

## Website Quality Manual for HUDCO

Document number: HUDCO/ITW/WQM/2025-26/01			
Issue number:	01	Revision number:	01
Issue date:	17-04-2025	Revision date:	

# Website Quality Manual

for

[www.hudco.org.in](http://www.hudco.org.in)



**HOUSING AND URBAN DEVELOPMENT CORPORATION LIMITED (HUDCO)**  
**Core-7-A, HUDCO Bhawan, India Habitat Centre, Lodhi Road, New Delhi - 110 003**  
**Website: [www.hudco.org.in](http://www.hudco.org.in)**

---

This Web Information Policy Document is intended for the information of HUDCO website viewers / stakeholders/ employees of HUDCO, and is not intended to be and should not be used by any other person or entity.

**Website Quality Manual for HUDCO**

**Revision History**

<b>Issue No.</b>	<b>Rev. No.</b>	<b>Dated</b>	<b>Issued By</b>	<b>Authorized By</b>	<b>Remarks</b>
1	0	17-04-2025	SM (IT)	ED (IT)	

# Website Quality Manual for HUDCO

## Table of Contents

<b>BACKGROUND INFORMATION</b>	<b>5</b>
1. SCOPE OF THE WEBSITE QUALITY MANUAL	5
2. ABOUT THE ORGANIZATION	5
3. WEBSITE ADDRESS, DATA CENTRE & HOSTING ORGANIZATION	5
4. PURPOSE OF THE WEBSITE	5
5. OBJECTIVES OF THE WEBSITE	5
6. RESPONSIBILITY & AUTHORITY	5
7. LIST OF PLATFORMS (H/W, S/W) & WEB TECHNOLOGIES USED	6
8. USE OF CONTRACTORS / SUB CONTRACTORS	6
<b>B. POLICIES (RELEVANT CLAUSE OF GUIDELINES TO INDIAN GOVT. WEBSITES 3.0):</b>	<b>6</b>
1. COPYRIGHT POLICY (CLAUSE 5.1.4)	6
2. HYPER LINKING POLICY (CLAUSE 5.4.4).....	6
3. PRIVACY POLICY (CLAUSE 5.3.3) .....	6
4. CONTENT CONTRIBUTION, MODERATION & APPROVAL POLICY (CMAP) (CLAUSE 5.4.3) .....	7
5. WEB CONTENT REVIEW POLICY (CRP) (CLAUSE 5.4.3) .....	7
6. CONTENT ARCHIVAL POLICY (CAP) (CLAUSE 5.4.3) .....	8
7. SECURITY POLICY (CLAUSE 7.7.2) .....	8
8. WEBSITE MONITORING PLAN (CLAUSE 5.4.3) .....	11
<b>C. RESPONSIBILITY AND AUTHORITY (WEBSITE MANAGEMENT TEAM) .....</b>	<b>11</b>
1. WEB INFORMATION MANAGER (CLAUSE 5.4.1) .....	11
<b>D. MONITORING PLANS .....</b>	<b>12</b>
1. CONTINGENCY PLAN IN THE EVENT OF DEFAACEMENT / NATURAL CALAMITY (CLAUSE 5.3.3) .....	12
1.1 CONTINGENCY PLAN IN THE EVENT OF DEFAACEMENT .....	12
A.1.1. Defacement Protection Policy .....	12
A.1.2. Monitoring of defacement of <Name of Ministry / Department / Organization Website / Portal / Web Application> website	13
A.1.3. Actions to be taken after defacement	13
A.1.4. Contact details in case of any eventuality of defacement	13
A.1.5. Time for Restoration of the <Name of Ministry / Department / Organization Website / Portal / Web Application> website after defacement	13
1.2 DATA CORRUPTION	13
1.3 HARDWARE/SOFTWARE CRASH	17
1.4 NATURAL DISASTERS	14
2. WEBSITE MONITORING PLAN	14
2.1 Persons responsible	14
2.2 Frequency of monitoring	14
2.3 Monitored Parameters	14
2.4 Utility of Monitored Parameters	15
2.5 ORGANISATION STRUCTURE	16
2.6 COMPLIANCE STATEMENT	16

## Website Quality Manual for HUDCO

<i>2.7 Guidelines for Indian Government Websites</i>	16
<i>2.8 Security Audit report</i>	16
<i>2.9 MISCELLANEOUS</i>	16
<i>2.10 Person responsible for updating of website quality manual</i>	16
<i>2.11 Declaration by Website Manager</i>	16
<i>2.12 DECLARATION</i>	16
<i>2.13 ANNEXURE – I: COMPLIANCE MATRIX FOR GUIDELINES FOR INDIAN GOVERNMENT WEBSITES (GIGW) 3.0</i>	17
<i>2.14 ANNEXURE – II: SECURITY AUDIT CERTIFICATE</i>	28
<i>2.15 ANNEXURE – III VAPT REPORT DETAILS</i>	29

## A. Background information:

### 1. Scope of the Website Quality Manual (WQM)

This Website Quality Manual (WQM) is the compilation of policies, processes and procedures being followed for developing & maintaining a well-engineered website of **Housing and Urban Development Corporation Ltd.**, Government of India. It aims to address site wide issues and improve the productivity of managed web operations in terms of :-

- a) Locating relevant information
- b) Facilitating ease of use
- c) Reducing legal liabilities
- d) Providing for efficient development and maintenance considerations

### 2. About the Organization

Housing and Urban Development Corporation Ltd. (HUDCO) was incorporated on April 25, 1970 under the Companies Act 1956, is a Navratna Public Sector Undertaking (PSU) under Ministry of Housing and Urban Affairs (MoHUA), listed on major Stock Exchanges (BSE & NSE). HUDCO is a premier techno-financing CPSE in the field of housing and urban development, playing a pivotal role in the socio-economic development of India for over five decades. HUDCO is Non-Banking Financial Company – Infrastructure Finance Company (“NBFC-IFC”), regulated by Reserve Bank of India (RBI).

### 3. Website Address, Data Centre & Hosting organization

S.No.	Type	Address
1	Website Address	<a href="https://hudco.org.in">https://hudco.org.in</a>
2	Data Centre Address	HUDCO Bhawan, IT Wing, India Habitat Center, Lodhi Road, New Delhi - 110003
3	Data Recovery Centre Address	ESDS Software Solution Ltd. Reliable Teach Park, A & B Wing, 2nd Floor, Dighe, Gavthewadi, Airoli Mumbai – 400 708, Maharashtra
4	Hosting Organization Address	Same as above

### 4. Purpose of the website

HUDCO website provides information about the corporation's activities and services. HUDCO has a social mandate to meet the housing needs of the poor and disadvantaged sections of the country.

### 5. Objectives of the website

To keep its stakeholders updated with latest information, products, and events etc. Keeping transparency by sharing all the statutory requirements, notices, releases, and news on website.

### 6. Responsibility & Authority

Activity	Conducted at (Division)	Conducted by (Responsibility)
Design	IT Wing, HUDCO	IT Wing, HUDCO

<b>Development</b>	IT Wing, HUDCO	Corporate Infotech (P) Ltd
<b>Contents</b>	Depts/ROs of HUDCO	IT Wing, HUDCO
<b>Testing</b>	IT Wing, HUDCO	IT Wing, HUDCO
<b>Monitoring</b>	IT Wing, HUDCO	IT Wing, HUDCO
<b>Hosting</b>	IT Wing, HUDCO	ESDS
<b>Promotion</b>	NA	NA
<b>Website Management</b>	IT Wing, HUDCO	Corporate Infotech (P) Ltd
<b>Security</b>	ESDS	ESDS

### List of Platform - Hardware, Software and Web Technologies used

S.No	Technologies / Platforms used	Remarks
1	HTML, CSS, Boot Strap, Javascript, ASP.NET, C#, jQuery, AJAX, MySQL, IIS (Internet Information Services) 40GB disk space	

#### 7. Use of Contractors / Sub Contractors

Currently, HUDCO website is being maintained by M/s Corporate Infotech Pvt Ltd. (CIPL), who is responsible for maintenance, updation and restoration of HUDCO website.

### B. Policies (relevant clauses of Guidelines to Indian Govt. Websites GIGW3.0):

#### 1. Copyright policy (clause 5.1.4)

Contents of HUDCO website may not be reproduced partially or fully, without due permission from HUDCO. If referred to as a part of another website, the source must be appropriately acknowledged. The contents of this website cannot be used in any misleading or objectionable context. The permissions to reproduce this material shall not extend to any material which is identified as being copyright of a third party. Authorization to reproduce such material must be obtained from the copyright holders concerned.

These terms and conditions shall be governed by and construed according to the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the exclusive jurisdiction of the courts of India.

#### 2. Hyper Linking policy (clause 5.4.4)

On HUDCO website, there are many links to other websites (external links). These external links have been placed only for user's convenience. HUDCO is not responsible for the contents and reliability of the linked websites and does not endorse the views expressed in them. HUDCO have no control and guarantee over availability of linked websites.

HUDCO do not permit its webpages to be loaded into frames on any other website; HUDCO website's pages must load on a newly opened browser window of the user. Following are few external links available on HUDCO website:

S.No.	External Links
1	<a href="https://www.pmindia.gov.in/en/">https://www.pmindia.gov.in/en/</a>

2	<a href="https://www.mha.gov.in/">https://www.mha.gov.in/</a>
3	<a href="https://mohua.gov.in/">https://mohua.gov.in/</a>
4	<a href="https://rajbhasha.gov.in/">https://rajbhasha.gov.in/</a>
5	<a href="https://gem.gov.in/">https://gem.gov.in/</a>

### 3. Privacy policy (clause 5.3.3)

As per standard rule, HUDCO website does not collect Personal Information about user who visits the website. Any person can generally visit the site without revealing Personal Information, unless user chooses to provide such information.

#### Site Visit Data

HUDCO never tracks or records information about individuals and their visits. HUDCO makes no attempt to link this information with the identity of individuals visiting the website unless an attempt to damage the site has been detected. HUDCO does not identify users or their browsing activities, except when a law enforcement agency may exercise a warrant to inspect the server provider's logs.

#### Use of Cookies:

A cookie is a piece of software code that a website sends to user's browser when user accesses information at that site. This website uses cookies but not for user information gathering.

