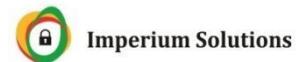


Report Release Date	17 th May 2025
Type of Audit	Web Application Audit
Type of Audit Report	First Audit Report
Period	14 th May 2025– 17 th May 2025

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

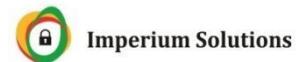


Document Preparation	
Document Title	Web Application Audit Report
Document ID	Qwegle Technologies
Document Version	1.0
Prepared by	Mr. Sanjeev Chavan
Reviewed by	Ms. Tasneam P
Approved by	Ms. Tasneam P
Released by	Ms. Tasneam P
Release date	17 th May 2025

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Document Control

Document Distribution List			
Name	Organization	Designation	Email Id
Ms. Tasneam P	Imperium Solution	Head - Information Security and Data Privacy	tasneam@imperiumpolution.com
Document Change History			
Version	Date	Remarks / Reason of change	
1.0	17 th May 2025	No Change	

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

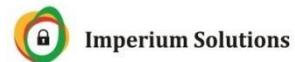


Table of Contents

DOCUMENT CONTROL	3
COMPANY PROFILE	5
IMPERIUM SOLUTIONS PROFILE	5
TARGETED AUDIENCE	5
AUDIT OBJECTIVE	5
AUDIT SCOPE	6
ENGAGEMENT SCOPE	7
DETAILS OF THE AUDITING TEAM	7
METHODOLOGY	9
AUDIT CONDUCTED	11
TOOLS/ SOFTWARE USED	11
RISK SUMMARY	12
MANAGEMENT SUMMARY	15
VULNERABILITY DETAILS	39

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Company Profile

Imperium Solutions Profile

Imperium Solutions is a Cert-IN empanelled, ISO 9001 and ISO27001 certified organization, focused on Information Security and Data Privacy domains. Established in June 2008, we aim to partner with our clients to build and implement appropriate Information Security and Data Privacy Controls. Imperium Solutions professionals have rich domain expertise across a cross section of industry verticals and the multi-dimensional skills to meet the ever-changing business needs of our clients.

Imperium Solution's unique blend of customer focus and consistency in delivering services of the highest quality provides a competitive edge to our clients.

Our portfolios of solutions help our clients achieve their business objectives while maintaining the security and privacy of their data.

Targeted Audience

Citing the identified risks and vulnerabilities as mentioned in the report, it should be considered as Strictly Confidential and accessible only to the Top Management, IT Manager, Software Development Team, Software Testing Team and senior staff members responsible for taking action.

Audit Objective

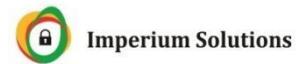
The objective of this vulnerability assessment and penetration testing exercise is to

1. Identify the vulnerabilities existing in the application module within the scope of the vulnerability assessment and penetration testing exercise.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



2. Determine whether the vulnerabilities can be exploited and information gathered from the same.
3. Recommend solutions to plug these vulnerabilities.

Audit Scope

The following web application within the scope of the VAPT exercise.

Sr. No.	Web Service Link
1	http://44.209.151.89:5173/

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

S. No	Asset Description	Criticality of Asset	Internal IP Address	URL	Public IP Address	Location	Hash Value (in case of applications)	Version (in Case of applications)	Other details such as make and model in case of network devices or security devices.
1.	Web Application	Not Applicable	Not Available	http://44.209.151.89:5173/			Application SHA value		Not Applicable

Engagement Scope

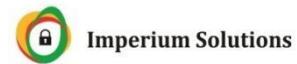
Details of the Auditing team

S. No.	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshot information published on CERT-In's website(Yes/No)
1	Mr. Sanjeev Chavan	Information Security Consultant	sanjeev.chavan@imperiumsolution.com	Masters in Computer Science	No

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



S. No.	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshot information published on CERT-In's website(Yes/No)
2	Ms. Tasneam P	Head - Information Security and Data Privacy	tasneam@imperi umsolution.com	CISA	Yes

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Methodology

The vulnerability assessment and penetration testing methodology is as outlined below:

Information Gathering

1. Study & scope the IT architecture & components for assessment
2. Determine the boundary of analysis
3. Impact analysis for Active scans, which includes assessment of Services or Servers scans in the operations environment.
4. Plan for Downtime & Contingency, if applicable
5. Estimate the scan process, based on the complexity of the target networks, hosts and applications
6. Define the scan Policy for each target. Scan Policy to define the level of scan – Information gathering, Policy checking, Port scanning, Password analysis, Attack stimulation etc.
7. Scan the targeted networks, hosts and applications based on the defined scan policy
8. Collect the scan results and analyse the security loopholes, configuration errors, default installation settings, overlooked setups, password quality, firmware/software revisions, patch fixes, security policy violations etc.
9. Submission of Assessment Reports with suggestions and recommendations to fix the vulnerabilities.

