VAPT/Security Testing Stage – I Report of Digital Pathology Web Application

Testing URL: https://117.221.20.181:8095/DigiPatho_Stage/

Submitted To:

HTG, CDAC Thiruvananthapuram

Submitted by
Information Security Services Team

Centre for Development of Advanced Computing (C-DAC),
Kolkata
Department of Electronics and Information Technology
Ministry of Communications & Information Technology, Government of India
Plot- E-2/1, Block-GP, Sector - V, Saltlake Electronics Complex,
Bidhannagar, Kolkata - 700 091 India

This is intentionally left blank

1. Document Control

Document Name	VAPT/Security Testing Stage - I Report of Digital Pathology Web Application
Document No:	**CDACK/ISS/VAPT/2025-26/WEB/DIGIPATHO/001**
Version	1.0
Document Date	19.12.2025
Prepared by	Mirza Alam Begg , C-DAC Kolkata
Reviewed by	Abhijit Chatterjee, C-DAC Kolkata
Doc. Classification	Confidential

Modification History

Sr. No	Description of Change & Remark	Date of Change	Version No.
1	Stage 1 Report – Initial Release	19.12.2025	1.0

Notice of Confidentiality

This document contains proprietary and confidential information of C-DAC Kolkata and HTG, CDAC Thiruvananthapuram. The recipient agrees to maintain this information in confidence and not reproduce or otherwise disclose this information to any person outside the group responsible for the evaluation of its contents.

Table of Contents

2. Background

Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) services, devices and networks. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

In India, the "National Cyber Security Policy" was thus proposed in 2013 with the goal to create safe and resilient cyberspace for citizens, businesses, and the Government and also to facilitate creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholder's actions for protection of cyber space. The mission is supposed to provide protection to cyberspace information and infrastructure, develop capabilities to prevent and respond to cyberattacks, and minimize damage through coordinated efforts of institutional structures, people, processes, and technology.

In this current context, HTG, CDAC Thiruvananthapuram. had empanelled C-DAC Kolkata as a service provider of Information Security related Services VA/PT related consultancy services. HTG, CDAC Thiruvananthapuram. has approached C-DAC Kolkata to conduct Web Application VA/PT on the Digital Pathology Web Application.

This document contains the detailed report on the Stage I VA/PT of Digital Pathology Web Application.

3. Vulnerability Classification & Severity Levels

In this comprehensive section, we meticulously evaluate the severity levels attributed to identified vulnerabilities within the assessment scope of the application. The primary objective is to provide a nuanced understanding of the potential risks that these vulnerabilities pose to the application and data.

Each vulnerability is systematically categorized into distinct severity levels, allowing for a clear and structured analysis of their impact on our security posture. To enhance accessibility and facilitate quick reference, each severity level is assigned a distinctive colour code. This color-coded system serves as an intuitive visual aid.

Accompanying the colour codes are succinct yet informative descriptions of the potential impact associated with each severity level. These descriptions offer a concise overview of the risks posed by vulnerabilities, aiding in the prioritization of remediation efforts.

Vulnerability Level	Description
Critical	Critical vulnerabilities pose an imminent and severe threat to the security of the application. The exploitation of these vulnerabilities carries the potential to inflict widespread and irreparable damage, impacting business continuity.
High	High vulnerabilities pose a significant security risk to our system, they can lead to serious consequences if exploited. Swift remediation is essential to prevent potential breaches and safeguard sensitive information from unauthorized access or compromise.
Medium	Medium-severity vulnerabilities present a moderate level of risk to our system. While not as urgent as critical or high-severity issues, these vulnerabilities should be addressed promptly to prevent them from escalating into more significant threats.
Low	Low-severity vulnerabilities represent a relatively low risk to our system. While they may not pose an immediate threat, addressing these vulnerabilities during routine security updates and maintenance is advised to uphold a strong security posture.
Informational	Informational vulnerabilities provide insights into potential improvements or best practices without posing a direct threat to our system's security. While not urgent, addressing these findings contributes to overall security enhancement.

4. Scope Details

The testing scope encompasses specific components and functionalities within the web application, including but not limited to login systems, user roles (such as Admin and other user), data processing modules, and APIs. A comprehensive evaluation will be conducted to ensure the thorough assessment of identified elements, with particular attention to the functionalities associated with the 'Admin' role and other 'User' roles within the system.

In Scope URL's List:

https://117.221.20.181:8095/_graphql
https://117.221.20.181:8095/_graphql/GetSuggestedNavigationDestinations
https://117.221.20.181:8095/case-studies
https://117.221.20.181:8095/collections
https://117.221.20.181:8095/DigiPatho_Stage/
https://117.221.20.181:8095/DigiPatho_Stage/Rest
https://117.221.20.181:8095/DigiPatho_Stage/Rest/dashboardservice
https://117.221.20.181:8095/DigiPatho_Stage/Rest/dashboardservice/getcountdash
https://117.221.20.181:8095/DigiPatho_Stage/Rest/dashboardservice/getEMRPatientListdctc
https://117.221.20.181:8095/DigiPatho_Stage/Rest/dashboardservice/getinitialdefaultmenu
https://117.221.20.181:8095/DigiPatho_Stage/Rest/dashboardservice/getinitialsubmenu
https://117.221.20.181:8095/DigiPatho_Stage/Rest/dashboardservice/getInstitutionType
https://117.221.20.181:8095/DigiPatho_Stage/Rest/imageviewerservice
https://117.221.20.181:8095/DigiPatho_Stage/Rest/imageviewerservice/fwdtotask
https://117.221.20.181:8095/DigiPatho_Stage/Rest/imageviewerservice/loadtechnicianlist
https://117.221.20.181:8095/DigiPatho_Stage/Rest/imageviewerservice/readaiannotationlist
https://117.221.20.181:8095/DigiPatho_Stage/Rest/insmanagementservice
https://117.221.20.181:8095/DigiPatho_Stage/Rest/insmanagementservice/getAllRegScreeningcamps
https://117.221.20.181:8095/DigiPatho_Stage/Rest/insmanagementservice/getAllRegScreeningHubs
https://117.221.20.181:8095/DigiPatho_Stage/Rest/insmanagementservice/gethospitalslist
https://117.221.20.181:8095/DigiPatho_Stage/Rest/insmanagementservice/readdistrictstbyState
https://117.221.20.181:8095/DigiPatho_Stage/Rest/insmanagementservice/registerhospital
https://117.221.20.181:8095/DigiPatho_Stage/Rest/loginservice
https://117.221.20.181:8095/DigiPatho_Stage/Rest/loginservice/getinitialconfig
https://117.221.20.181:8095/DigiPatho_Stage/Rest/loginservice/getsnomedurl
https://117.221.20.181:8095/DigiPatho_Stage/Rest/loginservice/loginaction
https://117.221.20.181:8095/DigiPatho_Stage/Rest/loginservice/logout
https://117.221.20.181:8095/DigiPatho_Stage/Rest/loginservice/mainpage
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/chkdup_save_update_delete
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/getMenuListByAppid
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/getTableDataByOneCondition
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/getTableMasters
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/getTableMasters_all
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/readMasDataBasedOnDynQuery
https://117.221.20.181:8095/DigiPatho_Stage/Rest/masterservice/setMenuSave_delete
https://117.221.20.181:8095/DigiPatho_Stage/Rest/patientreg
https://117.221.20.181:8095/DigiPatho_Stage/Rest/patientreg/getpatientprofile
https://117.221.20.181:8095/DigiPatho_Stage/Rest/slideregcerviScanService
https://117.221.20.181:8095/DigiPatho_Stage/Rest/slideregcerviScanService/getSlideDetailsbyID