#### Email Management

User's email address is recorded only if user chooses to send a message. It will only be used for the purpose for which user provides it and will not be added to a mailing list. User's email address will not be used for any other purpose unless it is intended by the user, and will not be disclosed, without user's consent.

#### Collection of Personal Information

If users are asked for any other personal information, user will be informed that how it will be used. If at any time user believes the principles referred to in this privacy statement have not been followed, or have any other comments on these principles, he/she can notify the webmaster through the contact us page.

### 4. Content Contribution, Moderation & Approval policy (CMAP) (clause 5.4.3)

HUDCO Website Contents are to be contributed by the various Wings and HUDCO Regional Offices to maintain uniformity and up-to-date information. In order that all contents posted on the website are authentic and latest, officers/wings contributing the contents must check them thoroughly for authenticity and accuracy before sending the content for updation. Before sending new/revised contents for posting in the website, all officers/ wings should adopt the procedure as indicated in the table below relating to content contribution, moderation, and approval. The content on the portal goes through the entire life cycle process of:

- Creation
- Modification

- Approval
- Moderation
- Publishing

Once the content is contributed it needs to be approved and moderated prior to being published on the Website. All the content received is published by Web Information Manager after due approvals.

#### **5. Web Content Review Policy (CRP) (clause 5.4.3)**

HUDCO has a robust policy of reviewing its content through routine testing of web pages and the content. Since this is a website, that has information for public, shareholders of the company and govt. departments etc., the website is reviewed every quarterly to provide up to date information to its users. Monitoring of website is done on regular basis.

#### **6. Content Archival Policy (CAP) (clause 5.4.3)**

Each of the content components is accompanied by meta data, source, and validity date. Under no circumstances, any content is to be displayed on the Website after the validity date.

For few of the components like announcements, tenders, job details, only the live content whose validity date is after the current date is shown on the Website. For other components like documents, schemes, services, forms, websites and contact directory, quarterly review is been done after the review of Content Review Policy. The content Element on the Website has different Entry/Exit Policy and Archival Policy as enlisted below:

<b>Content Element</b>	<b>Entry to Archive</b>	<b>Exit from Archive</b>
Tenders	At the end of the Financial Year of the said tender or the last date of the tender, whichever is later.	After 5 years
Careers	At the end of the submission date.	After 3 years
Press Releases	After 6 months.	After 1 year
Shareholding Patterns	After 5 years	To be retained for 5 years
Financial Presentations	After 5 years	To be retained for 5 years
Financial Results	After 5 years	To be retained for 5 years
Annual Reports	After 5 years	To be retained for 5 years

#### **7. Security policy (clause 7.7.2)**

- HUDCO website has been placed in protected zones with implementation of firewalls and IDS (Intrusion Detection System) and High-Availability solutions.
- Before launch of the website, simulated penetration tests have been conducted. Penetration testing has also been conducted many times after the launch.



- HUDCO website has been audited for known application-level vulnerabilities before the launch and all the known vulnerability has been addressed.
- Hardening of servers has been done as per the guideline of Cyber Security division before the launch of the Website.
- Access to web servers hosting HUDCO website is restricted both physically and through the network as far as possible.
- Logs at different locations are maintained for authorized physical access of Web servers.
- Web-servers hosting the website are configured behind IDS, IPS (Intrusion Prevention System) and with System Firewalls on them.
- All the development work is done in a separate development environment and is well tested on the staging server before updating it on the production server.
- After testing properly on the staging server, the applications are uploaded to the production server using SSH and VPN through a single point.
- The content contributed by/from remote locations are duly authenticated & is not published on the production server directly. Any content contributed must go through the moderation process before final publishing to the production server.
- All contents of the web pages are checked for intentional or unintentional malicious content before final upload to web server pages.
- Audit and Log of all activities involving the operating system, access to the system, and access to applications are maintained and archived. All rejected accesses and services are logged and listed in exception reports for further scrutiny.
- Help Desk staff at the Monitoring Team monitor the website at intervals of daily to check the web pages to confirm that the web pages are up and running, that no unauthorized changes have been made, and that no unauthorized links have been established.
- All newly released system software patches; bug fixes and upgrades are expediently and regularly reviewed and installed on the web server.
- On Production Web Servers, Internet browsing, mail and any other desktop applications are disabled. Only server administration related tasks are performed.
- Server passwords are changed at the interval of 3 months and are shared by Website developer team.
- Smt. Poonam B Rajpal has been designated as Administrator for website and shall be responsible for implementing this policy for each of the web servers. The administrator shall also coordinate with the Audit Team for required auditing of the server(s).
- HUDCO website has been re-audited for the application-level vulnerability after major modification in application development.
- HUDCO website has been audited before launch and has complied with all the points mentioned in the policies document of the Cyber Security Group mentioned above.
- HUDCO website has also been subjected to an automated risk assessment performed through vulnerability identification software before and after the launch and all the known vulnerabilities have been addressed.
- **Notice and Disclosures**

HUDCO website do not sell, trade, or disclose the personally identifiable information of its website users to any unauthorized third parties.

- **Data Quality and Access**

HUDCO website takes all steps possible to ensure that the data on the website is accurate. While reviewing the website, if something is found to be inaccurate, HUDCO will make every effort to correct said information as quickly as possible. If it is found to be an inaccuracy with the entire system, HUDCO works swiftly to correct the problem so that web experience is as trouble-free as possible. Any change to user account will not be reflected on the website until the following business day. The information contained on HUDCO website is subject to change without prior advance notice.

While using HUDCO website certain information such as user IP Address and time spent on pages may be collected. This non-personal information is collected to monitor any unauthorized use or access to HUDCO website. Anyone caught attempting to harm, steal information from, or otherwise damage HUDCO website will be prosecuted to the full extent of the law.

- **Application Security Audit**

A Content Management System (CMS) is being used in HUDCO website for displaying the information dynamically as per the users' requests. The application has been security audited for the known application-level vulnerabilities as per Top 10 OWASP and the application security vulnerabilities have been addressed before the launch of the Portal.

The website has been audited by Cert-in empaneled agencies periodically. The periodicity shall be one year from the date of issue of certificate or additional changes in the dynamic content carried out which-ever is earlier. A periodic check on the requirement of a security certificate is recommended to the Web Information Manager in case there are changes in the functionality or any other environmental changes.

- **Server Audit**

The Applications and Database servers hosting HUDCO website and Databases have been security audited. The hardening of the server has been done. The access to the server is restricted both physically and through the network as far as possible. The Logs are being maintained for authorized physical access to HUDCO. The servers have been placed behind the Application firewall to make them hidden to the outside public. All the development work is done on separate development environment and well tested on the staging server before updating it on the production server. HUDCO website contents on ESDS Data Centre servers are uploaded using secured SSH and VPN through a single point. The contents are first checked by approval authority before publishing on the website. All contents of the web pages are checked for intentional or unintentional malicious content before final upload of the same on the website. Audit and Log of all activities referring to the operating system, access to the system and access to applications are maintained and archived. All rejected accesses and services are logged and listed in exception reports for further scrutiny. All newly released system software patches, bug fixes and upgrades are deployed regularly and reviewed. The Antivirus has been deployed on the servers and is updated online.

- **Data Security**

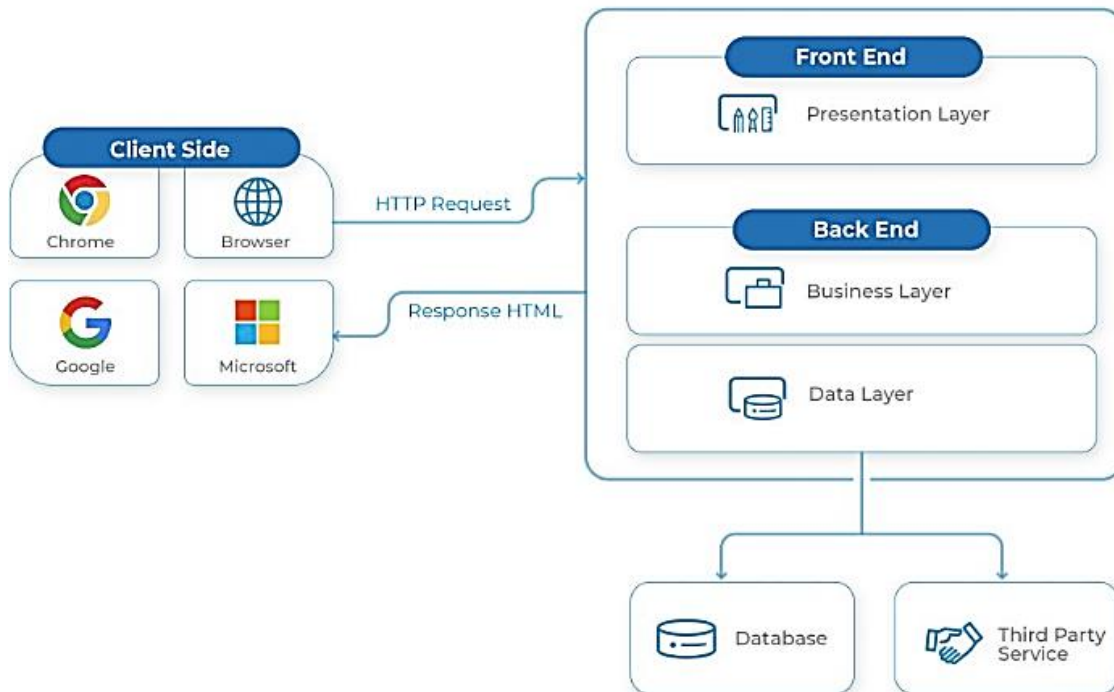
HUDCO takes Cyber security very seriously and has therefore taken every precaution to secure information of all stake holders. To secure the user's information, HUDCO has implemented

several security measures to prevent loss, theft, or misuse of any borrower data.

- **Website Access Rights**

Whether website is accessible in India only and necessary firewall rule has been applied in the system or, Website is accessible in entire world except Countries like X, Y & Z and necessary firewall rule has been applied in the system or, WIM shall identify that in which countries their websites are required to be accessible keeping in view to mitigate the cyber-attacks and accordingly firewall rules are updates.