Analysis

1. Analysis the scan results and details collected.

Report Preparation

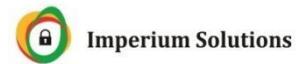
The report will comprise of the following assessment components

1. Vulnerability Assessment and Penetration testing Findings

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

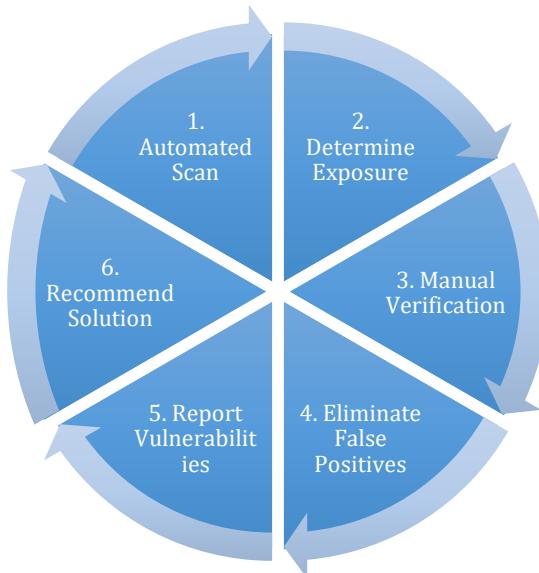
Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



2. Recommendations – Controls to be implemented to mitigate the identified vulnerabilities.

Vulnerability Assessment Methodology

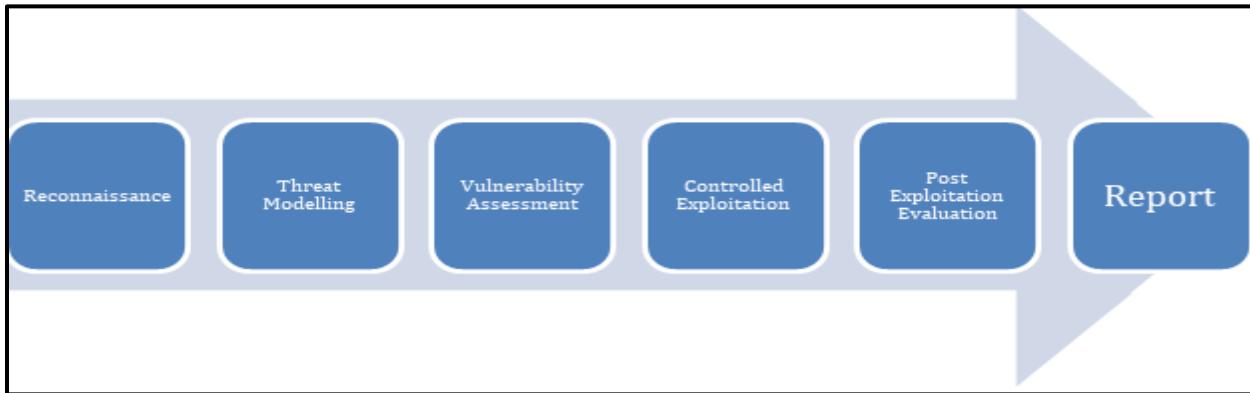
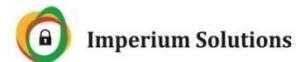


Penetration Testing Methodology

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Audit Conducted

Below are the details of the applications for which the Web audit was conducted.

Sr. No.	Web Service Link
1	http://44.209.151.89:5173/

Tools/ Software used

Sr. No.	Name of Tool/ Software used	Version of the tool/Software used	Open Source/Licensed
1.	BurpSuit Professional	V.2024.4	Licensed

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Risk Summary

The vulnerability assessment and penetration testing exercise aims to highlight the existing vulnerabilities within the application module and the different ways in which it can be addressed and closed.

We strongly recommend expeditious removal of the inconsistencies brought out in this report.

Risks have been defined as critical, high, medium and low.

Critical risks: These risks have to be addressed on priority. The system is extremely vulnerable and needs prompt mitigation.

High risk: There is a strong need for corrective measures. The existing system may continue to operate but the corrective action needs to be implemented as soon as possible

Medium risk: Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

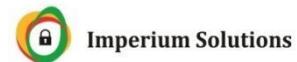
Low risk: Client Shall determine whether corrective actions are still required or decide to accept the risk.

