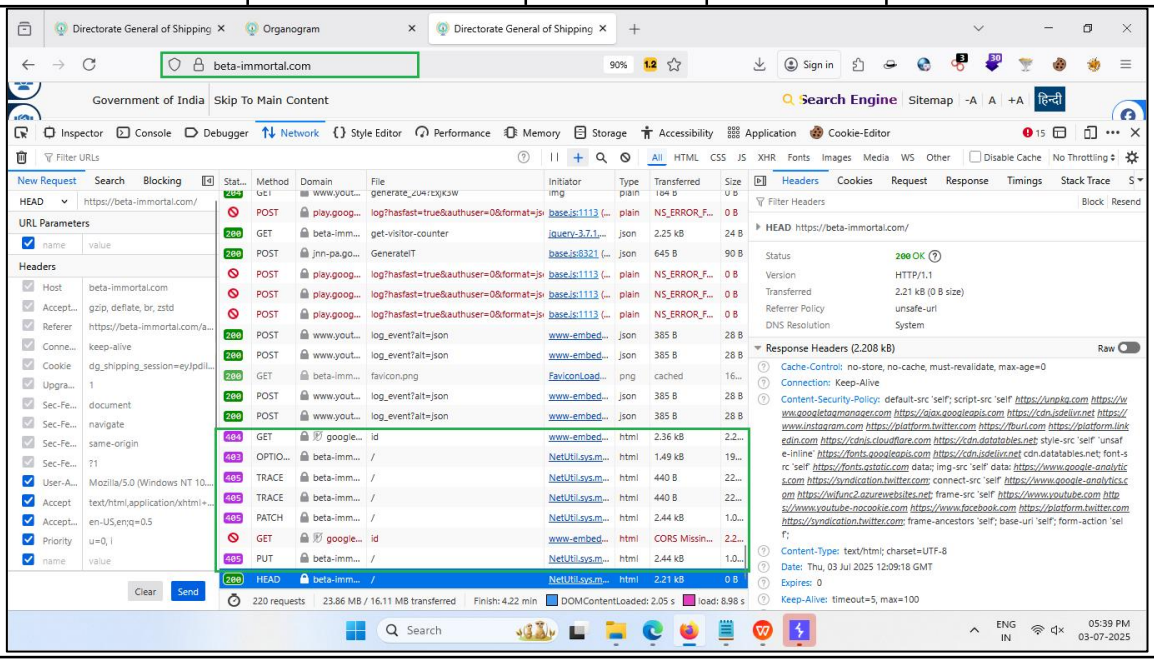
10. Missing Security Headers (Medium)

10.1.	https://beta-immortal.com/	**Missing Security Headers**	**Manual**	**CWE-693**	**This issue is resolved.**	**Patched & Closed**



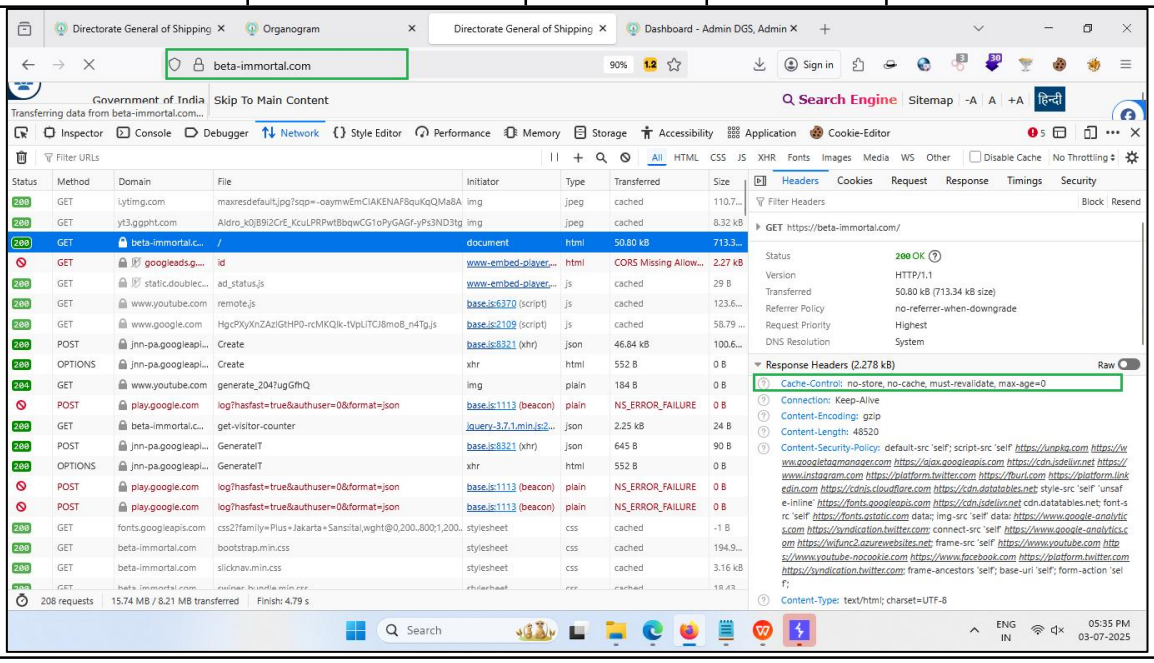
11. HTTP Methods Allowed (Low)

11.1.	https://beta-immortal.com/	HTTP Methods Allowed	Manual	CWE-650	This issue is resolved.	Patched & Closed