- **Website Architecture (In Block diagram)**



## 8. Website Monitoring Plan (clause 5.4.3)

HUDCO provides this website and the information it contains as a public service. This system is monitored to ensure proper operation, to verify the functioning of applicable security features, and for comparable purposes. Anyone using this system expressly consents to such monitoring. Website is monitored periodically. The parameters like Performance, Functionality, Broken Links and Traffic Analysis are ensured for its optimal performance. The Feedback mechanism through feedback form made available for taking feedback from the visitors. Also have a mechanism for feedback analysis It will help enhancements of the website as suggested by the visitors.

## C. Responsibility and Authority (Website Management Team):

### 1. Web Information Manager (WIM) (clause 5.4.1)

The Web Information Manager (WIM) shall ensure that there is a proper flow of content to the site and that content quality and user satisfaction issues are taken care of. To achieve this, the web information Manager coordinates with the various sections of HUDCO website. The Web Information Manager also undertakes the following activities with regards to the website being maintained by them:

- Web Information Manager is overall responsible for quality and quantity of information and services on the website.
- Formulation of policies concerning management of content on the web through its entire life cycle viz. Provision, Moderation Approval and Archival.
- Ensuring that all contents on the website remain always authentic, accurate and up-to-date and obsolete information or services removed.
- Changing and periodically validating links to related information.
- Ensuring the entry of the website at a prominent rank in all the major search engines so that the site's visibility is enhanced and users are made aware of its address.
- Replying to the feedback mails received from visitors either by himself or through someone designated by him for the purpose.
- The complete contact details of the Web Information Manager are displayed on HUDCO website. The visitor could contact him/her in case of some queries or requirements.
- Contact Detail of WIM is as follows:

<p><b>Poonam B Rajpal, Sr. Manager (IT),</b> <b>HUDCO Bhawan, IT Wing, India Habitat Center, Lodhi Road, New Delhi – 110003</b> <b>Email: pb@hudco.org</b></p>
--

For HUDCO website development and management, a team has been set up under the technical manager, having professional skills in HTML authoring, programming, design, content preparation etc., which works under the overall supervision of the web information manager. The Technical Manager/Website Team has experience and skill in the following knowledge areas:-

- Website Technology
- Website Testing
- Usability
- e-accessibility
- Performance
- Security
- DARPG Guidelines
- Content Management System

**Contact Detail of Technical Manager is as follows:**

<p><b>Abhishek Sharma, Website Developer, CIPL</b> <b>HUDCO Bhawan, IT Wing, India Habitat Center, Lodhi Road, New Delhi – 110003</b> <b>Email: abhishek.sharma91@cipl.org.in</b></p>
---

## **D. Monitoring Plans:**

### **1. Contingency plan in the event of defacement / natural calamity (clause 5.3.3)**

#### **1.1 Contingency Plan in the event of defacement**

##### **A.1.1. Defacement Protection Policy**

- HUDCO website is security audited for application vulnerabilities and performance.
- Any application-level modification on the website implies re-audit of the website.
- All the servers' configuration and logs are monitored timely.
- Only system administrator users are allowed to access the servers for doing administration and configuration tasks.
- All servers are in lock and net secured.
- Contents are updated through secured FTP using VPN.

##### **A.1.2. Monitoring of defacement of HUDCO website**

There are two ways of monitoring the defacement of HUDCO website.

- Security Operation Center (SOC), Help Desk team at HUDCO Data Center and Website hosting site (ESDS) are continuously monitoring HUDCO website by analyzing the log files. They are also monitoring the websites at regular intervals for possible defacement or undesirable change in HUDCO website.
- The Development team also monitors the website regularly. In case of any eventuality, whoever notices it first shall inform the Technical Manager and Web Information Manager on Phone as well as through email.

##### **A.1.3. Actions to be taken after defacement**

As soon as the Technical Manager and/or Web Information Manager receive the information regarding the defacement of the website, the following steps will be taken:

- Stoppage/partial stoppage of the website according to the degree of defacement.
- Analyzing log files and troubleshooting the source of defacement and blocking of the service.
- Analyzing type of defacement and fixing it.
- In case of complete loss of data, restoring the website data from backup or starting of website from DR site in case of long down time.
- Giving log files to the security division for analysis.
- Fixing of all vulnerabilities based on security recommendations and re-auditing of applications.
- Restoring the affected/corrupted contents from the backup and restoring the site.

#### A.1.4. Contact details in case of any eventuality of defacement

S.No	Name	Designation	E-mail	Contact No.	Organization
1	Rupesh Shah	ED(IT)	rupesh@hudco.org	9810713788	HUDCO
2.	Satpal Singh	DGM (IT)	ssatpal@hudco.org	9810079988	HUDCO
3.	Poonam B Rajpal	SM(IT)	pb@hudco.org	9810661642	HUDCO
4.	Abhishek Sharma	WD	abhishek.sharma91@cipl.org.in	9873477663	CIPL

#### A.1.5. Time for Restoration of HUDCO website after defacement

The time taken for restoration of HUDCO website depends on the degree of defacement and services affected by the defacement.

#### 1.2 Data Corruption

Regular back-ups of the website data are being taken in HUDCO Data Centre. These enable a fast recovery and uninterrupted availability of the information to the citizens in view of any data corruption.

#### 1.3 Hardware/Software Crash

Though such an occurrence is a rarity, still in case the server on which the website is being hosted crashes due to some unforeseen reason, the web hosting service provider ESDS has enough redundant infrastructure available to restore the website at the earliest'. Generally, Time required for starting a website from another server will take about 24 hours.

#### 1.4 Natural Disasters:

There could be circumstances whereby due to some natural calamity (due to reasons beyond the control of any person), the entire ESDS Data Center where HUDCO website is being hosted gets destroyed or ceases to exist. In such an eventuality, in-charge of HUDCO will instruct that HUDCO website to be started from the DR site. Natural Disasters (DR): Storage Based Replication Takes Place at DR site

### 2. Website Monitoring Plan

#### 2.1 Persons responsible

The following Quality Managers are responsible for the monitoring of HUDCO website:

<p><b>Poonam B Rajpal, Sr. Manager (IT),</b> <b>HUDCO Bhawan, IT Wing, India Habitat Center, Lodhi Road, New Delhi – 110003</b> <b>Email: pb@hudco.org</b></p>
--

#### 2.2 Frequency of monitoring

HUDCO website undergoes regular monitoring through manual methods as well as through web analyzer tools. This is password protected and is accessed by the Website Administrator. The monitored data is analyzed monthly by HUDCO SOC team and reports are compiled. The compiled report will be made accessible to Quality Managers on monthly basis and as and when required.

## 2.3 Monitored Parameters

Though reports can be obtained on virtually every aspect of HUDCO website, for regular analysis, the quality manager is responsible for analyzing and generating the following reports;

- **Visitor's dashboard:** This report presents an overview of the Visitors Pattern to the Portal.
- **Usage Pattern:** Geographic location of visitors i.e. from which cities and countries, visitors are visiting the website
- **Hits by Hour of the Day:** This report shows the most and the least active hour of the day for the report period. If there are several days in the report period, the value presented is the sum of all hits during that period for all days.
- **Referring sites:** This report identifies the domain names and IP addresses that refer visitors to the portal.
- **Search Phrases:** This report identifies Phrases that led the most visitors to the site and for each phrase, which search engine led visitors to the site.
- **Top Pages:** List of the most popular web pages on the portal and the number of visits for each.
- **Entry Pages:** This report shows the first or "entry" pages viewed in all visits. Every visit has one and only one Entry Page. A visitor's entry page may or may not be the "home Page" The Entry Page for a visit depends on how a visitor arrived at the website.
- **Browsers:** Browsers most common among visitors to the Website.
- **Platforms:** Operating systems mostly used by visitors to access HUDCO website.

HUDCO website is also monitored for quality issues like spelling errors and broken links. Spelling checks are done on a weekly basis and broken links are monitored daily.

## 2.4 Utility of Monitored Parameters

- Visitor's pattern and usage pattern reports present the demography of the users and will be helpful in providing feedback for the personalization features that will be added in the new website.
- Search phrases report is used to know what keywords are being used to search for the website. The Pages are then optimized for these keywords.
- Top Pages are the most viewed pages and entry pages are the pages of the website other than the homepage from where the User enters the homepage. Based on the search phrases report, these pages are first optimized for search engines.
- Browser and platform reports are used to optimize the website for the most used browsers.
- Hits by hour of the day report is used to know the time of the day when there are maximum hits on the server. It is ensured that the servers must work optimally at these times.
- Referring sites report is used for link exchange with the sites that are sending the

maximum visitors to the website.

- Spelling errors are rectified as soon as they are reported.
- Broken links reports are scanned and corrections made at the earliest.