https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice
https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice/getTableRoles_all
https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice/readdistrictstbyState
https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice/readSearchUserlist
https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice/readuserlist
https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice/registeruser_global
https://117.221.20.181:8095/DigiPatho_Stage/Rest/usermanagementservice/resetForgotpwd
https://117.221.20.181:8095/DigiPatho_Stage/scripts
https://117.221.20.181:8095/DigiPatho_Stage/scripts/assets
https://117.221.20.181:8095/DigiPatho_Stage/scripts/assets/css
https://117.221.20.181:8095/DigiPatho_Stage/scripts/assets/pages
https://117.221.20.181:8095/DigiPatho_Stage/scripts/assets/pages/menu-search
https://117.221.20.181:8095/DigiPatho_Stage/scripts/assets/pages/social-timeline
https://117.221.20.181:8095/DigiPatho_Stage/scripts/bower_components
https://117.221.20.181:8095/DigiPatho_Stage/scripts/bower_components/bootstrap
https://117.221.20.181:8095/DigiPatho_Stage/views
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/dashb
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/dashb/DasboardPHC.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/img
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/img/imageview.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/mas
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/mas/GeneralMasterMgmt.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/mas/InstitutionSetup.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/mas/ResetPassword.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/profile
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/profile/user-profile.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/SessionTimeoutRedirect.html
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/slideReg
https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/slideReg/SlideView.html
https://117.221.20.181:8095/enterprise
https://117.221.20.181:8095/events
https://117.221.20.181:8095/explore
https://117.221.20.181:8095/features
https://117.221.20.181:8095/features/actions
https://117.221.20.181:8095/features/code-review
https://117.221.20.181:8095/features/code-review/
https://117.221.20.181:8095/features/integrations
https://117.221.20.181:8095/features/project-management
https://117.221.20.181:8095/features/project-management/
https://117.221.20.181:8095/jaspermdegroot
https://117.221.20.181:8095/join
https://117.221.20.181:8095/joliss
https://117.221.20.181:8095/jquery
https://117.221.20.181:8095/jquery/jquery-ui
https://117.221.20.181:8095/jquery/jquery-ui/blob/master
https://117.221.20.181:8095/jquery/jquery-ui/commit
https://117.221.20.181:8095/jquery/jquery-ui/commits
https://117.221.20.181:8095/jquery/jquery-ui/commits/master
https://117.221.20.181:8095/jquery/jquery-ui/delete/master

https://117.221.20.181:8095/jquery/jquery-ui/delete/master/themes
https://117.221.20.181:8095/jquery/jquery-ui/delete/master/themes/base
https://117.221.20.181:8095/jquery/jquery-ui/delete/master/themes/base/images
https://117.221.20.181:8095/jquery/jquery-ui/find
https://117.221.20.181:8095/jquery/jquery-ui/find/master
https://117.221.20.181:8095/jquery/jquery-ui/network
https://117.221.20.181:8095/jquery/jquery-ui/network/members
https://117.221.20.181:8095/jquery/jquery-ui/projects
https://117.221.20.181:8095/jquery/jquery-ui/pulls
https://117.221.20.181:8095/jquery/jquery-ui/pulse
https://117.221.20.181:8095/jquery/jquery-ui/raw
https://117.221.20.181:8095/jquery/jquery-ui/raw/master
https://117.221.20.181:8095/jquery/jquery-ui/ref-list
https://117.221.20.181:8095/jquery/jquery-ui/ref-list/master
https://117.221.20.181:8095/jquery/jquery-ui/ref-list/master/themes
https://117.221.20.181:8095/jquery/jquery-ui/ref-list/master/themes/base
https://117.221.20.181:8095/jquery/jquery-ui/ref-list/master/themes/base/images
https://117.221.20.181:8095/jquery/jquery-ui/search
https://117.221.20.181:8095/jquery/jquery-ui/stargazers
https://117.221.20.181:8095/jquery/jquery-ui/watchers
https://117.221.20.181:8095/marketplace
https://117.221.20.181:8095/nonprofit
https://117.221.20.181:8095/orgs
https://117.221.20.181:8095/orgs/jquery
https://117.221.20.181:8095/orgs/jquery/hovercard
https://117.221.20.181:8095/peritpatrio
https://117.221.20.181:8095/PeterDaveHello
https://117.221.20.181:8095/pricing
https://117.221.20.181:8095/robots.txt
https://117.221.20.181:8095/scottgonzalez
https://117.221.20.181:8095/search
https://117.221.20.181:8095/security
https://117.221.20.181:8095/site
https://117.221.20.181:8095/site/dismiss_signup_prompt
https://117.221.20.181:8095/topics
https://117.221.20.181:8095/trending

5. Client Details

Name and Address of Client	:	HTG(Health Technology Group), CDAC Thiruvananthapuram CDAC Thiruvananthapuram, Vellayambalam, Thiruvananthapuram - 695033, Kerala, India
Contact information for the designated Single Point of Contact	:	Aswathy M G Mobile : 7025991130 Email : aswathy.mg@cdac.in

6. Brief:

6.1 Summary

URL of the Web Application	:	https://117.221.20.181:8095/DigiPatho_Stage/
Operating System	:	Microsoft Windows Server
Web Application Framework	:	Apache Tomcat, Node.js
Port Scanned	:	80, 443

6.2 Testing Summary

Type of Testing	:	Grey Box Testing
Testing Start Date	:	08.12.2025
Testing End Date	:	17.12.2025

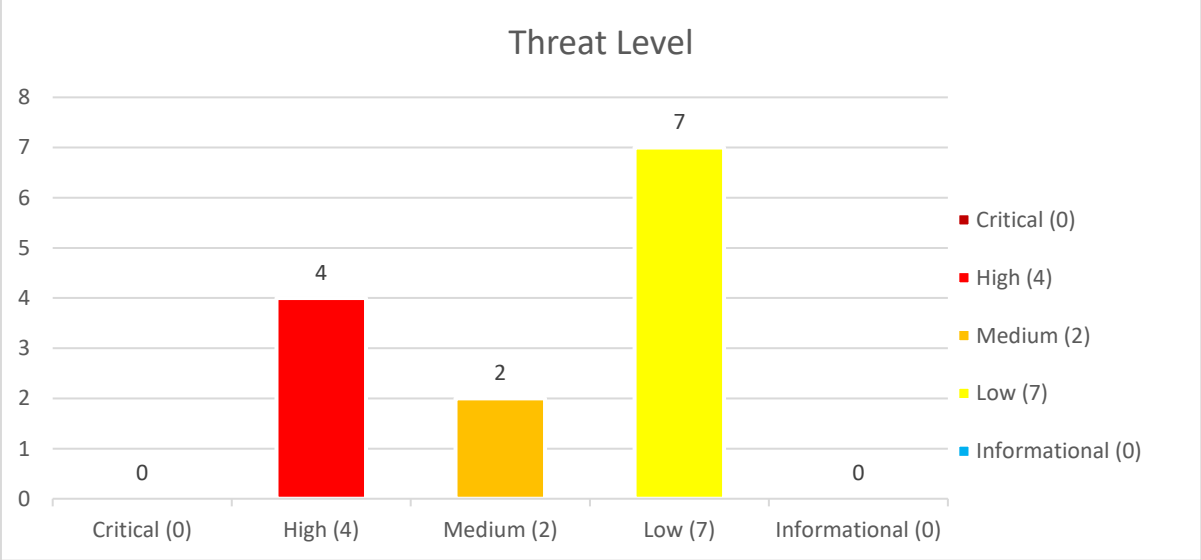
6.3 Risk Level

HIGH

One or more High severe vulnerabilities are discovered in the website and thus the overall threat level is rated as High.

6.4 Threat Summary

Total Threats Found : 13



7. Executive Summary

This report presents the results of the "Grey Box" penetration testing for Digital Pathology Web Application. The recommendations provided in this report structured to facilitate remediation of the identified security risks. This document serves as a formal letter of attestation for the recent Grey Box Penetration Testing of Digital Pathology Web Application.

Evaluation ratings compare information gathered during the course of the engagement to "best in class" criteria for security standards. We believe that the statements made in this document provide an accurate assessment of CDAC Thiruvananthapuram's current security as it relates to Web Application perimeter.

7.1 Assumptions & Constraints

As the environment changes, and new vulnerabilities and risks are discovered and made public, an organization's overall security posture will change. Such changes may affect the validity of this letter. Therefore, the conclusion reached from our analysis only represents a "snapshot" in time.