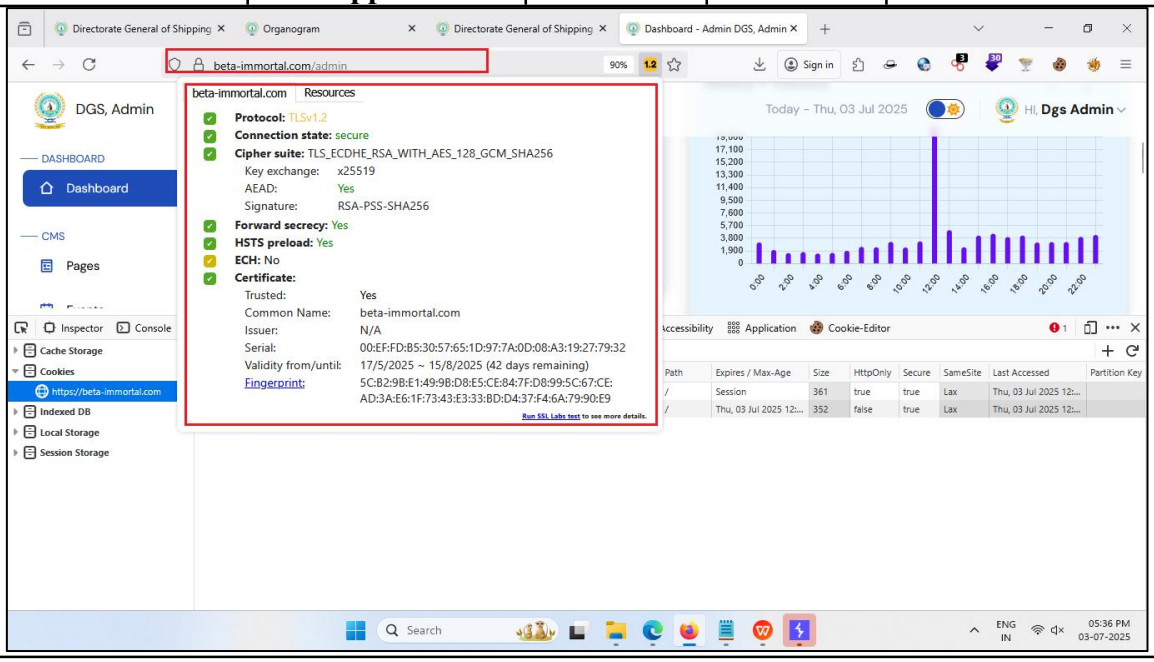


12. Improper Cache Control Header (Low)

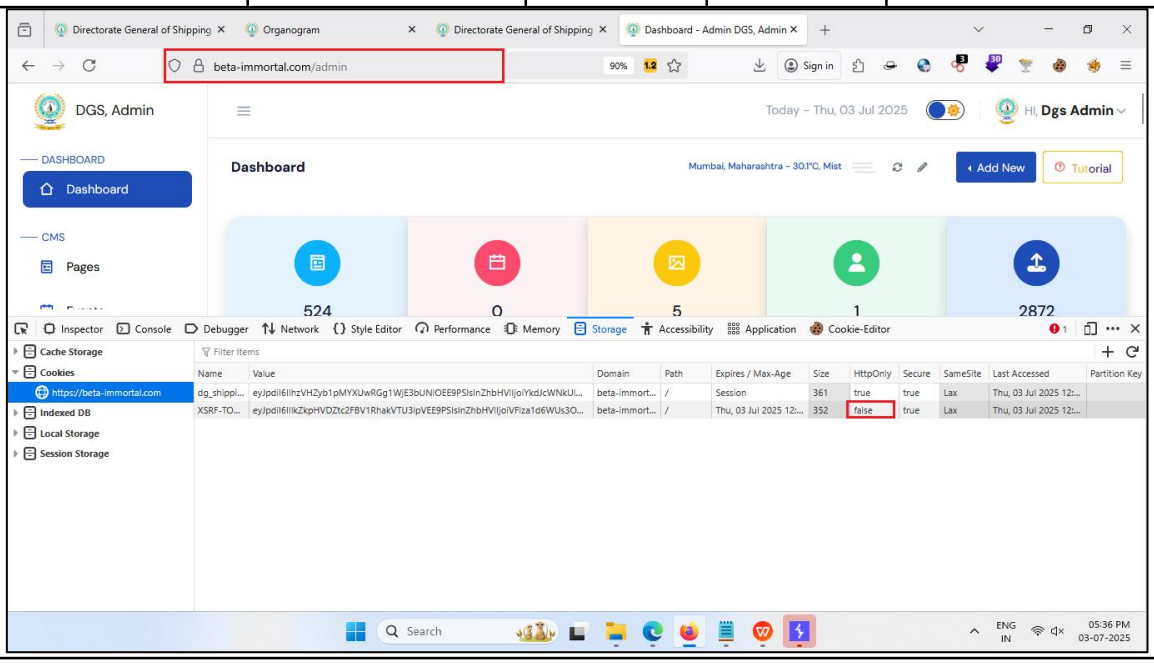
12.1.	https://beta-immortal.com/	Improper Cache Control Header	Manual	CWE-525	This issue is resolved.	Patched & Closed