## **E. Organization Structure**

HUDCO website Development and Management Team has following Structure:

<b>S.No</b>	<b>Role</b>	<b>Responsibility</b>
1	Website Developer	Corporate Infotech (P) Ltd.
2	IT service provider	Teqsys LLP
3	Content Management	HUDCO
4	Data Center/Hosting Organization	ESDS
5	Users	HUDCO
6	Application Developer	HUDCO

## **F. Compliance statement**

### **1. Guidelines for Indian Government Websites**

**Attached as Annexure – I**

### **2. Security Audit report**

**Attached as Annexure – II & III**

## **G. Miscellaneous**

### **1. Person responsible for updating of website quality manual**

Website Information Manager is responsible for updating of website quality manual

### **2. Declaration by Website Information Manager**

It is hereby declared that HUDCO Website ([www.hudco.org.in](http://www.hudco.org.in)) is updated from time to time as per compliance

**Website Information Manager**



## Annexure I - Compliance Matrix for Guidelines for Indian Government Websites (GIGW) 3.0

S.No.	Quality Guidelines	Observation	Remarks
1	Department Association to Government is demonstrated using Emblem/Logo in proper ratio and colour, prominently displayed on the homepage/home screen of the website/app. has nominated a Web Information Manager as defined in the guidelines.	Department Association to Government is demonstrated using Emblem/Logo in proper ratio and colour, prominently displayed on the homepage/home screen of the website/app. has nominated a Web Information Manager as defined in the guidelines.	Complied
2	Ownership information is displayed on the homepage/home screen and on all important entry pages/screens of the website/app and each subsequent page/screen is a standalone entity in terms of ownership, navigation, and context of content.	Ownership information is displayed on the homepage/home screen and on all important entry pages/screens of the website/app and each subsequent page/screen is a standalone entity in terms of ownership, navigation, and context of content.	Complied
3	Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned.	Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned.	Complied
4	Due permissions have been obtained for publishing any content protected by copyright.	Due permissions have been obtained for publishing any content protected by copyright.	Complied
5	Homepage/home screen of website displays the last updated/reviewed date.	Homepage/home screen of website displays the last updated/reviewed date.	Complied
6	Complete information including title, size, format, and usage instructions is provided for all downloadable material.	Complete information including title, size, format, and usage instructions is not provided for all downloadable material.	Complied
7	Statement: With respect to each, Circular, Notification, Document, Form, Scheme, Service and Recruitment notice, the following should be clearly listed on the Website: a. Complete title b. Language (if other than English) c. Purpose/procedure to apply (as applicable) d. Validity (if applicable)	Statement: With respect to each, Circular, Notification, Document, Form, Scheme, Service and Recruitment notice, the following should be clearly listed on the Website: a. Complete title b. Language (if other than English) c. Purpose/procedure to apply (as applicable) d. Validity (if applicable)	Complied
8	All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are removed from the website and/or placed into the archives as per the archival policy.	All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are not removed from the website and/or placed into the archives as per the archival policy.	Complied
9	All information about the government organization, useful for the citizen and other stakeholders, is present in the 'About Us' section and a mechanism is in place to keep the information up to date.	All information about the government organization, useful for the citizen and other stakeholders, is present in the 'About Us' section and a mechanism is in place to keep the information up to date.	Complied

10	Website has a 'Contact Us' page providing complete contact details of important functionaries in the government organization and this is linked from the homepage/home screen and all relevant places on the website/app.	Website has a 'Contact Us' page providing complete contact details of important functionaries in the government organization and this is linked from the homepage/home screen and all relevant places on the website/app.	Complied
11	Feedback is collected through online forms and a mechanism is in place to ensure timely response to feedback/queries received through the website.	Feedback is collected through online forms and a mechanism is in place to ensure timely response to feedback/queries received through the website.	Complied
12	Website provides a prominent link to the 'National Portal' from the homepage and subsequent pages belonging to the National Portal load in the new browser window.	Website provides a prominent link to the 'National Portal' from the homepage and subsequent pages belonging to the National Portal load in the new browser window.	Complied
13	The website has been tested on multiple browsers. Hindi/Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout).	The website has been tested on multiple browsers. Hindi/Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout).	Complied
14	The website has a readily available Help section linked from all pages of the website.	The website has a readily available Help section linked from all pages of the website.	Complied
15	Website uses Cascading Style Sheets (CSS) to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes.	Website uses Cascading Style Sheets (CSS) to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes.	Complied
16	Website is readable even when style sheets are switched off or not loaded.	Website is readable even when style sheets are switched off or not loaded.	Complied
17	Proper page title and language attribute along with metadata for page like keywords and description are appropriately included.	Proper page title and language attribute along with metadata for page like keywords and description are appropriately included.	Complied
18	Minimum content as prescribed in the guidelines is present on the homepage/home screen and all subsequent pages/screens.	Minimum content as prescribed in the guidelines is present on the homepage/home screen and all subsequent pages/screens.	Complied
19	Data tables have been provided with necessary tags/markup.	Data table tags not found	Complied
20	Content of the web page prints correctly on an A4 size paper.	Content of the web page does not print correctly on an A4 size paper.	Complied
21	Website is in the nic.in or gov.in domain. Educational Institutions and Research and Academic Institutions, which are eligible for registration under 'gov.in' may use 'edu.in', 'res.in' or 'ac.in' domains.	Website is not in the nic.in or gov.in domain. Educational Institutions and Research and Academic Institutions, which are eligible for registration under 'gov.in' may use 'edu.in', 'res.in' or 'ac.in' domains.	Complied
22	API integration with key government platforms (India Portal, DigiLocker, Aadhaar, Single-Sign-On,	No API integration is found in the application	Not Applicable

	MyGov, Data Platform, MyScheme) and similar websites of the government organization must be enabled for seamless exchange of Information and data.		
23	The government organization must ensure a consistent user experience and visual identities across all its websites/apps.	The government organization not ensure a consistent user experience and visual identities across all its websites/apps.	Complied
24	Websites/apps must provide integration with popular social media.	Website has not integrated with popular social media.	Complied
25	The language is free from spelling and grammatical errors.	The language is free from spelling and grammatical errors.	Complied

S.No.	Lifecycle Management Guidelines	Observation	Remarks
1	The government organization has nominated a WIM (Web Information Manager) as defined in the guidelines.	WIM is not found on Homepage	Complied
2	It has been ensured that all stationery of the government organization as well as advertisements/public messages issued by the government organization concerned prominently display the URL of the web site.	URL is not mentioned inside document and advertisements.	Not Applicable
3	Website has the following clearly defined policies and plans approved by the WIM. a) Copyright Policy b) Content Contribution, Moderation and Approval (CMAP) policy c) Content Archival (CAP) policy d) Content Review (CRP) policy e) Hyper linking Policy f) Privacy Policy g) Terms & Conditions h) Website Monitoring Plan. i) Contingency Management Plan j) Security Policy	Policies are not found on Homepage.	Complied
4	The mechanism is in place to check the accuracy of Hyperlinked Content and clear indications are given when a link leads out to a non-government website.		Complied
5	It is ensured through content moderation and approval policy that Website content is free from offensive/discriminatory language.	Content moderation policy is not on the website.	Complied
6	Documents/Pages in multiple languages are updated simultaneously.	Documents/Pages in multiple languages are updated simultaneously.	Complied
7	Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors.	Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors.	Complied

8	There are no links to 'under construction' pages.	There are no links to 'under construction' pages.	Complied
9	Documents are provided either in HTML or other accessible formats.	Documents are provided either in HTML or other accessible formats.	Complied
10	Website is bilingual with a prominent language selection link and uses Unicode characters.	Yes	Complied

S.No.	Accessibility Guidelines	Observation	Remarks
1	All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below.	All non-text content that is presented to the user does not have a text alternative that serves the equivalent purpose, except for the situations listed below.	Complied
2	For pre-recorded audio-only and pre-recorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labelled as such: a) Pre-recorded Audio-only: An alternative for time-based media is provided that presents equivalent information for pre-recorded audio-only content. b) Pre-recorded Video-only: Either an alternative for time-based media or an audio track is provided that presents equivalent information for pre-recorded video-only content.	Audio/video content not found	Complied
3	Captions are provided for all pre-recorded audio content in synchronized media, except when the media is a media alternative for text and is clearly labelled as such.	Audio/video content not found	Complied
4	An alternative for time-based media or audio description of the pre-recorded video content is provided for synchronized media, except when the media is a media alternative for text and is clearly labelled as such.	Audio/video content not found	Complied
5	Captions are provided for all live audio content in synchronized media.	Audio/video content not found	Complied
6	Audio description is provided for all pre-recorded video content in synchronized media.	Audio/video content not found	Complied
7	Information, structure, and relationships conveyed through presentation can be programmatically determined or are available in text.	Information, structure and relationships conveyed through presentation can be programmatically determined or are available in text.	Complied
8	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	Complied
9	Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, colour, size, visual location, orientation, or		Complied

	sound.		
10	Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.	Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.	Complied
11	The purpose of each input field collecting information about the user can be programmatically determined when: a. The input field serves a purpose identified in the Input Purposes for User Interface Components section; and b. The content is implemented using technologies with support for identifying the expected meaning for form input data.	"The purpose of each input field collecting information about the user can be programmatically determined when: a. The input field serves a purpose identified in the Input Purposes for User Interface Components section; and b. The content is implemented using technologies with support for identifying the expected meaning for form input data."	Complied
12	Colour is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Colour is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Complied
13	If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level.	Audio media not found	Not Applicable
14	The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: a) Large Text: (18 pt. or 14 pt. bold) Large-scale text and images of large-scale text have a contrast ratio of at least 3:1. b) Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. c) Logotypes: Text that is part of a logo or brand name has no contrast requirement.	Background and foreground colors do not have a sufficient contrast ratio.	Complied
15	Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality.	Texts are not zooming upto 200 percent	Complied
16	If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text except for the following: a) Customizable: The image of text can be visually customized to the user's requirements. b) Essential: A particular presentation of text is essential to the information being conveyed.	"If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text except for the following: a. Customizable: The image of text can be visually customised to the user's requirements. b. Essential: A particular presentation of text is essential to the information being conveyed."	Complied

	<ul style="list-style-type: none"> <li>a) Content can be presented without loss of information or functionality, and without requiring scrolling in two dimensions for:</li> <li>b) Vertical scrolling content at a width equivalent to 320 CSS pixels;</li> <li>c) Horizontal scrolling content at a height equivalent to 256 CSS pixels;</li> <li>d) Except for parts of the content which require a two-dimensional layout for usage or meaning.</li> </ul>	<p>"a. Content can be presented without loss of information or functionality, and without requiring scrolling in two dimensions for:</p> <ul style="list-style-type: none"> <li>b. Vertical scrolling content at a width equivalent to 320 CSS pixels;</li> <li>c. Horizontal scrolling content at a height equivalent to 256 CSS pixels;</li> <li>d. Except for parts of the content which require a two-dimensional layout for usage or meaning."</li> </ul>	Complied
18	<p>The visual presentation of the following has a contrast ratio of at least 3:1 against adjacent colour(s):</p> <ul style="list-style-type: none"> <li>a) User Interface Components: Visual information required to identify user interface components and states, except for inactive components or where the appearance of the component is determined by the user agent and not modified by the author.</li> <li>b) Graphical Objects: Parts of graphics required to understand the content, except when a particular presentation of graphics is essential to the information being conveyed.</li> </ul>	Background and foreground colors do not have a sufficient contrast ratio.	Complied
19	<p>In content implemented using markup languages that support the following text style properties, no loss of content or functionality occurs by setting all of the following and by changing no other style property:</p> <ul style="list-style-type: none"> <li>a) Line height (line spacing) to at least 1.5 times the font size.</li> <li>b) Spacing following paragraphs to at least 2 times the font size.</li> <li>c) Letter spacing (tracking) to at least 0.12 times the font size.</li> <li>d) Word spacing to at least 0.16 times the font size.</li> <li>e) Exception: Human languages and scripts that do not make use of one or more of these text style properties in written text can conform using only the properties that exist for that combination of language and script.</li> </ul>		Complied