Consultants performed discovery process to gather information about the target and searched for information disclosure vulnerabilities. With this data in hand, we conducted the bulk of the testing manually, which consisted of input validation tests, impersonation (authentication and authorization) tests, and session state management tests. The purpose of this penetration testing is to illuminate security risks by leveraging weaknesses within the environment that lead to the obtainment of unauthorized access and/or the retrieval of sensitive information. The shortcomings identified during the assessment were used to formulate recommendations and mitigation strategies for improving the overall security posture

7.2 Results Overview

The test uncovered vulnerabilities that may cause sensitive data leakage, broken confidentiality and integrity and availability of the resource. Identified vulnerabilities are easily exploitable and the risk posed by these vulnerabilities can cause damage to the application and company.

Overall Threat Level	**HIGH**

Risk Level	Vulnerability Discovered at	Name of the Vulnerability
HIGH	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html	Session Hijacking
	https://117.221.20.181:8095/DigiPatho_Stage/	Password Sent in Clear Text
	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html	Improper Input Validation
	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Stored Cross Site Scripting (Stored XSS)
MEDIUM	https://117.221.20.181:8095/DigiPatho_Stage/	Clickjacking

	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Insufficient Transport Layer Protection
LOW	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Input Field with Autocomplete Enabled
	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Missing Security Headers
	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Cookie Without Secure Flag Set
	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Cookie Without HTTP Only Flag Set
	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#	Same-Site Cookie Not Implemented
	https://117.221.20.181:8095/DigiPatho_Stage/	Outdated Components
	https://117.221.20.181:8095	Server Default page

7.3 Summary of business risks

Found Vulnerabilities/severity issues can lead to:

- Exposure of session identifiers may allow attackers to hijack active sessions, resulting in unauthorized access and account compromise.
- Transmission of credentials without encryption makes user passwords susceptible to interception, leading to unauthorized account access.
- Insufficient validation of user input may enable injection attacks, allowing attackers to manipulate application behavior or data.
- Persistent malicious scripts can execute in users' browsers, potentially leading to credential theft, session hijacking, or unauthorized actions.
- Lack of frame protection may allow attackers to trick users into performing unintended actions through deceptive user interface overlays.
- Weak or misconfigured encryption may expose sensitive data to man-in-the-middle attacks and unauthorized interception.
- Browser-stored sensitive information may be exposed on shared or compromised systems, increasing the risk of information disclosure.
- Absence of recommended HTTP security headers may expose the application to XSS, clickjacking, MIME-type sniffing, and data leakage attacks.
- Use of obsolete libraries or frameworks increases susceptibility to known vulnerabilities and publicly available exploits.
- Presence of default server pages may disclose system information and indicate insufficient production hardening.

7.4 Project limitations

The Grey Box assessment was conducted against production environment with all limitations, it provides.

8. Vulnerabilities in detail

1. Session Hijacking — HIGH

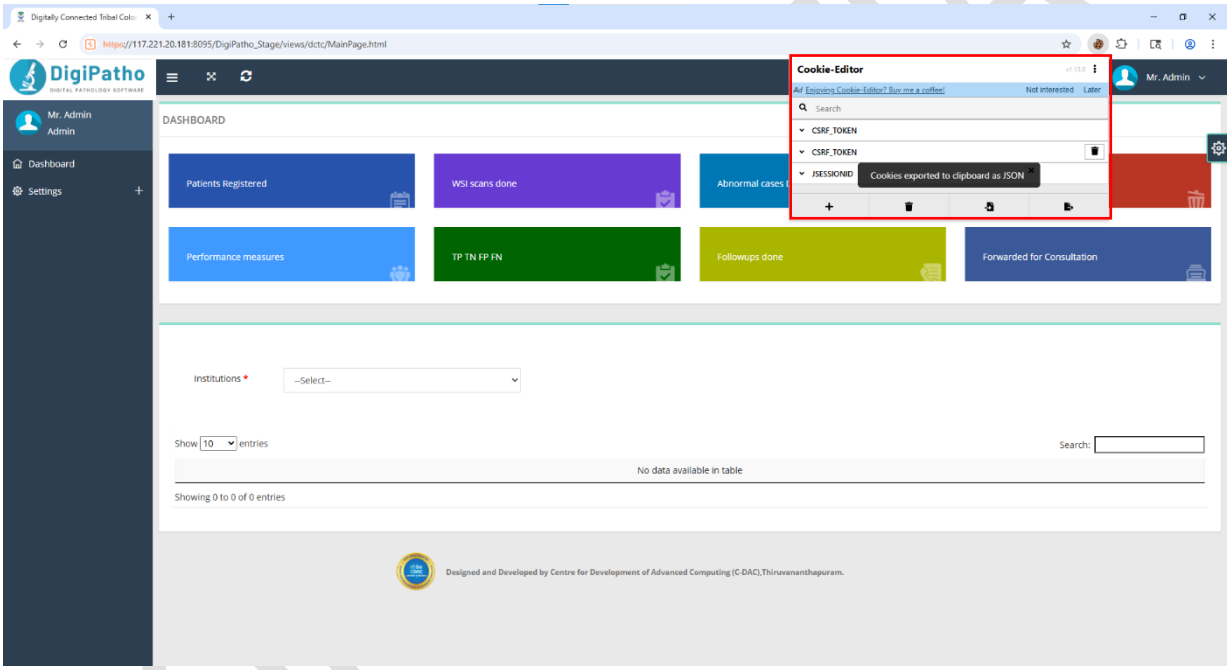
Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html
CWE : CWE-1353
OWASP : Identification and Authentication Failures

1.1 Description

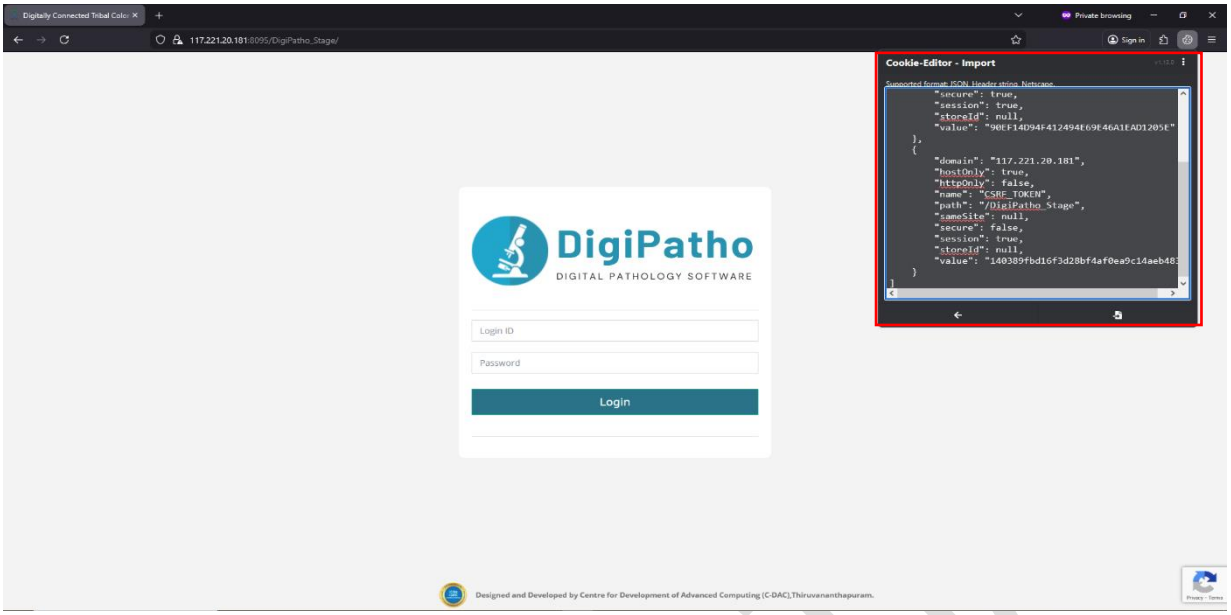
Session hijacking refers to the malicious act of taking control of a user's web session. A session, in the context of web browsing, is a series of interactions between two communication endpoints, sharing a unique session token to ensure continuity and security.