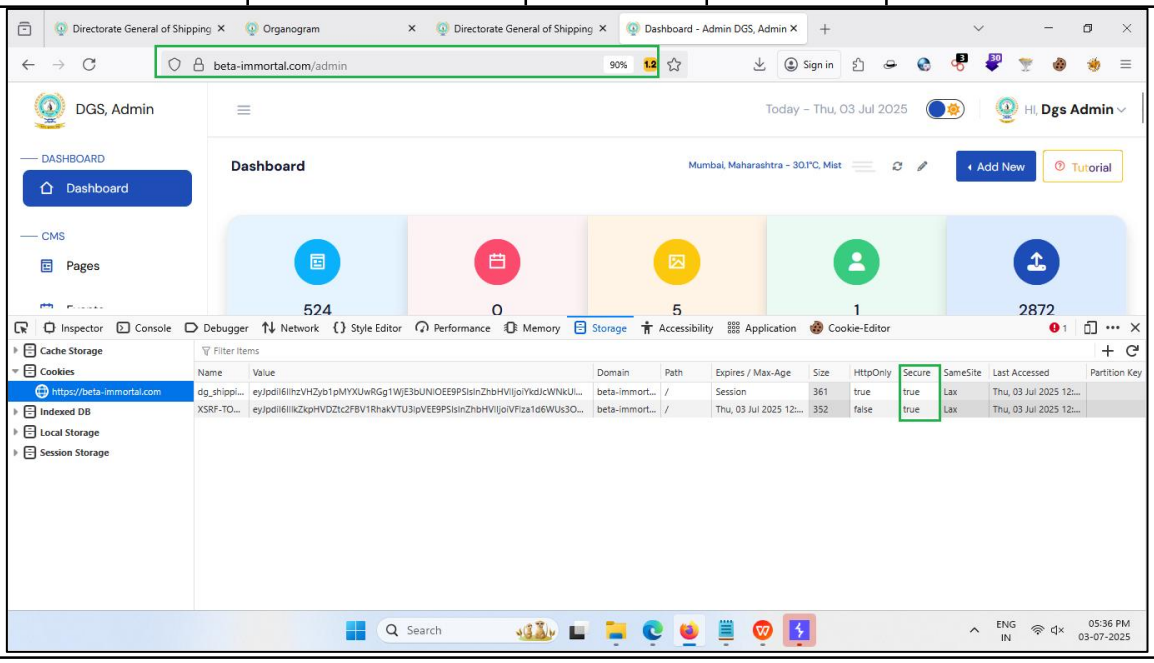
13. Insecure Transportation Layer Security Version 1.2 Supported (Low)						
13.1.	https://beta-immortal.com/	Insecure Transportation Layer Security Version 1.2 Supported	Manual	CWE-326	This issue will be resolved in Production Server.	Closed



14. Cookies without HTTPOnly Flag (Low)						
14.1.	https://beta-immortal.com/	Cookies without HTTPOnly Flag	Manual	CWE-1004	This issue will be resolved in Production Server.	Closed



15. Cookies without Secure Flag (Low)					
15.1.	https://beta-immortal.com/	Cookies without Secure Flag	Manual	CWE-614	This issue is resolved.



Patched & Closed

Conclusion

The auditee has successfully patched and addressed twelve out of the fifteen identified vulnerabilities. For the remaining three, remarks have been provided indicating that two will be resolved on the production server, while the third pertains to a non-critical dependency used solely for internal purposes and not exposed to the public domain, and therefore does not require resolution. It is now imperative to ensure ongoing compliance with the recommended security measures, incorporating them into all phases of the development process. Auditee should remain vigilant and well-versed in common web application vulnerabilities. We strongly advise adhering to the Guidelines for Secure Application Design, Development, Implementation & Operations issued by the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India. To further bolster the application's security posture, regular external and internal audits should be conducted.

Recommendations

Following are the other recommendations to improve the cyber security posture of the application and associated IT Infrastructure of the auditee organization.

1. Web Server Security and the OS hardening need to be in place for the production Server.

2. It is recommended that deploy and proper configure the SSL.

3. Web Application should comply with Guidelines for Indian Government Websites (GIGW).

4. Employ the latest stable version of the Transport Layer Security (TLS) protocol to ensure secure communication between the application and its users. Additionally, disable outdated and weak SSL cipher suites to enhance security and prevent potential exploits.

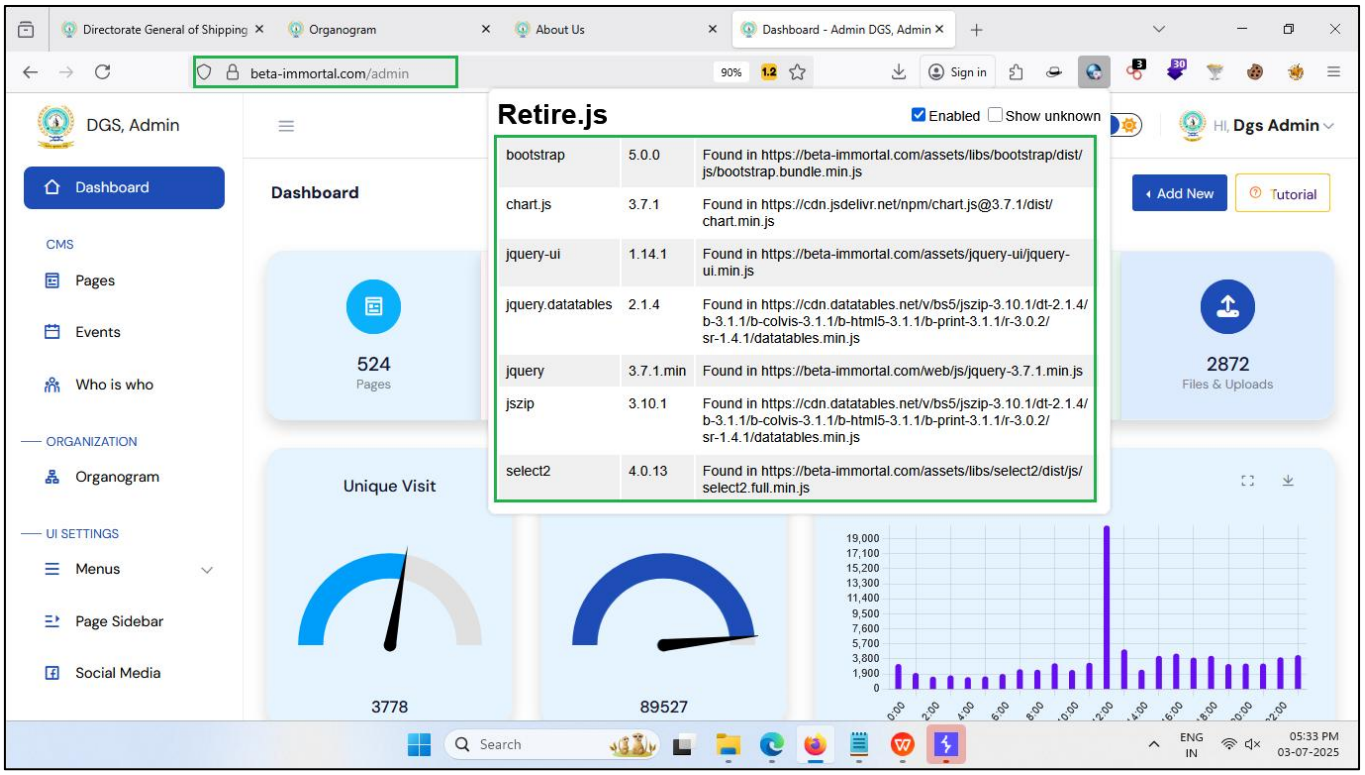
5. The developer team should follow the Guidelines for Secure Application Design, Development, Implementation & Operations issued by Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology Government of India. Conduct the regular external and internal audit to enhance the security posture of the application.