Likelihood	
Level	Definition
High	The threat's source is highly motivated and sufficiently capable, and controls that prevent the vulnerability from being exercised are ineffective.
Medium	The threat's source is motivated and capable, but controls are in place that may impede a successful exercise of the vulnerability.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



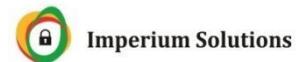
Likelihood	
Level	Definition
Low	The threat's source lacks motivation or capability, and controls are in place to prevent or significantly impede the vulnerability from being exercised.

Impact and Degree	
Level	Definition
High	High impact risks may result in the high costly loss of assets; risks that significantly violate, harm, or impede operations; or risks that cause human death or serious injury.
Medium	Medium impact risks may result in the costly loss of assets; risks that violate, harm, or impede operations; or risks that cause human injury.
Low	Low impact risks may result in the loss of some assets or may noticeably affect operations.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Risk	
Mitigation	Recommendation
Critical	This is a critical vulnerability and needs to be addressed immediately
High	There is a strong need for corrective measures. The existing system may continue to operate but the corrective action needs to be put in place as early as possible
Medium	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time
Low	Company to determine corrective actions or decide to accept the risk

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Management Summary

Our Information Security Assessment team would like to take this opportunity to thank all the participants for their assistance and co-operation in ensuring that the assessment could be completed smoothly and in a timely manner.

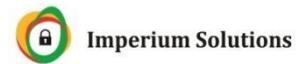
The web application module was in the scope of the VAPT activity. Critical and High vulnerabilities have been identified during the scan. The scan has been done using multiple tools followed by manual verification to reduce the risks of false positives. It is recommended that the Critical and High vulnerabilities be addressed immediately.

It is further recommended that the Application be scanned for vulnerabilities whenever there is a change in the configuration or at least once in a year, whichever is earlier. All changes to the application should be done through a proper change management process.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Below is the summarized report of the vulnerabilities.

Critical	High	Medium	Low	Information
0	03	10	11	00

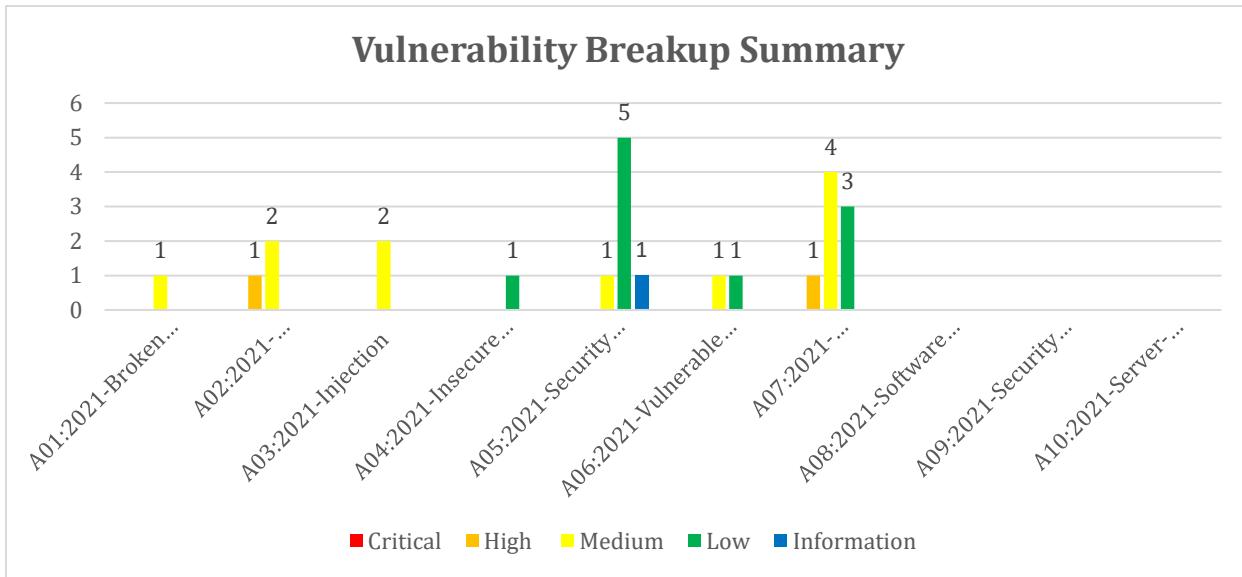
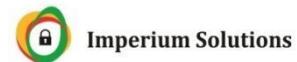