20	<p>Where receiving and then removing pointer hover or keyboard focus triggers additional content to become visible and then hidden, the following are true:</p> <ul style="list-style-type: none"> <li>a) Dismissible: A mechanism is available to dismiss the additional content without moving pointer hover or keyboard focus unless the additional content communicates an input error or does not obscure or replace other content</li> <li>b) Hover-able: If pointer hover can trigger the additional content, then the pointer can be moved over the additional content without the additional content disappearing.</li> <li>c) Persistent: The additional content remains visible until the hover or focus trigger is removed, the user dismisses it, or its information is no longer valid.</li> </ul>		Complied
21	<p>All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints.</p>		Complied
22	<p>If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away.</p>		Complied
23	<p>If a keyboard shortcut is implemented in content using only letter (including upper- and lower-case letters), punctuation, number, or symbol characters, then at least one of the following is true:</p> <ul style="list-style-type: none"> <li>a) Turn off: A mechanism is available to turn the shortcut off.</li> <li>b) Remap: A mechanism is available to remap the shortcut to include one or more non-printable keyboard keys (e.g., Ctrl, Alt).</li> <li>c) Active only on focus: The keyboard shortcut for a user interface component is only active when that component has focus.</li> </ul>	<p>"If a keyboard shortcut is implemented in content using only letter (including upper- and lower-case letters), punctuation, number, or symbol characters, then at least one of the following is true:</p> <ul style="list-style-type: none"> <li>a. Turn off: A mechanism is available to turn the shortcut off.</li> <li>b. Remap: A mechanism is available to remap the shortcut to include one or more non-printable keyboard keys (e.g., Ctrl, Alt).</li> <li>c. Active only on focus: The keyboard shortcut for a user interface component is only active when that component has focus." </li></ul>	Complied

24	<p>For each time limit that is set by the content, at least one of the following is true:</p> <ul style="list-style-type: none"> <li>a) Turn off: The user is allowed to turn off the time limit before encountering it; or Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or</li> <li>b) Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, “press the spacebar”) and the user is allowed to extend the time limit at least ten times; or</li> <li>c) Real-time Exception: The time limit is a required part of a real-time event (for example, an auction) and no alternative to the time limit is possible; or</li> <li>d) Essential Exception: The time limit is essential and extending it would invalidate the activity; or</li> <li>e. 20 Hour Exception: The time limit is longer than 20 hours.</li> </ul>		Not Applicable
25	<p>For moving, blinking, scrolling, or auto-updating information, all of the following are true:</p> <ul style="list-style-type: none"> <li>a) Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and</li> <li>b) Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential.</li> </ul>	<p>"For moving, blinking, scrolling, or auto-updating information, all of the following are true:</p> <ul style="list-style-type: none"> <li>a. Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and</li> <li>b. Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential." </li></ul>	Complied
26	<p>Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds.</p>		Not Applicable
27	<p>A mechanism is available to bypass blocks of content that are repeated on multiple Web pages.</p>	<p>A mechanism is available to bypass blocks of content that are repeated on multiple Web pages.</p>	Complied
28	<p>Web pages have titles that describe the topic or purpose.</p>	<p>Web pages have titles that describe the topic or purpose.</p>	Complied
29	<p>If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability.</p>	<p>If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability.</p>	Complied



30	The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general.	The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general.	Complied
31	More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process.	More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process.	Complied
32	Headings and labels describe topic or purpose.	Headings and labels describe topic or purpose.	Complied
33	Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible.	Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible.	Complied
34	All functionality that uses multipoint or path-based gestures for operation can be operated with a single pointer without a path-based gesture, unless a multipoint or path-based gesture is essential.		Not Applicable
35	For functionality that can be operated using a single pointer, at least one of the following is true: a) No Down-Event: The down-event of the pointer is not used to execute any part of the function. b) Abort or Undo: Completion of the function is on the up-event and a mechanism is available to abort the function before completion or to undo the function after completion. c) Up Reversal: The up-event reverses any outcome of the preceding down-event. d) Essential: Completing the function on the down-event is essential.		Not Applicable
36	For user interface components with labels that include text or images of text, the name contains the text that is presented visually.	For user interface components with labels that include text or images of text, the name contains the text that is presented visually.	Complied
37	Functionality that can be operated by device motion or user motion must also be operable by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: a) Supported Interface: The motion is used to operate functionality through an accessibility supported interface. b) Essential: The motion is essential for the function and doing so would invalidate the activity.	The default human language of each Web page can be programmatically determined.	Not Applicable
38	The default human language of each Web page can be programmatically determined.	The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of	Complied

		indeterminate language and words or phrases that have become part of the vernacular of the immediately surrounding text.	
39	The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language and words or phrases that have become part of the vernacular of the immediately surrounding text.	When any user interface component receives focus, it does not initiate a change of context.	Complied
40	When any user interface component receives focus, it does not initiate a change of context.	When any user interface component receives focus, it does not initiate a change of context.	Complied
41	Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behaviour before using the component.	Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behaviour before using the component.	Complied
42	Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user.	Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user.	Complied
43	Components that have the same functionality within a set of Web pages are identified consistently.	Components that have the same functionality within a set of Web pages are identified consistently.	Complied
44	If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.	If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.	Complied
45	Labels or instructions are provided when content requires user input.	Labels or instructions are provided when content requires user input.	Complied
46	If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content.	If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content.	Complied
47	For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: a. Reversible: Submissions are reversible. b. Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. c. Confirmed: A mechanism is available for reviewing, confirming and correcting information before finalising the submission.	For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: a. Reversible: Submissions are reversible. b. Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. c. Confirmed: A mechanism is available for reviewing, confirming and correcting information before finalising the submission.	Not Applicable
48	In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their	HTML and CSS Errors are present on the website	Complied

	specifications, elements do not contain duplicate attributes and any IDs are unique, except where the specifications allow these features.		
49	For all user interface components (including but not limited to form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.	For all user interface components (including but not limited to form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.	Complied
50	In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus.	In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus.	Complied

<b>S.No.</b>	<b>Security Guidelines</b>	<b>Observation</b>	<b>Remarks</b>
1	The website, web application, web portal or mobile app is Security Audited and an Audit Clearance certificate is issued by NIC, STQC or a CERT-In empaneled vendor before hosting in production environment.	Security audit pending	Certificate available on website
2	Hosting Environment must be secured for ensuring confidentiality, integrity, and availability (CIA).	No info received	Certificate available on website
3	Website has clearly defined Security Policy, Privacy Policy and Contingency Management Plan approved by the Web Information Manager.	Policies are not defined	Complied

## Annexure II - Security Audit Certificate

Allied Boston  
sustainable excellence...achieved.



# SAFE TO HOST

## THIS COMPLIANCE CERTIFICATE IS PRESENTED TO

Organization	Housing & Urban Development Corporation Limited
Application	HUDCO Website
Type of Audit	Website/Web Application
URL (Staging)	http://10.2.103.89:8081/
URL (Production)	https://www.hudco.org.in/
Initial Testing	02/11/2023 - 02/11/2023
Re-validation	07/02/2024 - 07/02/2024
Report ID	R2306087 - 002
Hash	9c5e7a329684fa3427e8293465539cf075 c12afcc4d4cf001ceb591f0a261dfc

### CONCLUSION/s

- No vulnerabilities were found during the re-validation, pl. refer final report.
- The said application/s is safe for hosting with privileges of read permission for general public.

### RECOMMENDATION/s

- Application should be deployed on hardened Server & Operating System.
- SSL should be deployed before putting on the production server.
- The certificate is valid for **ONE YEAR** from the date of issue or **till any changes made in the code of the application or any new vulnerability is discovered whichever is earlier.**
- Conduct proactive testing periodically & ensure any new changes introduced in the application undergo a security testing before they are published on the network.



Scan to verify

Issued on: 27/02/2024

Certificate No.: C2306087 - 002



**T. Ganguly**  
Head - Information Security

Allied Boston Consultants India Pvt. Ltd. is an IT Security Auditing Organization, empanelled by Indian Computer Emergency Response Team (CERT-IN), Ministry of Electronics & Information Technology, New Delhi, Government of India

for more details: [itsec@alliedboston.com](mailto:itsec@alliedboston.com) [+91-9899589111](tel:+91-9899589111) [www.alliedboston.com](http://www.alliedboston.com)

## Annexure – III - VAPT Report

Housing and Urban Development Corporation



# Cyber Security Audit Final Report

**Website/Web Application,**  
HUDCO Main Website

**Housing and Urban Development Corporation**

Report Date: **February 27, 2024**

Report ID: **R2306087 - 002**

Issued By,

**Allied Boston Consultants India Pvt. Ltd.**

2205, Express Trade Towers 2, Sector - 132, Noida - 201301, India

Tel.: **+91. 120. 4113528 / 4113529**

CRM: **+91. 9953432070**

URL: **www.alliedboston.com**

**Allied Boston Consultants India Pvt. Ltd.** is an **IT Security Auditing Organization**, empanelled by Indian Computer Emergency Response Team (**CERT-IN**), Ministry of Electronics & Information Technology, New Delhi, Government of India  
**For more details, please contact: Email: [itsec@alliedboston.com](mailto:itsec@alliedboston.com), Phone: +91.9899589111, Website: [www.alliedboston.com](http://www.alliedboston.com)**

DOCUMENT PROPERTIES	
Document Version Control	1.1
Author	Allied Boston Consultants India Pvt. Ltd
Report Type	Final Report
Report Link	Provide Later

DOCUMENT SUBMISSION DETAILS	
Date of Report	February 27, 2024
Submitted To	Dr. Satpal Singh (DGM(IT))
Classification	Confidential
Geographical detail of Client (State/UT)	New Delhi

DOCUMENT DISTRIBUTION LIST		
S.No.	Name of Testing Team	Responsibility
1	Mr. Pravesh Grewal	Tester
2	Miss. Priyanka Jangid	Reviewer

## DISCLAIMER

This document is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this disclaimer is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this document is strictly prohibited. If you received this document in error, please notify us immediately by telephone and return the original document to us at the address below. If you have received an electronic copy of the document, please remove it immediately after reading this disclaimer.