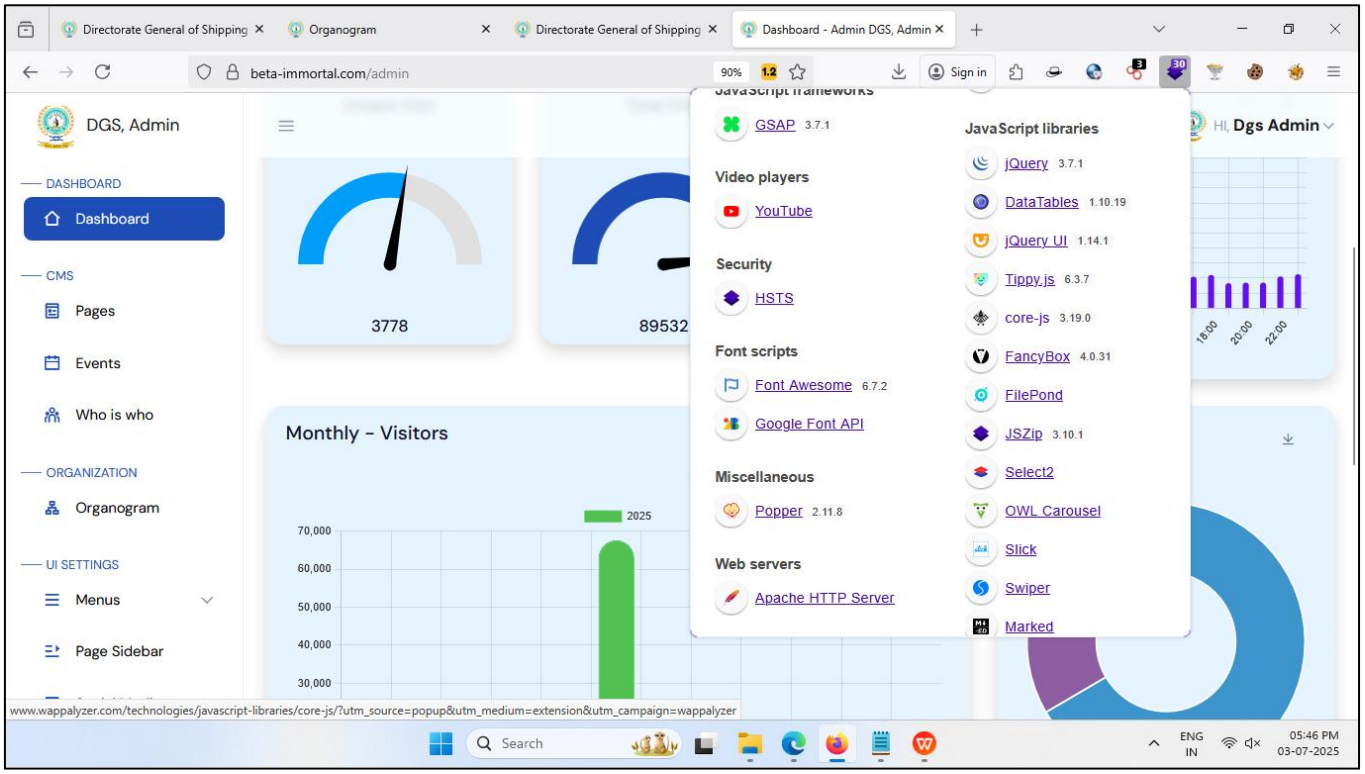
6. The Auditee organization must comply with the Directions issued by CERT-In (Notification No. 20(3)/2022-CERT-In) dated 28 April 2022 under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

7. The Developer Team of auditee must also follow the Technical Guidelines on Software Bill Of Materials (SBOM) version 1.0 issued by CERT-In dated 03.10.2024.

Appendix 1: Proof of Concept of the Software Components & Dependencies

1. Components used:





Compliance to Directions issued by CERT-In under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet dated 28 April 2022

The Government of India appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette in terms of the provisions of sub-section (1) of section 70B of the Information Technology Act, 2000 (IT Act, 2000). As per provisions of sub-section (4) of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents
d) coordination of cyber incident response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

.

As per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under sub- section (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

All Service providers, intermediaries, data centres, body corporate, Virtual Private Server (VPS) providers, Cloud service providers , VPN Service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and Government organisations shall follow these Cyber Security Directions issued by CERT-In dated 28.4.2022.