1.2 Proof of Concept

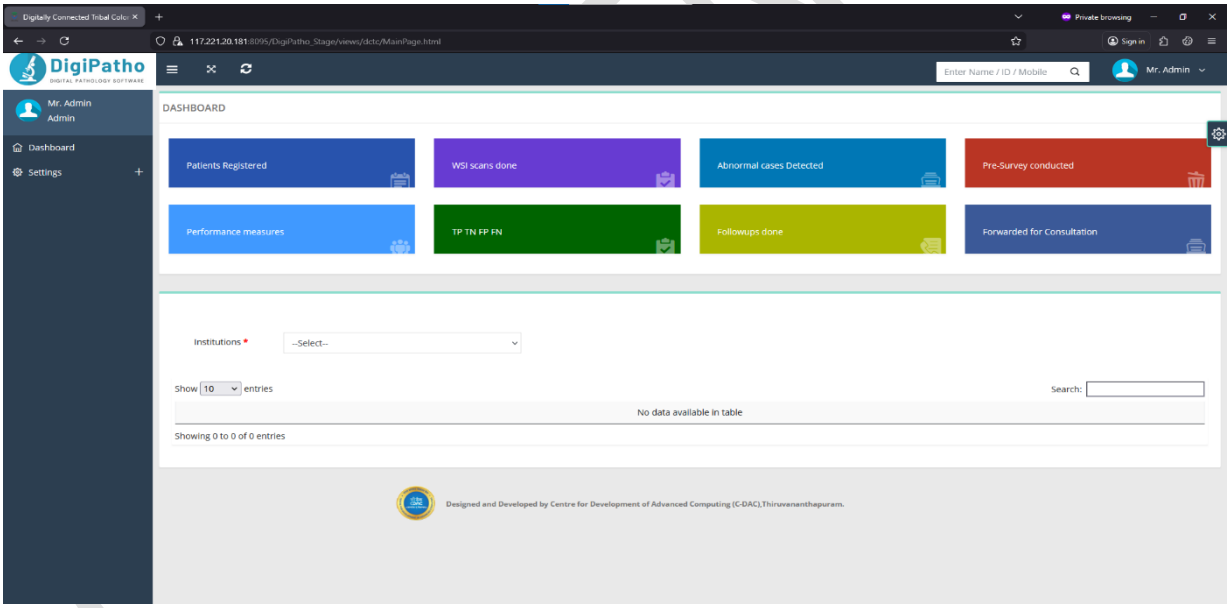
1.2.1 Step 1 In the first step normally logged in as "admin" user and exported the cookie value.



1.2.2 Step 2 In the next step, imported the captured cookie into the incognito window of the same browser.



After successfully import the cookie in the incognito window, it is clearly seen that the user has logged in successfully without entering the credentials.



1.3 Workaround/Solutions

To mitigating Session Hijacking Vulnerability Implement

- Use strong passwords and multifactor authentication.
- Keep software up to date.
- Install web session cookie management frameworks.
- Always rotate session keys after authentication.

TOP

2. Password Sent in Clear Text HIGH

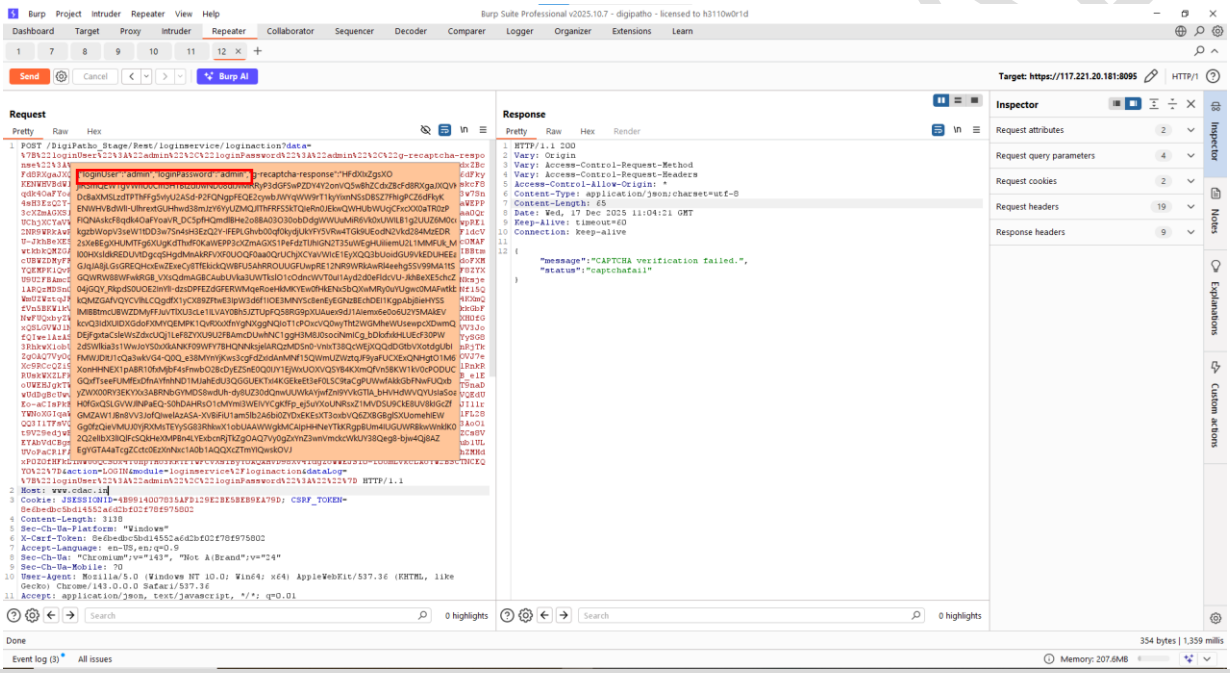
Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/
CWE : CWE-319
OWASP : Sensitive Information Sent via Unencrypted Chanel

2.1 Description

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic.

2.2 Proof of Concept

2.2.1 Step 1 Intercept login request to the server.



2.3 Workaround/Solutions

To address Password Sent in Clear Text Vulnerability, it's essential for applications to employ transport-level encryption like SSL or TLS. This ensures that all sensitive communications between the client and server are securely protected. Additionally, sensitive information such as passwords should be encrypted before transmission to further enhance security measures.

TOP

3. Improper Input Validation HIGH

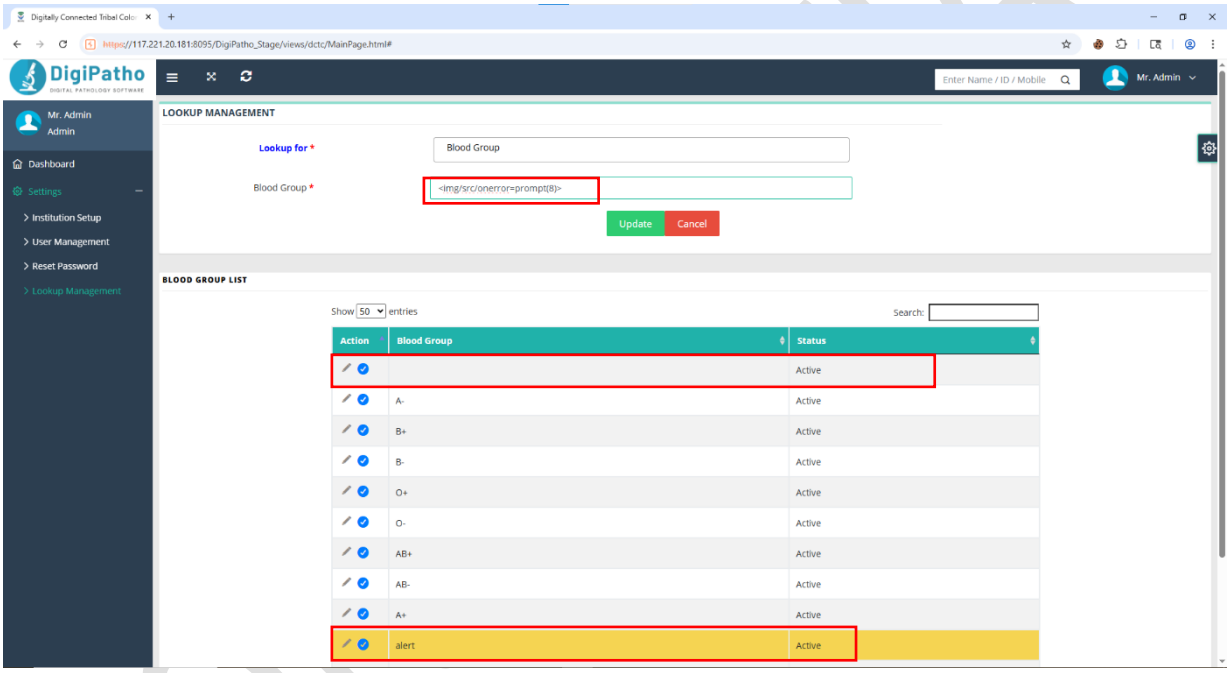
Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html
CWE : CWE-20
OWASP : Improper Data Validation

3.1 Description

Improper input validation vulnerability occurs when a software application fails to adequately validate and sanitize user inputs, allowing malicious actors to inject malicious data. Inadequate input validation opens the door for attackers to exploit vulnerabilities, potentially compromising the integrity, confidentiality, and availability of the system.