Figure 1: Vulnerability Distribution with severity

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

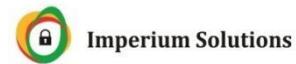


S. No	Affected Asset	Observation/ Vulnerability title	CVE/CWE	Control Objective	Control Name	Audit Requirement	Severity	Recommendation	Reference	New or Repeat observation
1	http://44.209.151.89:5173	Brute force Attack	CWE-307	NA	NA	NA	High	Temporarily lock accounts after a number of failed login attempts.	https://owasp.org/www/w-community/nitity/attacks/Brute_force_attacks/Brute_force_attacks/	New Observation
2	http://44.209.151.89:5173	Credential transmitted to Server in Plain Text	CWE-319	NA	NA	NA	High	Use HTTPS for all web traffic, especially during login or	https://www.acunetix.com/vulnerabilities/web/password-transmi	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

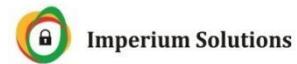


								API authentication.	tted-over- http/	
3	http://44.209.151.89:5173/	Vertical Previleage Escalration	CWE 434	NA	NA	NA	High	Assign roles and permissions clearly (e.g., user, moderator, admin).	https://www.acunetix.com/vulnerabilities/web/tag/privilege-escalation/	New Observatio n
4	http://44.209.151.89:5173/	Broken Authentication Via Response Mainupulation	CWE-345	NA	NA	NA	Medium	Never expose authentication status flags in client-controllable data (like	https://owasp.org/Top10/A07_2021-Identification_and_Authentication	New Observatio n

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

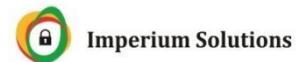
Period: Period: 14th May 2025 – 17th May 2025



								JSON, local storage, cookies without HttpOnly).	tion Failures/	
5	http://44.209.151.89:5173/	Captcha not implemented	CWE-799	NA	NA	NA	Medium	For better user experience, use invisible or adaptive CAPTCHA based on behavior.	https://www.acunetix.com/vulnerabilities/webscanner/plugins-login-no-captcha-ha-security/	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

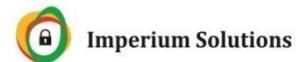


Period: Period: 14th May 2025 – 17th May 2025

								bypass-1-4-1/	
6	http://44.209.151.89:5173/	Configuration file Accessible	CWE-538	NA	NA	NA	Medium	Ensure sensitive files (e.g., .env, config.php) are not directly accessible via HTTP.	https://www.acunetix.com/vulnerabilities/web/config-file-disclosure/
7	http://44.209.151.89:5173/	Sensitive Data not masked	CWE-359	NA	NA	NA	Medium	Filter out or redact sensitive fields before writing to logs (e.g.,	https://cwe.mitre.org/data/definitions/200.html

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



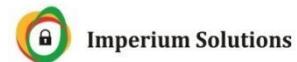
Period: Period: 14th May 2025 – 17th May 2025

								passwords, tokens, PII).		
8	http://44.209.151.89:5173/	Session Token in Url	CWE-598	NA	NA	NA	Medium	Store session tokens in secure, HttpOnly, SameSite cookies instead of URLs.	https://www.unetix.com/vulnerabilities/web/session-id-in-url/	New Observation
9	http://44.209.151.89:5173/	Json Syntax Error	CWE-116	NA	NA	NA	Medium	Use strict schema validation (e.g., using AJV in Node.js or	https://www.victimlearn.com/json-injection/	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

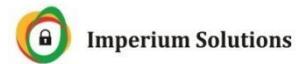


								jsonschema in Python)		
10	http://44.209.151.89:5173/	Improper Error Handling	CWE-209	NA	NA	NA	Medium	Ensure that error messages shown to users do not contain sensitive information. Use generic messages like "Something went wrong."	https://owasp.org/www-w-community/Improper_Error_Handling	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

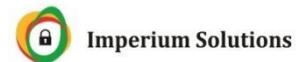


								Please try again later" rather than exposin g technic al details.		
11	http://44.209.151.89:517 <u>3/</u>	Improper Input Validation	CWE-20	NA	NA	NA	Medium	Whitelisting should be used wherever possible. Only allow known, safe inputs (e.g.,	https://cwe.mitre.org/data/definitions/20.html	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