Glossary

1. **CERT-In:** The Government of India appointed "**Indian Computer Emergency Response Team (CERT-In)**" vide notification dated 27th October 2009 published in the official Gazette In terms of the provisions of sub-section (1) of section 70B of the Information Technology Act, 2000 (IT Act, 2000). As per provisions of sub-section (4) of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber security:-

    a) collection, analysis and dissemination of information on Cyber incidents;
    b) forecast and alerts of Cyber security incidents;
    c) emergency measures for handling Cyber security incidents
    d) coordination of Cyber incident response activities;
    e) issue guidelines, advisories, vulnerability notes and white-papers relating to information security practices, procedures, prevention, response and reporting of Cyber incidents;
    f) such other functions relating to Cyber security as may be prescribed.

2. **Directions issued by CERT-In dated 28 April 2022 :** As per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centers, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under sub- section (7) of the section 70B of the IT Act, 2000 and other laws as applicable. All Service providers, intermediaries, data centers, body corporate, Virtual Private Server (VPS) providers, Cloud service providers , VPN Service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and Government organizations shall follow these Cyber Security Directions issued by CERT-In dated 28.4.2022.

    https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

3. **Common Vulnerability and Exposure(CVE):** The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures.

4. **Common Weakness Enumeration (CWE)**: Common Weakness Enumeration (CWE) is a list of common software and hardware weakness types that have security ramifications. A "weakness" is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.

[END OF REPORT]

भारतसरकार/ GOVERNMENT OF INDIA
पत्तन, पोतपरिवहनऔर जलमार्गमंत्रालय /
MINISTRY OF PORTS, SHIPPING AND WATERWAYS
नौवहनमहानिदेशालय, मुंबई
DIRECTORATE GENERAL OF SHIPPING, MUMBAI

DGS Circular 12 of 2024

File No 11-33/7/2024-COMP - DGS **Date: 09.05.2024**

Subject: Social Media Policy for the Directorate General of Shipping, Mumbai-reg.

1. Whereas, the Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, has formulated Framework and Guidelines for Government Organisations for use of Social Media for enabling government agencies to make use of Social Media as dynamic medium of interaction. These guidelines have enabled the various Government agencies to create and implement its own social media strategy.

2. Whereas, the Directorate on similar lines has formulated its own Social Media policy for its new website. The Social Media Policy of the Directorate General of Shipping is attached as **Annexure.**

3. This issues with the approval of the Director General of Shipping, Mumbai.

09/05/2024

(Ravi Kumar Moka)
Deputy Director General of Shipping (IT & E-gov)

Encl: Annexure

To,
1. All Wing Heads of the Directorate
2. All allied offices and field offices
3. All the stakeholders of the Directorate

Annexure

SOCIAL MEDIA POLICY
Directorate General of Shipping, Mumbai
Government of India

1: Introduction:

Social media has transformed the society like never before. It helps in connecting people easily and also emerged as one of the most convenient mode of sharing of information. It is different from traditional media tools like newspaper, magazine, radio and television, with more depth, vibrancy and immediate effect. With social media, common citizens are not only a consumer of information, but also the generator of content.

Highlighting the importance of social media and in a bid to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media for Government Organisations has been formulated by the Department of Electronics and Information Technology Ministry of Communications & Information Technology, Government of India. These guidelines have enabled the various Government agencies to create and implement its own social media strategy.

1.2: Need for Social Media policy:

Social media gives voice to the unheard, with immediate and non-stop reach. It offers the governments and its initiatives a platform to engage with their stakeholders — especially citizens in real time and get a pulse of the mood among the public without any bureaucratic or political filter, which later can be used to make policies citizen oriented. Many government agencies across India use various social media platforms to reach out to citizens, businesses and experts to seek inputs into policy making, get feedback on service delivery, create community based programmes etc. However, many apprehensions remain including, but not limited to issues related to authorisation to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement, creating synergies between different channels of communication, compliance with existing legislations etc. It was therefore felt that Guidelines for use of Social Media were required which would enable project owners/implementers to effectively use these platforms.

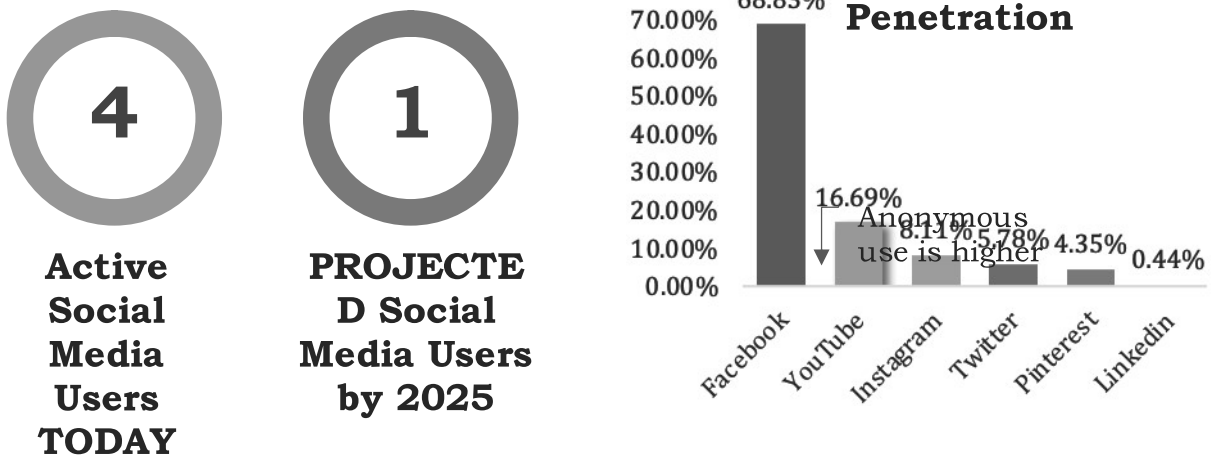
1.3: Defining Social Media:

Kaplan and Haenlein in 2010 classified social media into six different types: collaborative projects, blogs and microblogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. A brief description of some of the most common types of social media is given below:

Platform Type	Description
Social Networking	Social Networking is an online service that enables its users to create virtual networks with likeminded people akin to social networks in real life. It often offers the facilities such as chat, instant messaging, photo sharing, updates, etc. Currently, social networking sites are the most prominent version of social media. Facebook with 800 million users is oneof the most well known social networking sites.