3.2 Proof of Concept

3.2.1 Step 1 In the Lookup Management section, in the "Blood Group" input box added a malicious JavaScript code.



3.2.2 Step 2 On submitting, the message gets saved without any validation.

3.3 Workaround/Solutions

To address the improper input validation vulnerability, a comprehensive solution involves implementing both server-side and client-side validation mechanisms.
On the server side, robust input validation should be enforced through thorough scrutiny of user inputs, using methods such as input validation libraries and ensuring adherence to predefined data formats.
Additionally, server-side security controls, like parameterized queries and proper encoding, should be implemented to prevent common exploits such as SQL injection.

TOP

4. Stored Cross Site Scripting (Stored XSS) HIGH

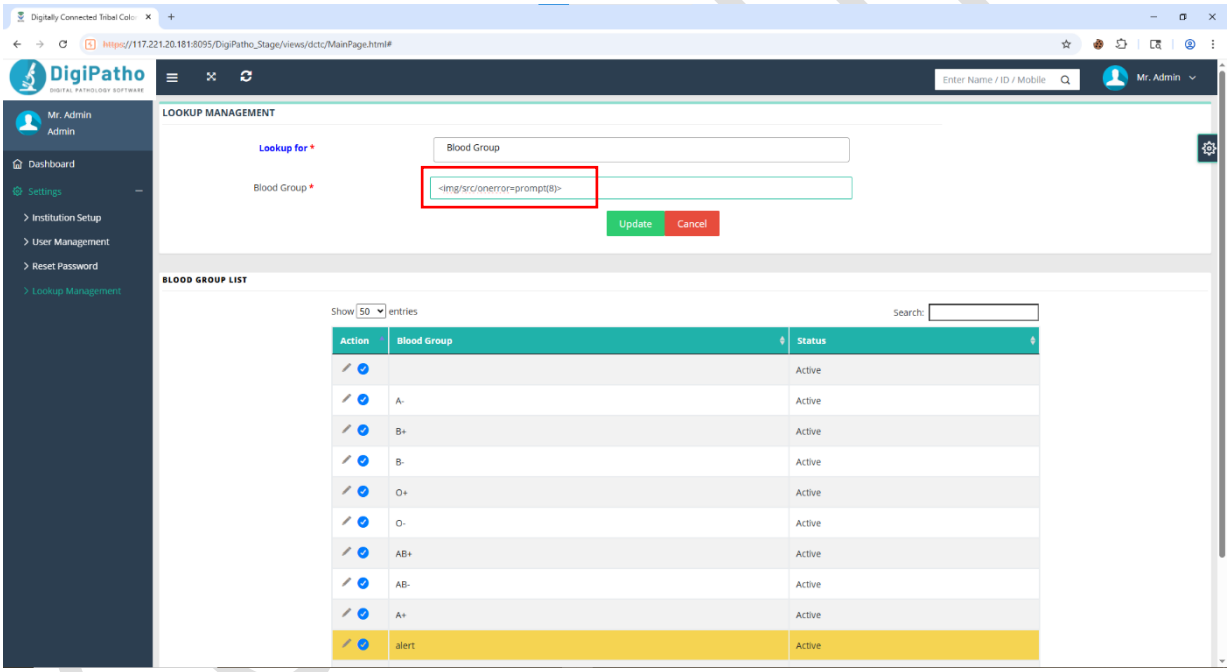
Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#
CWE : CWE-79
OWASP : Cross Site Scripting (XSS)

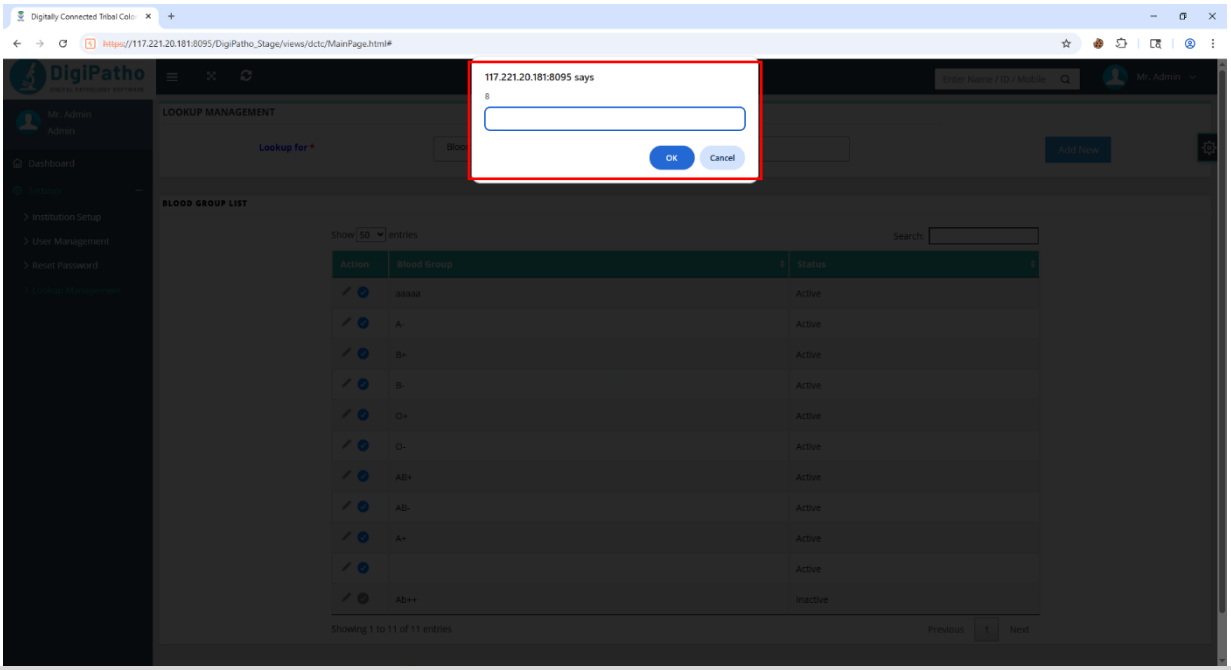
4.1 Description

Stored cross-site scripting vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes.

4.2 Proof of Concept

4.2.1 Step 1 Visit 'https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#', on this page in the Blood Group input field added the XSS payload and observed that the payload is saved.