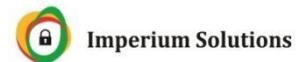
Period: Period: 14th May 2025 – 17th May 2025



								specific characters, length, and data types).		
12	http://44.209.151.89:5173/	Weak Password Policy	CWE-521	NA	NA	NA	Medium	Prevent users from reusing their last N passwords (e.g., last 5 or 10 passwords).	https://www.acunetix.com/vulnerabilities/webs/weak-password/	New Observation
13	http://44.209.151.89:5173/	Unencrypted Communication	CWE-319	NA	NA	NA	Medium	Ensure that all web traffic is encrypted	https://www.acunetix.com/vulnerabilities/webs/weak-password/	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

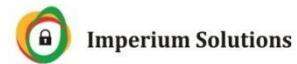


Period: Period: 14th May 2025 – 17th May 2025

								ed with TLS (Transport Layer Security), previously known as SSL.	ties/webs/ssl-tls-not-implemented/	
14	http://44.209.151.89:5173/	Missing Security Headers	CWE 693	NA	NA	NA	Low	Implementation Security Headers, Adds, Adds, recommends, Header security headers to your web server configuration.	https://cheatshheetseries.oswasp.org/chartsheets/HTTP-Headers/Security-Headers-to-your-web-server-configuration.html	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

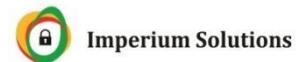


Period: Period: 14th May 2025 – 17th May 2025

								ration or applicat ion respons e.		
15	http://44.209.151.89:5173/	Concurrent Login	CWE-307	NA	NA	NA	Low	Implement a policy to allow only a single active session per user at a time (or a limited number of sessions). This can help	https://owasp.org/www-project-web-security-testing-guide/Iatest/4-Web_Application_Security_Testing/06-Session_Manag	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



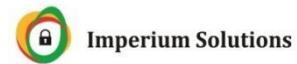
Period: Period: 14th May 2025 – 17th May 2025

								prevent multiple logins and control access to the user account more securely.	ement Testing/ 11- Testing for Co ncurren t Sessi ons	
16	http://44.209.151.89:5173/	Lack of Phone number Verification	CWE-284	NA	NA	NA	Low	When users enter a phone number, send a one-time passcode (OTP) to that number. The	https://cwe.mitre.org/data/definitions/345.html	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

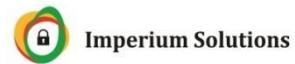


								user must then enter the correct OTP to verify ownership of the phone number .		
17	http://44.209.151.89:5173/	clickjacking Attack	CWE-1021	NA	NA	NA	Low	The X-Frame-Options HTTP header prevents your content from being embed	https://owasp.org/www-w-community/Security %20-%20Clickjacking	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

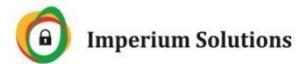


								ded into an iframe. This can block clickjacking attacks by disallowing your page from being embedded on malicious sites.		
18	http://44.209.151.89:5173/	Exposed Directory File	CWE-548	NA	NA	NA	Low	Disable directory listing on the web server	https://www.acunetix.com/vulnerabilities/we	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

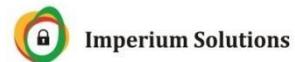
Period: Period: 14th May 2025 – 17th May 2025



								(e.g., Apache, Nginx). This prevent s attacke rs from viewing the content s of director ies that do not have an index file (e.g., index.htm l, index.p hp).	b/direct ory-listings/	
--	--	--	--	--	--	--	--	---	--	--

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



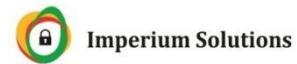
Period: Period: 14th May 2025 – 17th May 2025

19	http://44.209.151.89:5173/	Outdated Component Used	CWE-1104	NA	NA	NA	Low	Ensure that all components (e.g., libraries, frameworks, APIs) are updated to the latest stable version that has received security patches	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_COMPONENTS/	New Observation
20	http://44.209.151.89:5173/	Functionality Not Working	CWE-802	NA	NA	NA	Low	Conduct unit testing, integration	https://www.invicti.com/web-	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

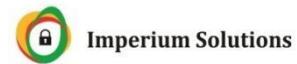


								ion testing, and user acceptance testing (UAT) to ensure that all features are functioning as expected in different environments and scenarios.	vulnerability-scanner /vulnerabilities /classification/ cwe-22/	
--	--	--	--	--	--	--	--	---	--	--

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

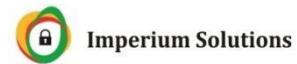


21	http://44.209.151.89:517 3/	Allow origin Allow origin Misconfiguration	CWE-345	NA	NA	NA	Low	If the origin must be dynamic (i.e., vary based on the request), implement logic to check the Origin header and ensure it matches a whitelis	https://www.acunetix.com/vulnerabilities/web/misconfiguration/	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