Blogs	Blogs are descriptive content pages created and maintained by individual users and may contain text, photos and links to other web sites. The main interactive feature of Blogs is the ability of readers to leave comments and the comment trail can be followed.
Micro Blogs	Micro Blogs are similar to Blogs with a typical restriction of 140 characters or less, which allows users to write and share content. Twitter is the most well known micro blogging site.
Vlogs and Video Sharing sites	Video Blogs or Vlogs are blogging sites that mainly use video as the main form of content supported by text. YouTube is the largest video sharing site.
Wikis	A Wiki is a collaborative website that allows multiple users to create andupdate pages on particular or interlinked subjects. While single page is referred to as "wiki page" the entire related content on that topic is calleda "Wiki". Wikipedia is the pioneering site of this type of platform.

1.4: Social Media Usage Trends in India:



***Around 3 out of 4 social media users are Facebook users. The penetrations of the other platforms are much lower – with users mostly in the urban areas. YouTube is predominantly used for consumption, and not engagement / discussion.

2: Principles for Government Officials Using Social Media (In Official Capacity):

The interactive nature of social media ensures multi-dimensional communication and response time is often immediate. With the speed of communication not offering the luxury of differentiating between official and personal content, using social media for official purposes should be follow some guiding principles to keep conversation and interaction smooth:

- ***Identity of the User:*** Always identify clearly who you are, what is your role in the department and publish in the first person. Disclaimer may be used when appropriate
- ***No Unauthorised Comment:*** Do not initiate a conversation, comment or respond to a reaction unless authorised. This must be the firmly adhered to especially in the matters that are sub-judice, draft legislations or relating to other individuals
- ***Maintain Relevance:*** Comment only on issues relevant to your area and make pertinent comments.
- ***Professional Approach:*** Be polite and respectful during all discussions. Never make personal comments for or against any individuals or agencies. Stay away from political discussions.
- ***Be Open to Criticism:*** Always react to comments (positive or negative) with grace. It is NOT necessary to respond to each and every comment.
- ***Follow the Rule:*** Always keep relevant rules and regulations first. Never infringe upon Intellectual Property Rights or Copyright of others.
- ***Respect Privacy:*** Never reveal personal information about other individuals or your own private and personal details.
- ***Law of the Land:*** Information Technology Act, 2000 and its amendments thereafter and all other applicable laws governing the territory of India.

3: Guidelines for Using Social Media by Government Organizations

The Framework and Guidelines for Use of Social Media for Government Organisations by the Ministry of Electronics and Information Technology Ministry of Communications & Information Technology, Government of India (MeitY) highlights a set of guiding principles that may be used while making use of Social Media.

DGS will be adopting the same Framework and Guidelines drafted by MeitY with minor modifications for the following reasons:

- It is a comprehensive document taking care of the sensitive nature of the presence and interaction of government agencies in social media;
- The concerns, structure and requirements of the State Government and its agencies are taken care of by the Framework and Guidelines;
- MeitY is a full-fledged ministry under the Union Government. It has the expertise in issuing guidelines and make amendments.

Objectives: The objective for the use of social media is not just to disseminate information but also to undertake public engagement for a meaningful public participation for formulation of public policy. Government organisations are exploring the use of social media for public engagements for disseminating information, policy making, recruitment, generating awareness, education etc. about public services. Therefore, Social Media may be used for:

- Seeking feedback from citizens
- Re-pronouncement of Public Policy
- Issue based as well as Generic interaction
- Brand Building or Public Relations
- Generating Awareness and education on National Action Plans and implementation strategies

3.1. DGS can engage social media in any of the following manner:

- By making use of any of the existing external platforms, or
- By creating their own communication platforms. It will not only be cost effective, but also effective in penetrating messages across the target audience.
- The choice of the platform – whether owned or externally leveraged should be made based on the following factors:
    - Duration of engagement - whether the engagement sought is to be an ongoing activity or created for a specific time-bound purpose
    - Type of Consultation – whether the consultation is open to public or confined to a particular group of stakeholders e.g. experts
    - Scope of Engagement – whether the consultation requires daily, weekly, bi-weekly or even hourly interaction
    - Existing Laws – whether existing laws permit use of such platforms and the requirement under such laws regarding data protection, security, privacy, archiving etc.

3.2. Social Media Governance Structure:

Since use of social media is a round-the-clock engagement, traditional media rules and regulations do not apply in totality.

Two most important aspects of social media are its:

- Viral characteristic – news spreads exponentially; and
- Demand for instant gratification – queries, responses and counter-responses are posted instantaneously.

However, since the official pages of departments must reflect the official position, some measure of control must be included in the flexible design of communication.

Just as rules and regulations exist for interaction with traditional media, similar rules must be created for engaging with social media.

Some of the key aspects of such a governance structure include:

3.2.1: Account Governance:

Account Creation: A social media account establishes an organisation's online identity. Wherever possible, the same name for the different social networking accounts may be adopted to ensure ease of search on the internet. Another important facet of online identity is the need for it to be rendered effectively in either long form e.g. website address or in 15 characters or less (this is the Twitter maximum).

Account Administration: One or two officials handling the accounts (the social media expert handling the account in case the work is outsourced) will be responsible for the dafty and sanctity of the accounts and handles.

Login and passwords: Each new account requires a user name and/or email address and a password. A proper record of login ids and password must be maintained. This is critical as multiple people may be authorised to post on behalf of the department.