4.3 Workaround/Solutions

Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression.
Input which fails the validation should be rejected, not sanitized.
User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

TOP

5. Action Spoofing (Clickjacking) MEDIUM

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/
CWE : CAPEC-103, CWE-1021
OWASP : Clickjacking

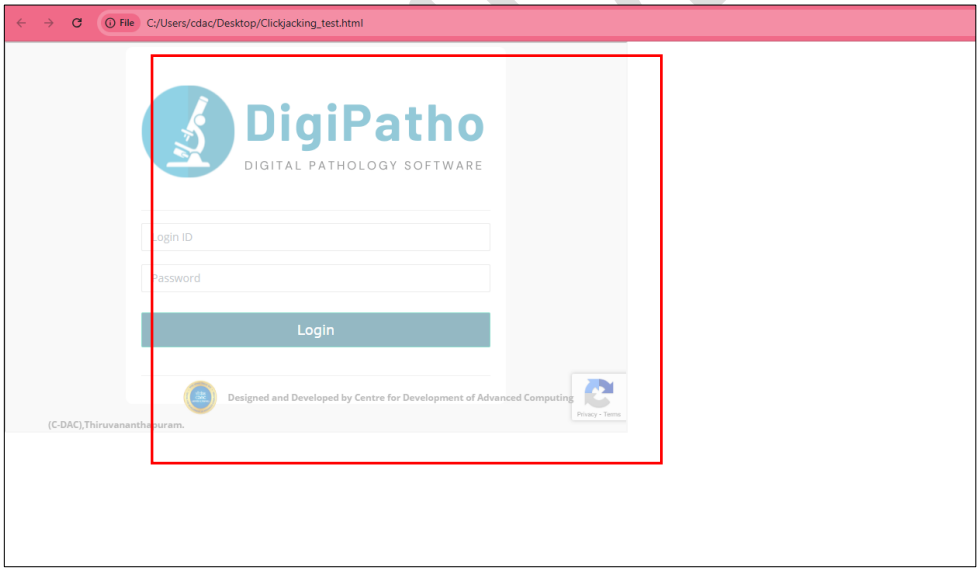
5.1 Description

The web application server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN, for that reason the webpage can be rendered anywhere by using this malicious actor can tricking user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

5.2 Proof of Concept

5.2.1 Step 1 It is observed that the webpage is being rendered from a different domain from this code fragment.

```
<html>
    <style>
        iframe {
        width: 800px;
        height: 500px;
        position: absolute;
        top: 0; left: 0;
        filter: alpha(opacity=50);
        opacity: 0.5;
        }
    </style>
    <iframe src="https://117.221.20.181:8095/DigiPatho_Stage/">
</html>
```



5.3 Workaround/Solutions

Configure backend server to include an X-Frame-Options header and a CSP header with frame-ancestors directive.

TOP

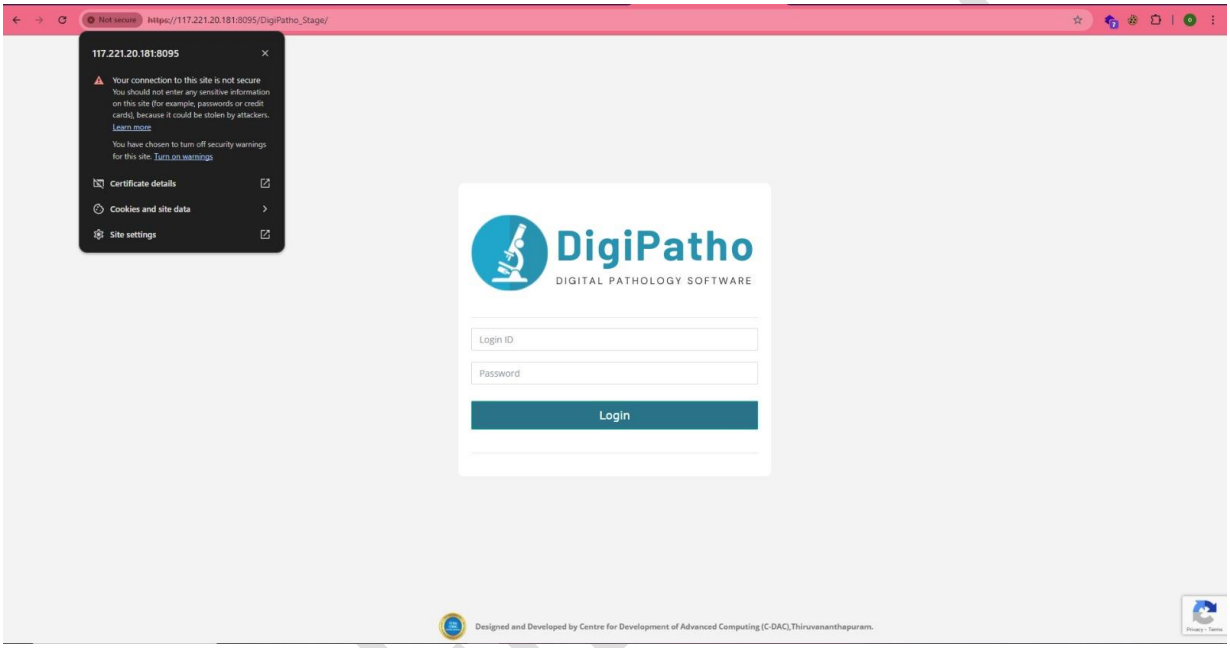
6. Insufficient Transport Layer Protection MEDIUM

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html
CWE : CWE-818
OWASP : Insufficient Transport Layer Protection

6.1 Description

The web application doesn't use SSL/TLS (HTTP) for secure communication channel.

6.2 Proof of Concept



6.3 Workaround/Solutions

Production servers should use **TLS 1.3** (preferred) or **TLS 1.2** and a valid SSL/TLS certificate to ensure a secure communication channel.

TOP

7. Input Field with Autocomplete Enabled LOW

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html
CWE : CWE-451, CWE-1021
OWASP : Insufficient Anti-automation

7.1 Description

Enabling autocomplete in an input field can introduce a security vulnerability known as "autocomplete abuse." This occurs when sensitive information, such as usernames or passwords, is stored by the browser and then unintentionally revealed through autocomplete suggestions. Attackers can exploit this by tricking users into revealing sensitive data or by leveraging browser extensions to extract information.

7.2 Proof of Concept

7.2.1 Step 1 Auto completing username in login page.

7.3 Workaround/Solutions

The `autocomplete` value can be configured in two different locations.
The first and most secure location is to disable the `autocomplete` attribute on the `<form>` HTML tag. This will disable `autocomplete` for all inputs within that form. An example of disabling `autocomplete` within the form tag is `<form autocomplete=off>`.
The second slightly less desirable option is to disable the `autocomplete` attribute for a specific `<input>` HTML tag. While this may be the less desired solution from a security perspective, it may be preferred method for usability reasons, depending on size of the form. Implement this in all the user input section throughout the application.

TOP

8. Missing Security Headers LOW

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#
CWE : CWE-693
OWASP : Improper Neutralization of HTTP Headers

8.1 Description

The web application doesn't use most of the Security Headers recommended by OWASP Secure Headers Project (OSHP).

8.2 Workaround/Solutions

Use these Security Headers with the recommended values and also use Content Security Policy (CSP):

Security Header	Recommended Value
X-Frame-Options	DENY
X-XSS-Protection	1
X-Content-Type-Options	nosniff
Referrer-Policy	strict-origin-when-cross-origin
Content-Type	text/html; charset=UTF-8
Strict-Transport-Security	max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Origin	https:// 117.221.20.181:8095
HTTP Cross-Origin-Opener-Policy	same-origin
Cross-Origin-Embedder-Policy	require-corp
Cross-Origin-Resource-Policy	same-site
X-DNS-Prefetch-Control	off

N.B: And also remove 'Server' and 'X-Powered-By' headers from responses.