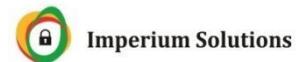


								t of trusted origins.		
22	http://44.209.151.89:5173/	Old Password Set as New Password	CWE-759	NA	NA	NA	Low	When users attempt to change their password, ensure that the new password is different from the old password.	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web-Application-Security-Testing/04-	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

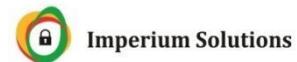
Period: Period: 14th May 2025 – 17th May 2025



								rd. This is a simple yet crucial validati on check.	Authent ication Testing/ 09- Testing for W eak Pas sword Change or Res et Func tionaliti es	
23	http://44.209.151.89:5173/	Unwanted http Method Enable	CWE-444	NA	NA	NA	Low	Review the HTTP methods allowed by your web server and application, and	https://owasp.org/www-project-web-security-testing-guide/v-4.14/Web%20Application%20Security%20Testing	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



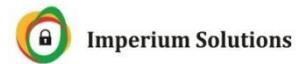
Period: Period: 14th May 2025 – 17th May 2025

								disable any that are unnecessary for the functioning of the application.	application Security Testing/02- Configuration and Deployment Management Test Plan Methods	
24	http://44.209.151.89:5173/	Open port	CWE-200	NA	NA	NA	Low	Identify and close any open ports that are not needed	https://mas.org/MASE/MAS_VS-NETWORK/MA	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

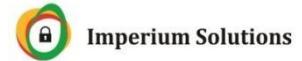


								for legitimate purposes. This includes ports related to unused services, outdated protocols, or any service that does not need to be exposed to the	SWE-0051/	
--	--	--	--	--	--	--	--	---	---------------------------	--

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

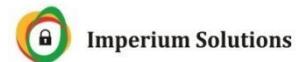


								internet .		
--	--	--	--	--	--	--	--	---------------	--	--

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Detailed Report

Vulnerability Details

Vulnerability Severity Level:

Critical	
High	
Medium	
Low	
Information	

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



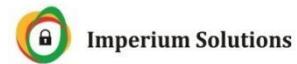
01 : Brute Force Attack

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	A Brute Force Attack occurs when an attacker systematically attempts all possible combinations of usernames and passwords until the correct one is found. This typically targets login forms, APIs, or password-protected resources that do not have adequate protection mechanisms in place.
Detailed observation / Vulnerable point	Unauthorized access to sensitive user accounts or administrative interfaces Credential stuffing when credentials from other breaches are reused
CVE/CWE	CWE-307
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	High

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Recommendation	Temporarily lock accounts after a number of failed login attempts. Use exponential backoff or CAPTCHA after repeated failures
Reference	https://owasp.org/www-community/attacks/Brute_force_attack
New or Repeat observation	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Period: Period: 14th May 2025 – 17th May 2025

References to evidences / Proof of Concept

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: `http://10.10.10.11:8080/200`

Update Host header to match target

Add

Clear

Auto

Refresh

⑦ Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 60

Payload type: Simple list Request count: 60

⑦ Payload Options [Simple list]

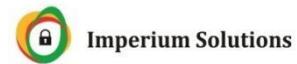
This payload type lets you configure a simple list of strings that are used as payloads.

Paste password
Load 12345678
Remove 1234
Clear queryy
Duplicate 12345
Deduplicate origin
Add pass
baseball
football
Enter a new item
Add from list

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Results	Positions	Payloads	Resource Pool	Options			
Filter: Showing all items							
Request	Payload		Status	Error	Timeout	Length ^	Comment
49	asshole		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
50	6969		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
51	pepper		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
52	daniel		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
53	access		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
54	123456789		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
55	654321		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
56	joshua		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
57	maggie		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
58	starwars		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
59	silver		400	<input type="checkbox"/>	<input type="checkbox"/>	279	
60	william		400	<input type="checkbox"/>	<input type="checkbox"/>	279	

Request Response

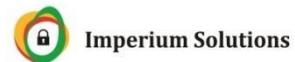
Pretty Raw Hex Render

```
1 HTTP/1.1 400 Bad Request
2 X-Powered-By: Express
3 Access-Control-Allow-Origin: *
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 31
6 ETag: W/"1f=mrQGkx/r4K/ssDwseqQciH0yM"
7 Date: Fri, 16 May 2025 15:12:17 GMT
8 Connection: close
9
10 {
    "error": "Invalid credentials"
}
```

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



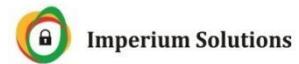
02: Credential Transmitted to Server in Plain Text