## LEGAL NOTICE

As used herein, Confidential Information shall mean any information and data of a confidential or proprietary nature which is disclosed by **Housing and Urban Development Corporation** to **Allied Boston Consultants India Pvt. Ltd.** such as customer information, proprietary technical, financial, personnel, marketing, pricing, sales and/or commercial information with respect to computer networking, data communications and computing services as well as drawings, reports, ideas, concepts, designs and inventions, computer source and object code and computer programming techniques; and all record bearing media containing or disclosing such information and techniques which are disclosed pursuant to this report. **Allied Boston Consultants India Pvt. Ltd.** shall maintain the Confidential Information and its contents cannot be disclosed or copied without the prior written consent of **Housing and Urban Development Corporation**.

## LIMITATION ON DISCLOSURE AND USE OF THIS REPORT

This report contains information concerning potential vulnerabilities of **Housing and Urban Development Corporation** systems and methods of exploiting them. **Allied Boston Consultants India Pvt. Ltd.** recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein. **Allied Boston Consultants India Pvt. Ltd.** has retained and secured a copy of the report for customer reference. All other copies of the report have been delivered to **Housing and Urban Development Corporation**. Security assessment is an uncertain process, based upon past experiences, currently available information, and known threats. It should be understood that all information systems, which by their nature are dependent on human beings, are vulnerable to some degree.

Therefore, while **Allied Boston Consultants India Pvt. Ltd.** considers the major security vulnerabilities of the analyzed systems to have been identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures. In addition, the analysis set forth herein is based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities associated with the operation of **Housing and Urban Development Corporation's** systems described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities, will also change.

**Allied Boston Consultants India Pvt. Ltd.** makes no undertaking to supplement or update this report on the basis of changed circumstances or facts of which **Allied Boston Consultants India Pvt. Ltd.** becomes aware after the date hereof, absent a specific written agreement to perform supplemental or updated analysis.

This report may recommend that **Housing and Urban Development Corporation** to use certain software or hardware products manufactured or maintained by other vendors. **Allied Boston Consultants India Pvt. Ltd.** bases these recommendations upon its prior experience with the capabilities of those products. Nonetheless, **Allied Boston Consultants India Pvt. Ltd.** does not and cannot warrant that a particular product will work as advertised by the vendor, nor that it will operate in the manner intended.

This report was prepared by **Allied Boston Consultants India Pvt. Ltd.** for the exclusive use and benefit of **Housing and Urban Development Corporation** and is deemed proprietary information.

## LIMITED LIABILITY

The vulnerability assessment provides a snapshot of the current security problems of the application/system, and it is limited in terms of time and personnel. Therefore, we cannot provide a 100% guarantee that the system will stay secure over time.



## Table Of Content

<b>1. Executive Summary</b> .....	<b>6</b>
1.1. Test Goal & Objective .....	<b>6</b>
1.2. Scope of Testing .....	<b>7</b>
1.3. Summary of Findings .....	<b>8</b>
<b>2. Engagement Details</b> .....	<b>10</b>
2.1. Methodology .....	<b>10</b>
2.2. Tools Used For Testing .....	<b>11</b>
2.3. Test Narrative .....	<b>12</b>
<b>3. Detailed Report Of Vulnerabilities</b> .....	<b>14</b>
<b>4. Conclusion</b> .....	<b>25</b>
4.1. Dependency .....	<b>25</b>
4.2. Verdict .....	<b>25</b>
<b>5. Way Ahead</b> .....	<b>27</b>
<b>6. Glossary</b> .....	<b>27</b>
6.1. Reference .....	<b>27</b>

## 1. EXECUTIVE SUMMARY

Allied Boston Consultants India Pvt. Ltd. conducted a **Website/Web Application** security audit of **Housing and Urban Development Corporation**. This test was performed using industry standard frameworks and tools to assess defensive posture and provide security assistance through proactively identifying vulnerabilities, severity ranking, and remediation steps.

### 1.1. TEST GOAL & OBJECTIVE

The goal was to find out technology vulnerabilities in the **Housing and Urban Development Corporation Website/Web Application**. The tests were carried out with the close coordination of Client Development team.

Vulnerability Assessment and Penetration Testing (VAPT) is a process to evaluate the security risks in the websites / web applications / thick clients that are delivered over the internet, vital for business operations with many web apps processing sensitive data, in order to reduce the probability of a threat (i.e., intruder / hacker getting unauthorized access by exploiting weaknesses) and to eliminate cyber security exposures. VAPT includes anything from automated vulnerability assessment to human-led penetration testing and full-scale red team simulated cyber-attacks.

Using the OWASP (Open Web Application Security Project) and other industry standards, testing is done to identify security risks (such as injection flaws, security misconfigurations, authentication weakness, database interaction errors, poor session management, input validation problems, broken access controls, flaws in application logic etc.), analyze and attempt to harmlessly exploit all design / implementation / operational vulnerabilities identified, prioritize severity levels (High, Medium, Low) and report the vulnerabilities outlining key findings, provide supplementary technical information (where possible), and provide appropriate remedial actions.

## 1.2. SCOPE OF TESTING

The security audit was required to be conducted internally, towards the organization's intranet facing Website/Web Application.

<b>APPLICATION NAME</b>	HUDCO Main Website
<b>TESTING / STAGING URL</b>	http://10.2.103.89:8081/
<b>PRODUCTION URL</b>	https://www.hudco.org.in/
<b>TESTING TYPE</b>	Black Box

### 1.2.3. TIMELINES

<b>INITIAL AUDIT</b>	From <b>November 02, 2023</b> to <b>November 02, 2023</b>
<b>RE-AUDIT (VALIDATION OF CLOSURE)</b>	From <b>February 07, 2024</b> to <b>February 07, 2024</b>

### 1.2.4. REASON FOR CONDUCTING AUDIT

Certificate of safe hosting

### 1.3. SUMMARY OF FINDINGS

During this assignment **01-Medium, 5-Low** vulnerability(s) were found. The below table summarizes the list of findings identified during Initial testing.

S.N.	Finding Name	Severity	Status
1	Host Header Injection	Medium	Closed
2	Using Components with Known Vulnerabilities	Low	Closed
3	Unencrypted communication	Low	Closed as Dependency
4	Missing Security Headers	Low	Closed
5	HTTP OPTIONS Method Enabled	Low	Closed
6	Strict Transport Security Not Enforced	Low	Closed

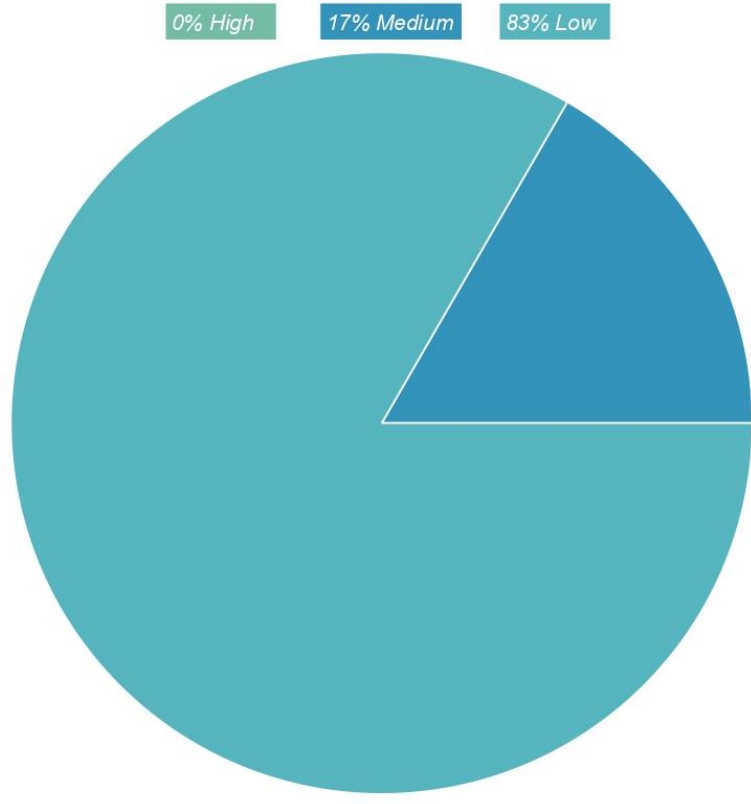
After **Housing and Urban Development Corporation Website/Web Application** development team took closure action, completed closure validation (re-audit).

#### 1.3.1. RISK EVALUATION

Risk evaluation is done based on the vulnerabilities found on the assets that need to be protected while taking into consideration the threat agents that may be involved in a real-time scenario. Based on the results of this security audit, the risk that malicious actors/elements pose to the application was **MEDIUM**.