TOP

9. Cookie without Secure Flag set LOW

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#
CWE : CWE-614

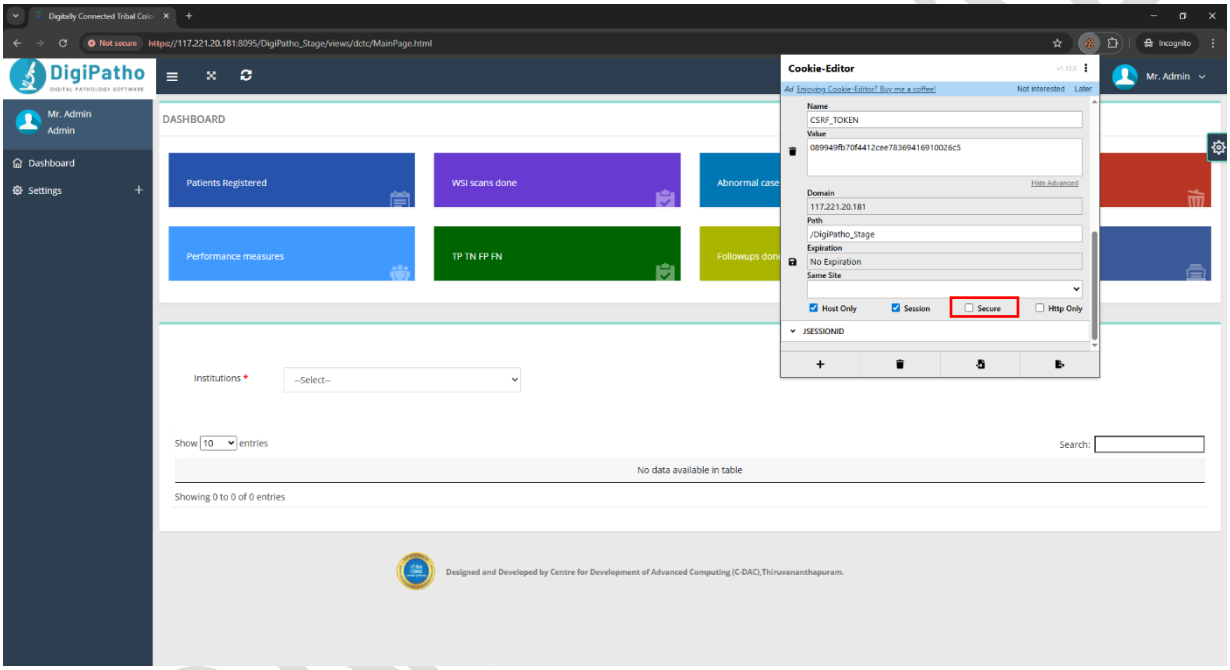
9.1 Description

In the web application cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

9.2 Proof of Concept

9.2.1 Step 1

Secure Cookie Flag not set in the application.



9.3 Workaround/Solutions

Update the code to include the Secure flag when setting cookies. This can typically be achieved by adding the "Secure" attribute to the cookie when it is being created or modified.

TOP

10. Cookie without HttpOnly Flag set LOW

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#
CWE : CWE-614, CWE-1004

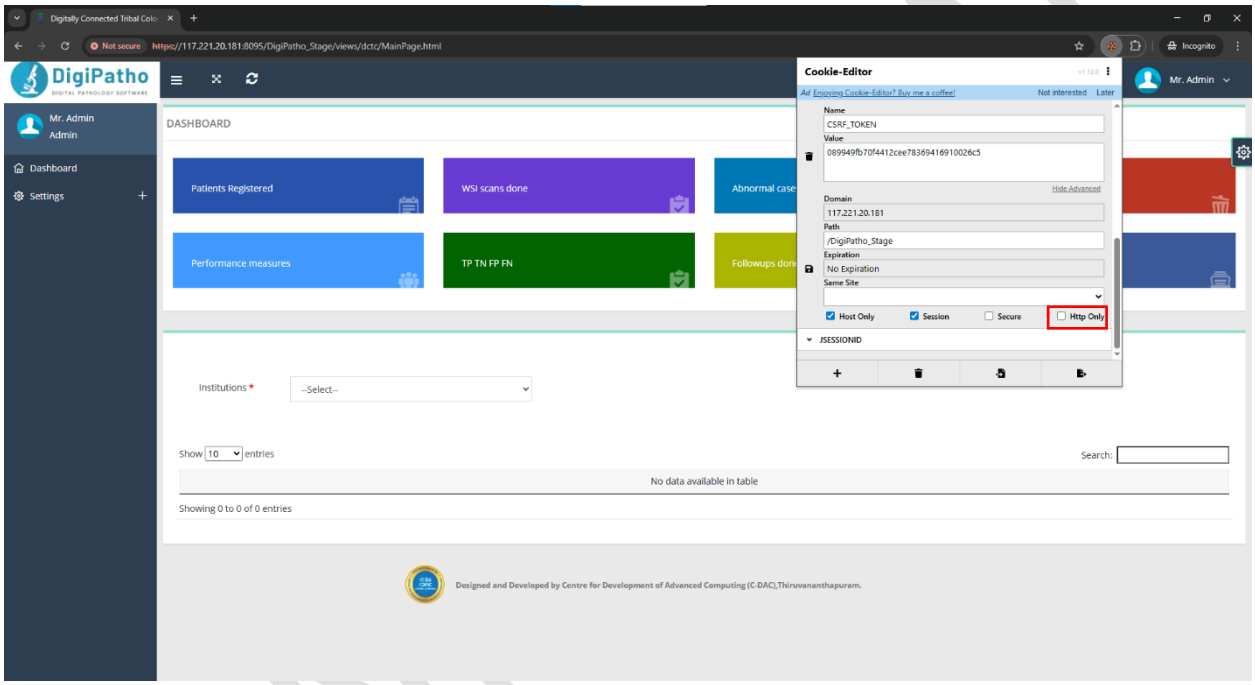
10.1 Description

The Secure attribute for sensitive cookies in HTTP sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.

10.2 Proof of Concept

10.2.1 Step 1

HTTP Only Flag not set in the application.



10.3 Workaround/Solutions

Update the code to include the Secure flag when setting cookies. This can typically be achieved by adding the "HTTP Only" attribute to the cookie when it is being created or modified.

TOP

11. Same-Site Cookie not implemented LOW

Affected URL	:	https://117.221.20.181:8095/DigiPatho_Stage/views/dctc/MainPage.html#
CWE	:	CWE-1275
OWASP	:	SameSite Cookie

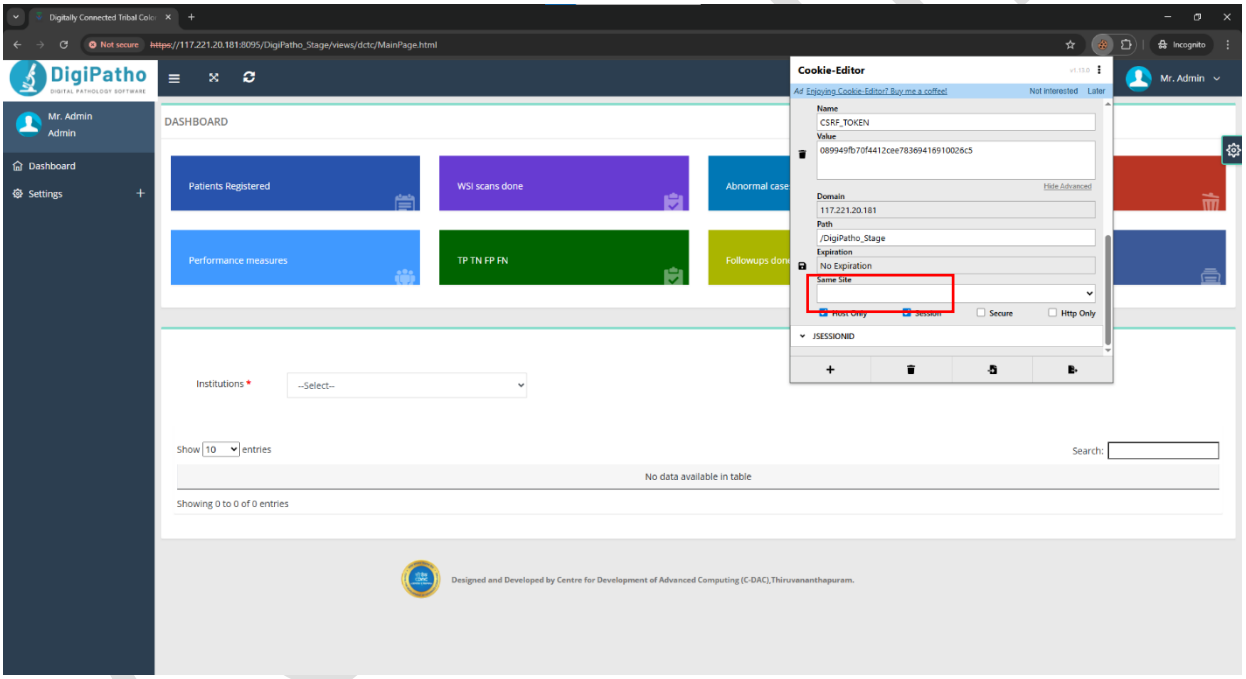
11.1 Description

The SameSite attribute controls how cookies are sent for cross-domain requests. This attribute may have three values: 'Lax', 'Strict', or 'None'. If the 'None' value is used, a website may create a cross-domain POST HTTP request to another website, and the browser automatically adds cookies to this request. This may lead to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).