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	This vulnerability occurs when sensitive data — such as usernames, passwords, API keys, or session tokens — is transmitted over the network without encryption, such as via HTTP instead of HTTPS, or via other insecure protocols like FTP, SMTP, or Telnet.
Detailed observation / Vulnerable point	Credential interception by attackers via sniffing (Man-in-the-Middle attacks)
CVE/CWE	CWE-319
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	High
Recommendation	Use HTTPS for all web traffic, especially during login or API authentication.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

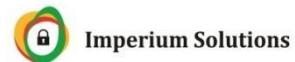


Reference	https://www.acunetix.com/vulnerabilities/web/password-transmitted-over-http/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a terminal window displaying a POST request to the endpoint /api/v1/user/login. The request includes various headers such as Host, Content-Length, Accept, User-Agent, and Origin. The JSON payload is highlighted with a red box and shows an identifier, password, and rememberMe field. <pre>1 POST /api/v1/user/login HTTP/1.1 2 Host: 44.209.151.89:3000 3 Content-Length: 78 4 Accept: / 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Origin: http://44.209.151.89:5173 8 Referer: http://44.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US,en;q=0.9 11 Connection: close 12 13 { 14 "identifier": "m0d0film@gmail.com", 15 "password": "OPDC@admin", 16 "rememberMe": false 17 }</pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



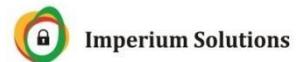
03: Vertical Privilege Escalation

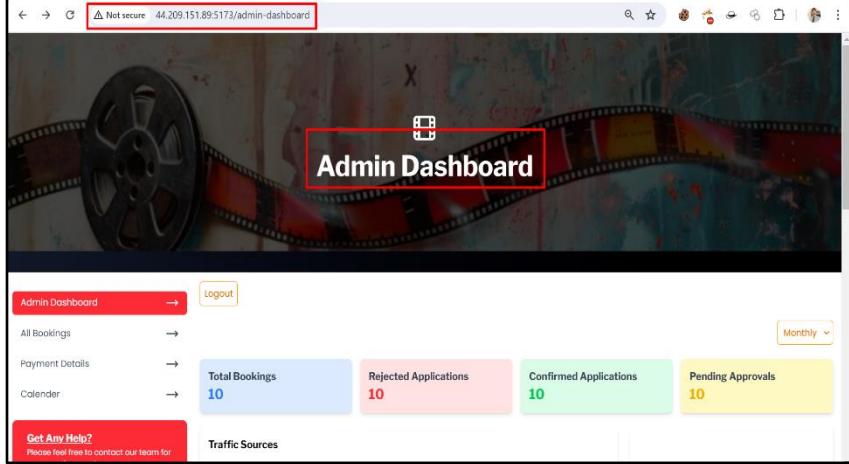
Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Vertical privilege escalation occurs when a user gains access to higher-level privileges or functions than they are authorized for. For example, a regular user accessing an admin dashboard, or an unprivileged user performing actions that only a system administrator should be able to perform.
Detailed observation / Vulnerable point	Unauthorized access to administrative features. Data manipulation, deletion, or exfiltration
CVE/CWE	CWE-269
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	High

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

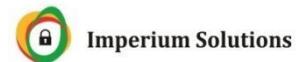


Recommendation	Assign roles and permissions clearly (e.g., user, moderator, admin). Check permissions on the server-side for every sensitive action.
Reference	https://www.acunetix.com/vulnerabilities/web/tag/privilege-escalation/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

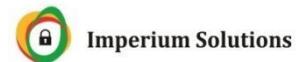
Period: Period: 14th May 2025 – 17th May 2025



This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

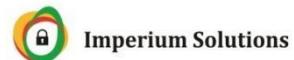


The image displays two screenshots of a web application interface. The top screenshot shows the 'User Dashboard' with a context menu open over the header area. The 'Paste' option in the menu is highlighted with a red box. The dashboard itself has a 'Welcome back, test user!' message, a sidebar with links for 'New Bookings', 'Booking History', 'Payment History', and 'Profile', and a 'Quick Actions' section with 'New Booking' and 'View Application Form' buttons. The bottom screenshot shows the 'Admin Dashboard' with a large 'Admin Dashboard' title. It features a sidebar with 'Logout' and links for 'All Bookings', 'Payment Details', and 'Calender'. Below the sidebar are four colored boxes showing booking statistics: 'Total Bookings 10' (blue), 'Rejected Applications 10' (red), 'Confirmed Applications 10' (green), and 'Pending Approvals 10' (yellow). A 'Monthly' dropdown menu is visible in the top right corner of this section.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