Account Status:It is important to define whether the engagement may be undertaken through official accounts only or the officials may be permitted to use personal accounts also for posting official responses. It determines who says what on behalf of

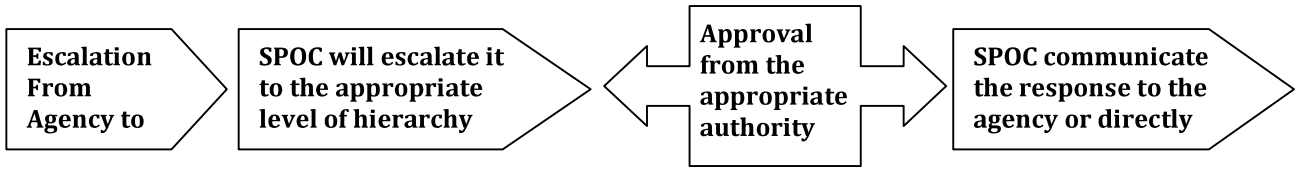
your organisation and in what form it is published. It also outlines how each piece of published information is presented where it is published. The most important aspect is whether the responses are in Official or Personal Capacity.

3.2.2: Response and Responsiveness:

Responsiveness: This indicates the how often would the pages/information be updated, in what manner would the responses be posted, what would be the turnaround time of responses etc. The major attraction of social media is the spontaneity and immediacy of response and feedback and those visiting the site would expect the some kind of response within a pre-defined time limit.

Response:While creating a policy for responses, it may be noted that -

- Not all posts/comments need to be responded to immediately and individually. Also, wherever a response is required all posts should be kept short and to the point.
- While employees are free to post response in their personal capacity, it is mandatory that while they are doing so, they must clearly identify themselves, confidential information must not be divulged and should not be seen to represent "official view" unless authorised to do so.
- Another important aspect that needs to be addressed is the Escalation Mechanism. There has to be a defined hierarchy not only of responses but also of queries. An official from the department (not below the rank of Dy. DGS) be made the Single Point of Contact (SPOC) for any issues related escalation of any content/response related mechanism. The official will be solely responsible for escalation/resolution within the Department and co-ordination with the agency.
- Since Social Media needs quick reaction and traditional file based escalations can't work, any escalation via email should be considered valid and official form of document.



3.2.3: Resource Governance:

Allocation of Resources: Since using social media is a resource intensive exercise, it is important to ensure that resources and their responsibilities are clearly marked out very early. Many organisations have a dedicated team including outsourced resources to manage their engagement while others primarily use internal resources. More often than not, it is advisable to create a dedicated team. One of the key issues that impacts the resource requirement is whether the conversation is moderated or un-moderated. In case of moderated conversation, dedicated resource/s is critical. One of the key resources is an internal champion within the system who can lead the strategy within the department. It is important to note that since the engagement in social media requires different skill sets, the champion and other resources identified would require orientation & training specifically for the tasks assigned to them and keep abreast of the fast paced developments in this media.

Roles & Responsibilities: The roles and responsibilities of the team responsible for creating, managing and responding on social media platforms must be clearly defined.

- In Indian context, they may also need to be aligned to roles and responsibilities defined for responding to RTIs.
- For most interactions, flexibility may be given to the staff to respond to regular queries or comments.
- Escalation mechanism defined in the DGS structure must clearly define accountability at all levels.
- The role definition must not be limited just to responses, but also include responsibility for matters related maintenance of login ids and passwords, issues related to data security, archives, privacy, etc. For example, while the existing web content team may be assigned the responsibility for responding to usual queries; special technical expertise may be required to ensure appropriate levels of security.
- The Corporate Communication department will be responsible for administering this policy.
- The Social Media Teamwhether in-house employees or outsourced will manage the day-to-day application process and update the DGS website web page.
- All social media accounts officially recognized by DGS must have at least two DGS employees as administrators at all times to ensure adherence to this policy.
- Should a DGS employee administrator of an account leave the organization for any reason or no longer wishes to be an account administrator, it is the DDGS or DGS's to designate another employee to be an account administrator and remove the former employee's administrative permissions to the site.
- If two employees are not available to serve as account administrators, a member of the Social Media Staff may serve in that capacity.
- Employees identified as administrators of accounts are responsible for managing and monitoring content of their social media accounts. Administrators are responsible to remove content that may violate the organizations IT Policies or the Terms and Conditions of use.
- Guidelines for Content:
    - Users are expected to adhere to same standards of conduct online as they would in the workplace. Laws and policies respecting contracting and conflict of interest, as well as applicable policies and guidelines for interacting with stakeholders and in the social media context just as they do in personal interactions. Users are fully responsible forwhat they post to social media sites and tag official social media handles of DGS.
    - Use good judgment about content and respect privacy laws. Do not include confidential information about DGS, its staff, or its stakeholders. Post only content that is not threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal.
    - Representation of your personal opinions as being endorsed by the DGS or any of its constituent entities is strictly prohibited. DGS's name or logos may not be used to endorse any opinion, product, private business, cause, or political candidate.

- By posting content to social media sites, the poster represents that the poster owns or otherwise has all of the rights necessary to lawfully use that content or that the use of the content is permitted by fair use. Posters also agree that they will not knowingly provide misleading or false information, and those they will indemnify and hold DGS harmless for any claims resulting from the content.
- While DGS shall have the right to remove or cause the removal of any content for any lawful reason, including but not limited to, content that it deems threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal.
- When using or posting online material that includes direct or paraphrased quotes, thoughts, ideas, photos, or videos, always include citations. Provide a link to the original material if applicable.
- Refrain from using information and conducting activities that may violate DGS or Government rules and regulations.
- If employees or stakeholders also maintaintheir own personal social media accounts, you should avoid creating confusion over whether or not the account is associated with DGS. If you identify yourself as an employee or stakeholder online, it should be clear that the views expressed on your site are not those of the DGSand you are not acting in your capacity as an authorized person of DGS.