11.2 Proof of Concept

11.2.1 Step 1

Same Site Cookie attribute not defined in the application.



11.3 Workaround/Solutions

Set the SameSite attribute of a sensitive cookie to 'Lax' or 'Strict'. This instructs the browser to apply this cookie only to same-domain requests, which provides a good defence in depth against CSRF attacks.

TOP

12. Outdated Components LOW

Affected URL : https://117.221.20.181:8095/DigiPatho_Stage/
CWE : CWE-1352
OWASP : Vulnerable and Outdated Components (A06:2021)

12.1 Description

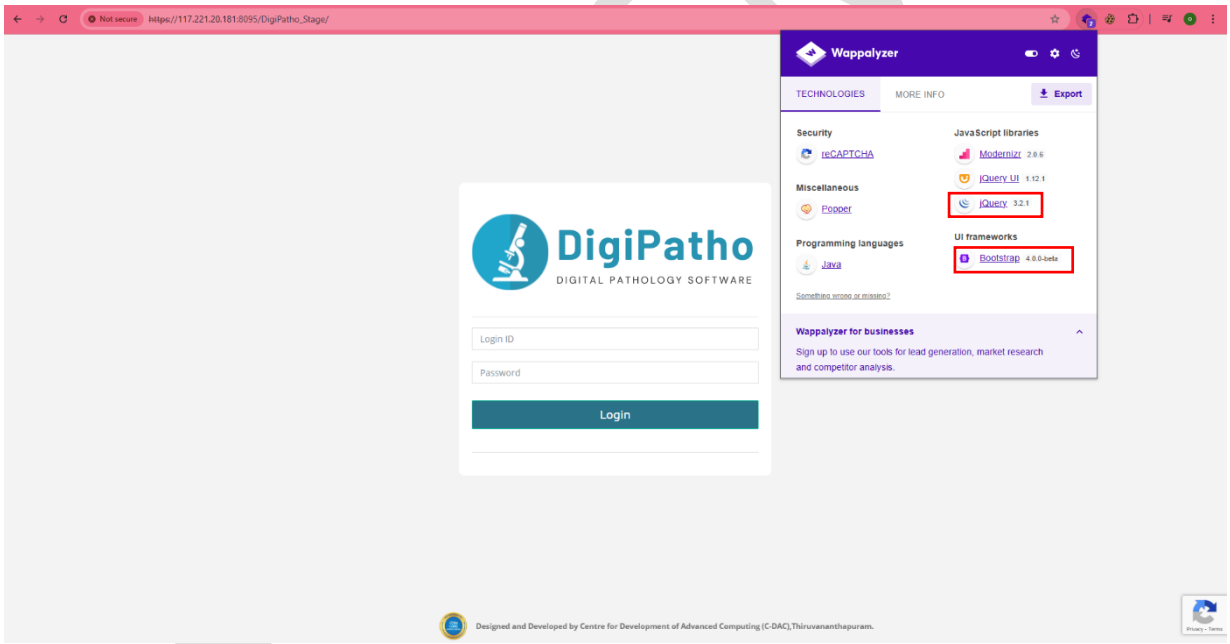
Vulnerabilities arising from the use of vulnerable and outdated components pose a significant cybersecurity risk. These components, which may include software libraries, frameworks, or third-party modules, can have known security flaws that threat actors exploit to gain unauthorized access, compromise data, or launch attacks.

12.2 Proof of Concept

12.2.1 Step 1

The web application is using the following components which are outdated and are susceptible to well-known vulnerabilities.

Name of the component	Version used in the web application	Latest Stable Version
jQuery	3.2.1	3.7.1
Bootstrap	4.0	5.3



12.3 Workaround/Solutions

Ensure that you regularly update and utilize frameworks or third-party libraries that undergo active monitoring and updates, exclusively opting for the latest versions or those free from known vulnerabilities.

TOP

13. Server Default Page LOW

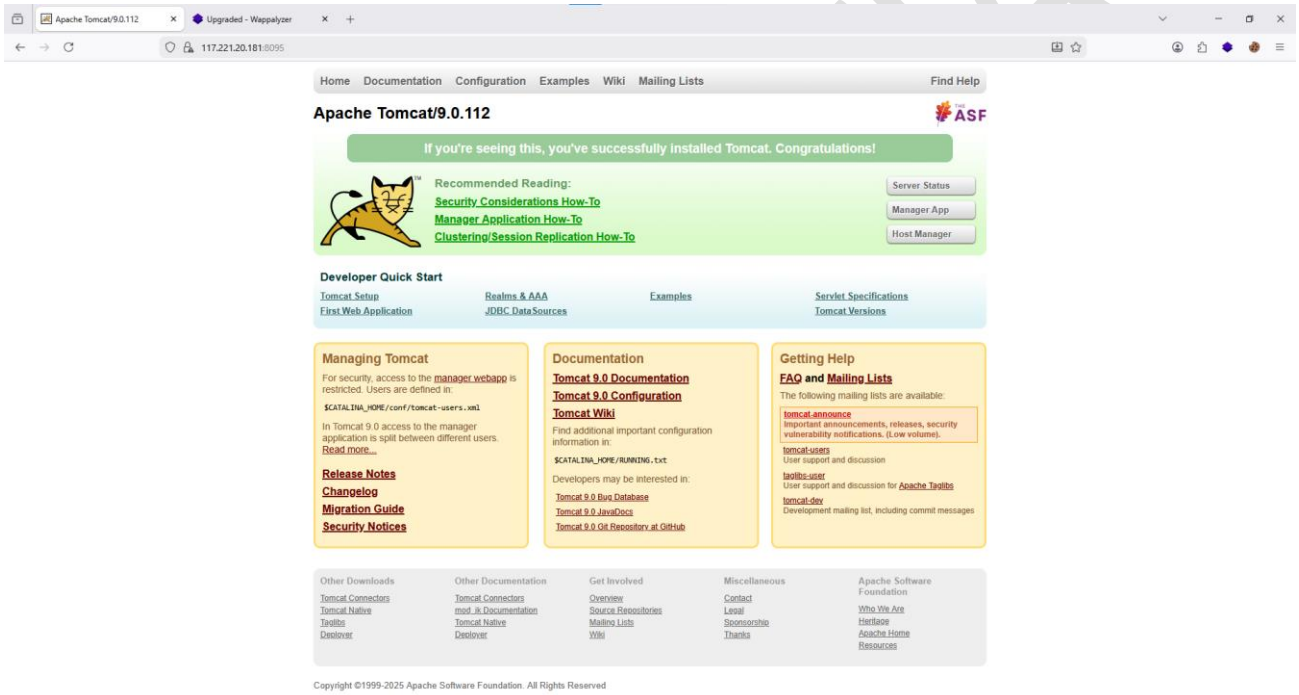
Affected URL : https:// 117.221.20.181:8095
CWE : CWE-200
OWASP : Security Misconfiguration

13.1 Description

It was observed that the web server is hosting and exposing a default server page. Default pages may disclose information about the underlying server technology, software version, or configuration details. Such information can assist an attacker in reconnaissance and may be leveraged to identify potential vulnerabilities specific to the server environment.

13.2 Proof of Concept

13.2.1 Step 1 It observe that the server responds with a **default welcome or test page**, indicating that the default configuration has not been removed or replaced.



13.3 Workaround/Solutions

- Remove or disable the default server page from the web root directory.
- Replace the default page with a custom application-specific landing page.
- Ensure unnecessary files, sample pages, and test configurations are removed from the production server.
- Perform a configuration review to minimize information disclosure.

TOP

****** End of Report ******