### 1.3.2. GRAPHICAL SUMMARY

Vulnerability Chart



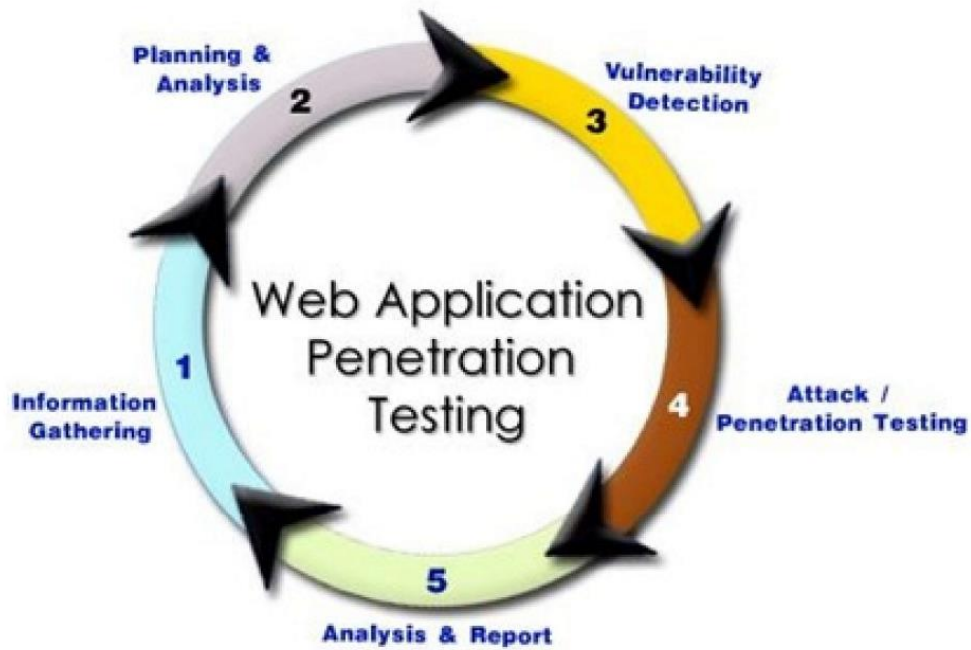
## 2. ENGAGEMENT DETAILS

### 2.1. METHODOLOGY

A vulnerability assessment and penetration test simulate covert and hostile activities in order to identify exploitable vulnerabilities and to expose potential entryways to vital or sensitive data that, if discovered and misused by a malicious individual, could pose increased risk and liability to the organization, its executives and shareholders.

**Allied Boston Consultants India Pvt. Ltd.** security consultants who perform penetration tests attempt to gain access to online assets and company resources through the website / web application / thick client from the external perspective, much like an attacker would do, the results clearly articulating the underlying security issues and recommendations.

Our Web Application Security Assessment Flowchart is as follows,



### 2.1.1. INFORMATION GATHERING

The application details are understood. The test environment was provided by the organization's development team. Testing was conducted during normal business hours. The tester locates publicly accessible information and finds out ways that can be exploited for getting into the systems. The tester employs tools like port scanners for completely understanding the software systems in a network and pinpoints different findings probable impact on the organization.

### 2.1.2. PLANNING

The scope was defined based on the nature, timing, and extent of the evaluation, which was to be conducted in consultation with the organization's development team. The planning process was initiated by defining penetration testing's objectives, thereby goals are defined jointly by the tester and the organization's development team so that both parties have the same level of understanding and objectives. The nature and type of the tools to be used was determined by the **Allied Boston's** Security Team.

### 2.1.3. ATTACK & VAPT

It was done presuming that the tester was an external attacker. The tools were used for this purpose.

**Vulnerability detection** – Response of target app to several intruder attack is understood. Static as well as dynamic analysis is used. The former method is used to check whether the application code is behaving in the exact way it should be while running or not & the latter one involves its inspection in the running condition.  
**Penetration testing** – It utilizes web app attacks like cross-site scripting (XSS), backdoor, and SQL injection for uncovering the target's vulnerabilities which are exploited to comprehend the destruction that they can cause.

POC, where applicable, for the vulnerabilities which was exploited during the test was compiled for further reporting along with remediations for closing them in a planned manner.

**Standards and Framework Followed:**

A. Open Web Application Security Project Framework (OWASP) – top 10 vulnerabilities verified, viz.,

1. Injection
2. Broken Authentication and Session Management
3. Sensitive Data Exposure
4. XML External Entity
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

## 2.1.4. ANALYSIS & REPORT

The test results were consolidated based on the rating of the vulnerabilities reported and compiled into the report briefing any sensitive data accessed and vulnerabilities exploited.

**Severity Rating** – Depicts the severity of impact to the organization. It could represent business impact, financial impact or damage to customer, partner or reputation.

Severity	Color Notation	Severity Description
<b>HIGH</b>	<b>Red</b>	It is imperative, that effort to be undertaken immediately to mitigates the vulnerabilities in this category.
<b>MEDIUM</b>	<b>Orange</b>	Medium threats need to be reviewed and discussed after which its treatment should be designed as a part of the security plan.
<b>LOW</b>	<b>Green</b>	Low threats need to be reviewed and discussed.

The report was then created by articulating the analyses so performed along with recommendations for closure. Results are collated in tabular form for easy reference.

Vulnerability will be accompanied by a short description and screenshots (where applicable).

## 2.2. TOOLS USED FOR TESTING

**2.2.1. Commercial Tools:** Burp Suite Professional

**2.2.2. Opensource Tools:** Nuclei, Dirsearch

Further, **Manual Testing** was also performed to analyze and validate the results from using the above testing tools.

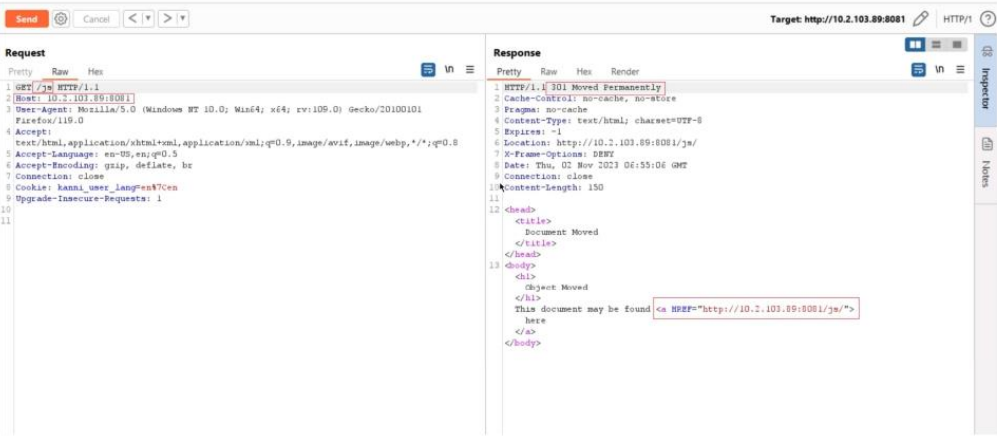


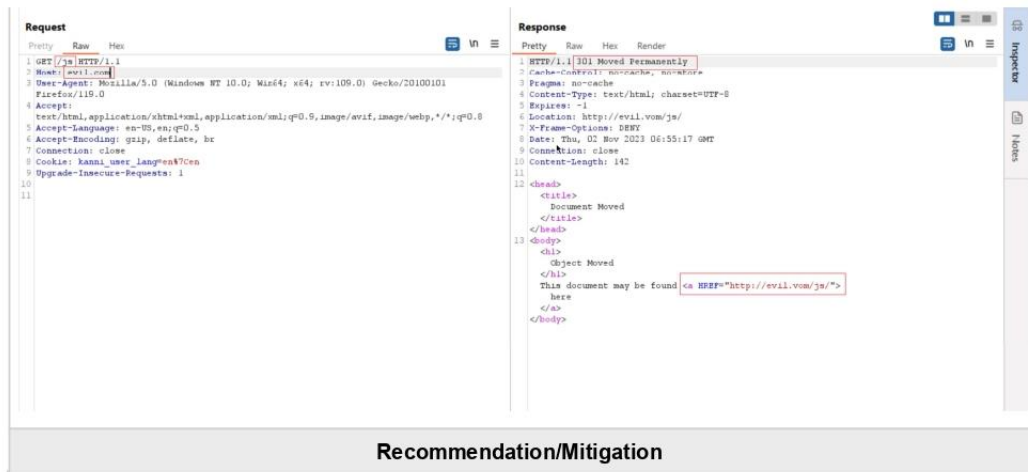
### 2.3. TEST NARRATIVE

The purpose & business context of the application has been understood and the possible ways in which a malicious entity would approach to find vulnerabilities in the application have been identified. The OWASP methodology has been followed to find vulnerabilities in the application and is documented in the rest of the report.

### 3. DETAILED REPORT OF VULNERABILITIES

#### 3.1 HOST HEADER INJECTION

Vulnerability Description		Severity
<p>It is common practice for the same webserver to host several websites or web applications on the same IP address. This is why the host header exists. The host header specifies which website or web application should process an incoming HTTP request. The web server uses the value of this header to dispatch the request to the specified website or web application.</p>		<b>Medium</b>
Vulnerability Identification Number (CWE)	Attributing Factor	
Improper Input Validation - (CWE-20)	Coding Error	
Affected Platform(URLs)		
1. <a href="http://10.2.103.89:8081/js">http://10.2.103.89:8081/js</a>		
Penetration Testing: Proof of Concept		
Step 1.		
		
Step 2.		



**Recommendation/Mitigation**

To prevent HTTP Host header attacks, the simplest approach is to avoid using the Host header altogether in server-side code. Double-check whether each URL really needs to be absolute. You will often find that you can just use a relative URL instead. This simple change can help you prevent web cache poisoning vulnerabilities in particular.

**Mitigations must be implemented throughout the application.**

**3.2 USING COMPONENTS WITH KNOWN VULNERABILITIES**

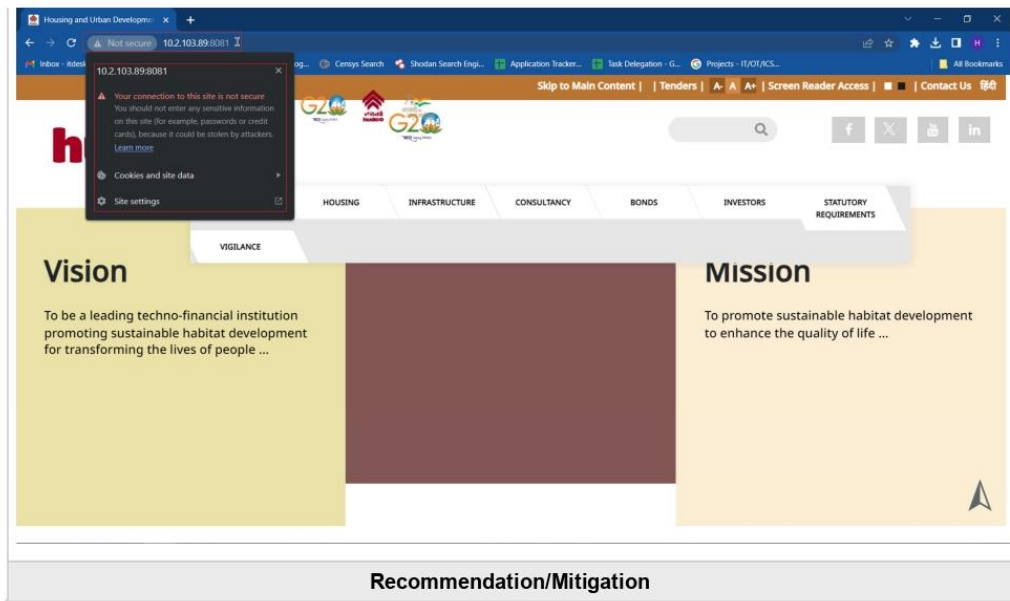
Vulnerability Description		Severity
<p>The use of third-party libraries can introduce a range of multiple vulnerabilities, including some that can be used to hijack user accounts like XSS etc.</p> <p>Common third-party libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.</p> <p>Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.</p>		Low
Vulnerability Identification Number (CWE)	Attributing Factor	
Use of Unmaintained Third Party Components - (CWE-1104)	Vulnerable Software Versions	
Affected Platform(URLs)		
1. http://10.2.103.89:8081/js_new/jquery.min.js		
Penetration Testing: Proof of Concept		
Step 1.		