Accountability: Clearance systems that distinguish between situations when an official position is required, and when open conversation is appropriate. This has to have at its heart a redefinition of accountability. The officials designated for engagement with citizen using the social media should be covered under a well defined immunity provision in consonance with the RTI Act and the IT Act and the IT Amendment Act 2008.

3.2.4: Content Governance:

Content Creation & Social media profiles overlap, therefore sharing consistent content on all social media platforms should form the bedrock of content policy. While the social media tools allow everyone to become a creator, for the official account, content will have to be specified and tailored to the site on which it is being published.

Accessibility:In order to enable wider participation, content creation and availability should be in English and Hindi and must not be limited to text alone. The content should adequately address challenges related to accessibility in other State Languages as well as accessibility of content for differently-abled.

Moderation: A moderation policy should also be published if the platform permits others to add their own content; this informs people what they can post whilst protecting others who may visit your platform. The moderation policy should include matter related to copyright, rights to addition and deletion etc.

Records Management: When any information is shared or guidance given online, it is necessary to ensure that all relevant records are captured, trail is generated and records are managed appropriately. It is important that the rules regarding record keeping are DGS upfront so that those seeking historical data are aware of statutes and limitations. Some of the important aspects that may be kept in mind while defining record management guidelines are as under:

- The requirements for existing legislations e.g. RTI etc. need to be kept in mind and are paramount in influencing decisions regarding record keeping
- Ordinarily, if online consultations do not impact decision making, lead to or influence policy making (e.g. seeking information about nodal officers, or any other public document, or responding to generic comments such as governance should be improved etc.) the agencies may decide that no record of such interactions will be maintained.
- However, if consultations are necessarily being undertaken on specific policy or governance issues or that may influence decision making (e.g. inputs into Plan Document, consultation on policy frameworks etc.) then all necessary records need to be maintained. If the agency is using a social media site that does not facilitate record keeping, then there are various other options that may be explored. Some of the options are given below and may be exercised based on need and resources available:
    - Records may be created agency's internal platform and records be maintained with appropriate tags e.g. creator/sender, dates, posting site etc.
    - Screenshots may be captured and stored in soft or hard (copy) format and filed at appropriate place.
    - A summary may be created of the information/consultation and filed.

Since most of the social media platforms are based outside India and are not governed by Indian Laws, or managed and controlled by Indian regulations, specific policies may be drafted related to information security and archiving. If required the agencies may engage with the Social Media Service Providers to work out Service Level Agreements for

- Complaint and response mechanism between the agency and the Service Provider
- Content Storage
- Shared access of the content
- Archival mechanisms

Legal Provisions: In India, the legal implications must be viewed in accordance with the law of land e.g. RTI Act, Information Technology Act, 2000 and its amendments thereafter and all other applicable laws governing the territory of India. These policies must be circulated internally to ensure uniformity of response.

5.3: Communication Strategy:

- Some of key aspects of communication strategy include – Integration of Social Media into the day to day activity of the Department, connection with existing networks/users/followers, sharing content across sites and publicising use of social networking through traditional media.

- While the social media tools allow everyone to become a creator, for the official account, content will have to be specified and tailored to the site on which it is being published.
- Adequate care must be taken to avoid propagation of unverified facts and frivolous misleading rumours which tend to circulate often through miscreants on social media platforms.
- It must be reiterated here that social media should only be one of the components of the overall citizen engagement strategy and government departments must desist from using social media as the only medium to communicate with their stakeholders.
- Initially, DGSmay just aim to post information regularly.

5.4: Engagement Analysis:

Social media monitoring must be an integral part of any social media strategy. Social media data is different from other data or information because organizations have no control over its creation or dissemination on the Web and in order to understand and analyze the data a structure has to be imposed externally on it. Today a multitude of tools offer solutions for measuring conversation, sentiment, influences and other social media attributes. They helpin discovering conversations about project and organizations and can be used to proactively engage with stakeholders. The Social Network Analysis (SNA) Software facilitates both quantitative as well as qualitative analysis by mining the raw data and combining it with individual and socio matrix. While some SNA software also have the features that enable them to import and/or store databases from social network, others perform preferential analysis to predict individual level or network outcome. Many social media monitoring platforms offer demographic information such as age and location. This information can be used to expand the reach of your platform by creating a geo-targeted campaign focused on areas that generate the most traffic to your social media site.

Some considerations for Data Analysis include:

- Data Definition: Selection of platforms, pages and/or organizations
- Depth and detail of analysis on each page: Areas or sections of the page to analyze (Wall, Discussion board, Pictures, etc.)
- Time-frame: Last one month etc.
- Criteria for determining the importance of the pages: notability, popularity, intentions/goals of pages, etc.

Some of challenges encountered in analysis may be related to

- Overlapping functions of posts: many comments and responses serve multiple purposes
- Difficulties in disentangling "push" messages from "pull" messages
- Inexhaustible range of topics that extend beyond your area of interest
- Unpredictable patterns of conversation and user exchange

These challenges may be mitigated by taking the following steps:

- **Limit Scope of Analysis**: Making a small start and defining Top 5 or 10 metrics may help organize the Data e.g. No. of mentions, No. of comments on specific posts, No. of retweets, No. of likes or shares etc.
- **Creation of Dashboard**: There are many free tools available that can help create a dashboard view of the data which can be pulled in through RSS feeds. This will help keep tab on latest happenings

- **Connect with responders**: It is a good idea to collate information/link to profiles about people who respond to queries or topics of your organizations interest, also observe their preference of response – individual mail, wall posting etc. Over a period of time this will help generate a broad profile of people who respond to your efforts
- **Follow the followers/Leaders**: Follow your followers and leaders on other networks/platforms to hear what is being talked about. This would help in spotting the trends in discussion.