### 3.3 UNENCRYPTED COMMUNICATION

Vulnerability Description		Severity
<p>The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.</p> <p>To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.</p> <p>Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.</p>		<b>Low</b>
Vulnerability Identification Number (CWE)	Attributing Factor	
Inadequate Encryption Strength - (CWE-326)	Deployment error	
Affected Platform(URLs)		
1. http://10.2.103.89:8081/		
Penetration Testing: Proof of Concept		
Step 1.		

## Housing and Urban Development Corporation

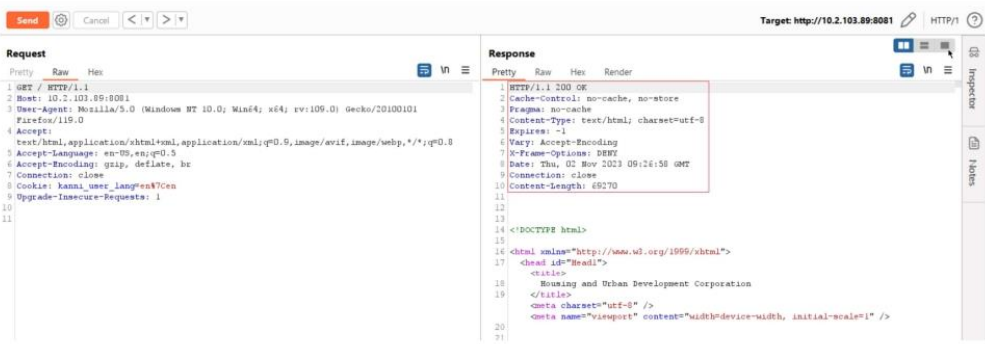


Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server.

The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

**Mitigation must be implemented throughout the Application/ API where applicable.**

### 3.4 MISSING SECURITY HEADERS

Vulnerability Description		Severity
<p>HTTP response headers that your application can use to increase the security of your application. Once set, these HTTP response headers can restrict modern browsers from running into easily preventable vulnerabilities. It intends to raise awareness and use of these headers.</p>		Low
Vulnerability Identification Number (CWE)	Attributing Factor	
Protection Mechanism Failure - (CWE-693)	Coding Error	
Affected Platform(URLs)		
1. http://10.2.103.89:8081/		
Penetration Testing: Proof of Concept		
Step 1.		
		
Recommendation/Mitigation		

For additional security implement the following security headers in the Static Website:

**Content-Security-Policy:** default-src, base-uri, **X-Content-Type-Options:** nosniff;  
**Referrer-Policy:** strict-origin-when-cross-origin

For additional security implement the following headers in the Dynamic Web Application:

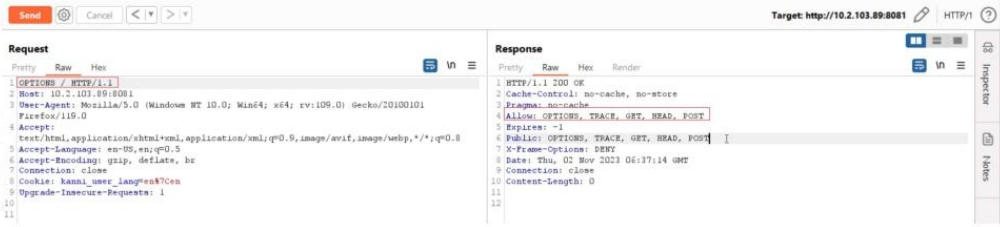
**Content-Security-Policy:** default-src, base-uri, **X-Content-Type-Options:** nosniff; **Cache-Control:** no-cache, no-store, max-age=63115200; **Clear-Site-Data:** "\*" ; **Referrer-Policy:** strict-origin-when-cross-origin .



Housing and Urban Development Corporation

**Mitigation must be implemented throughout the Application/ API where applicable.**

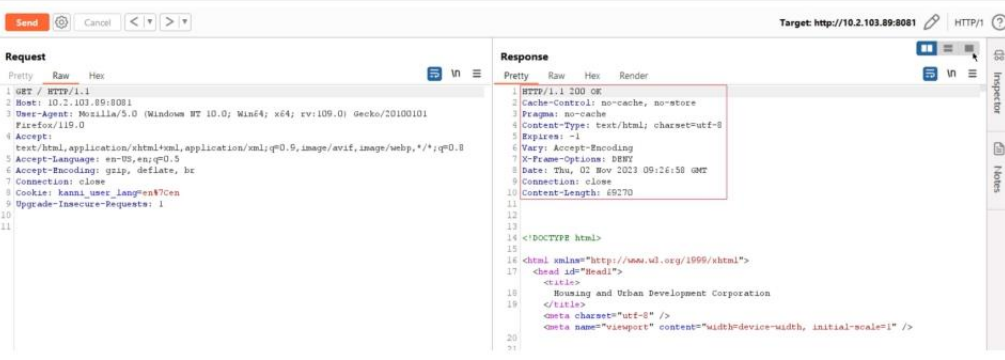
### 3.5 HTTP OPTIONS METHOD ENABLED

Vulnerability Description	Severity
HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server. It represents a request for information about the communication options available on the request/response chain identified by the Request-URI.	Low
Vulnerability Identification Number (CWE)	Attributing Factor
Trusting HTTP Permission Methods on the Server Side - (CWE-650)	Coding Error
Affected Platform(URLs)	
1. http://10.2.103.89:8081/	
Penetration Testing: Proof of Concept	
Step 1.	
	
Recommendation/Mitigation	

It's recommended to disable the OPTIONS Method on the web server.

**Mitigation must be implemented throughout the Application where applicable.**

### 3.6 STRICT TRANSPORT SECURITY NOT ENFORCED

Vulnerability Description		Severity
<p>The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.</p>		Low
Vulnerability Identification Number (CWE)	Attributing Factor	
Unprotected Transport of Credentials - (CWE-523)	Coding Error	
Affected Platform(URLs)		
1. http://10.2.103.89:8081/		
Penetration Testing: Proof of Concept		
Step 1.		
 <p>The screenshot shows a network inspector tool displaying an HTTP request and response. The request is a GET for / HTTP/1.1. The response is a 200 OK with headers including Cache-Control: no-cache, no-store, Expires: -1, and Vary: Accept-Encoding. The response body contains HTML for 'Housing and Urban Development Corporation'.</p>		
Recommendation/Mitigation		

The application should instruct web browsers only to access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where to expire time is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag.

Housing and Urban Development Corporation

**Mitigation must be implemented throughout the Application/ API where applicable.**

## 4. CONCLUSION

Based on this **Website/Web Application** Penetration Testing conducted by **Allied Boston Consultants India Pvt. Ltd.** It was observed that **MEDIUM, LOW** vulnerabilities did exist within the **Housing and Urban Development Corporation Website/Web Application**.

S.N.	Finding Name	Severity	Status
1	Host Header Injection	Medium	Closed
2	Using Components with Known Vulnerabilities	Low	Closed
3	Unencrypted communication	Low	Closed as Dependency
4	Missing Security Headers	Low	Closed
5	HTTP OPTIONS Method Enabled	Low	Closed
6	Strict Transport Security Not Enforced	Low	Closed

The **1- Medium, 4- Low** reported vulnerability(s) has been patched as per remediations provided.

## 4.1. DEPENDENCY

The **1-Low** vulnerability has been closed with dependency based on the below client response:

Dependency response vide email February 07, 2024 quoted below:

1. Unencrypted communication

Severity: **Low**

**Response:** The staging server is prepared for testing purposes. Hence, the SSL is implemented in the production server.

**Auditor Judgement:** The SSL certificate has been implemented in the production URL (<https://www.hudco.org.in/>). Hence, closed as dependency.

## 4.2. VERDICT

**SAFE TO HOST**

## 5. WAY AHEAD

A monitoring mechanism should be instituted to ensure compliance levels are maintained as per planned outcomes. All critical Type of audit shall be tested once a year and/or when changes are made and/or when new threats and vulnerabilities are reported which shall be applicable to the organization's **Website/Web Application**.

## 6. GLOSSARY

### Type of Assessment:

**Black Box Penetration Testing:** A penetration tester has no previous knowledge of the system to be tested. It is like blind testing as the pen testers find their own way into the system. This test checks if a threat actor can launch an attack with severely limited information. Mostly, the pen testers receive the name of the organization and URL. Test to be conducted for evaluating the security stance of the organization.

**Production URL:** The production environment is the live and operational version of an application, where the end-users are accessing/interacting with the application on a real-time basis.

**Testing/Staging URL:** The Testing /Staging URL is provided by the Auditee to the testing team with the purpose of conducting the security audit to identify the vulnerabilities with respect to the application's functionality. It is near replica of the production environment.

**NOTE:** In case the production URL is provided for security audit/testing, in this case the production URL shall be considered as Testing/Staging URL. Once the testing is completed and applicaton is "Safe to Host", the test data in the production URL may be removed and made live and operational to enable end-user access/interact on a real time basis

### 6.1. REFERENCE

1. OWASP WEB SECURITY TESTING GUIDE

[END OF REPORT]