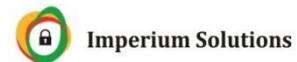
04: Broken Authentication Via Response Manipulation

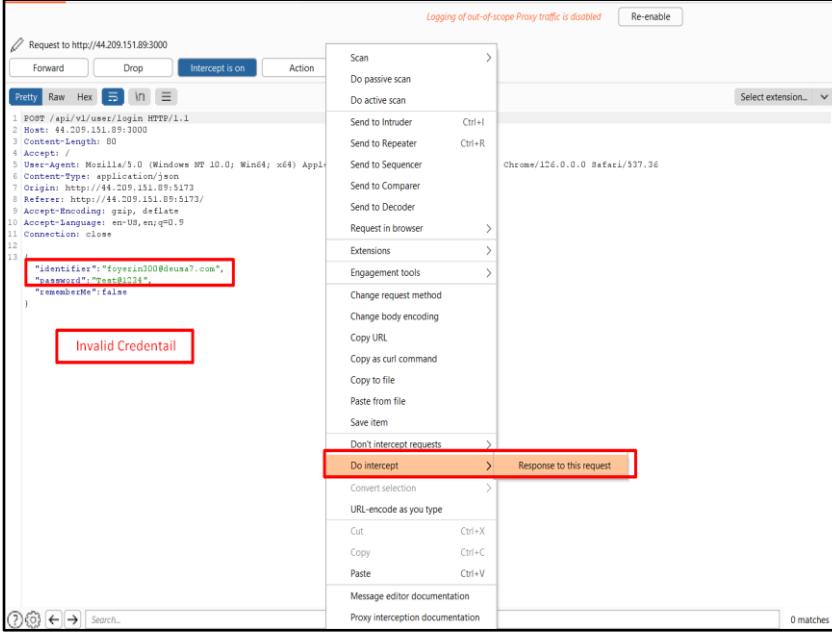
Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Broken Authentication via Response Manipulation occurs when a web application incorrectly trusts user-controllable client-side data (such as HTTP responses, status codes, or headers) to confirm authentication or login success.
Detailed observation / Vulnerable point	Bypass of authentication Account takeover Privilege escalation Full compromise of application security trust model
CVE/CWE	CWE-345
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium
Recommendation	Do not rely on client-side logic to determine whether a user is logged in. Validate tokens/sessions on the server for each sensitive request.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

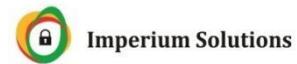


Reference	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	 <p>The screenshot shows a NetworkMiner capture of a POST request to http://44.209.151.89:3000/api/v1/users/login. The request body contains the following JSON payload:</p> <pre> 1 POST /api/v1/users/login HTTP/1.1 2 Host: 44.209.151.89:3000 3 Content-Length: 80 4 Accept: / 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 6 Content-Type: application/json 7 Origin: http://44.209.151.89:3000 8 Referer: http://44.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US, en;q=0.9 11 Connection: close 12 13 { "identifier": "foyerin3D0Bdeusa7.com", "password": "Text@1234", "rememberMe": false } </pre> <p>A red box highlights the password field. Below the request, an error message "Invalid Credential" is displayed.</p> <p>The NetworkMiner context menu is open, showing options like Scan, Do passive scan, Do active scan, and various send actions. A sub-menu under "Do intercept" is also visible.</p>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



The screenshot displays two log entries from a proxy tool interface:

Log entry 1 (Invalid Credential Response):

```
HTTP/1.1 400 Bad Request
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 31
ETag: W/"1f-aMxQGQz/cxf/mnDmseqQClH5yM"
Date: Fri, 16 May 2025 09:48:38 GMT
Connection: close
{
  "error": "Invalid credentials"
}
```

A red box highlights the JSON response body, and a red callout box says: "Modify the invalid Credential response with valid Credential response".

Log entry 2 (Valid Credential Response):

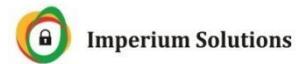
```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 340
ETag: W/"194-aXf6nJNedgOp6eIHeVPTC5bdc"
Date: Fri, 16 May 2025 07:11:00 GMT
Connection: close
{
  "message": "Login successful",
  "user": {
    "_id": "68243ae6cc098334a97a49e9",
    "name": "John Doe",
    "email": "johndoe123@gmail.com",
    "phoneNo": "+919876543210",
    "role": "ADMIN"
  }
}
{
  "token": "eyJhbGciOiJIUzI1NiJ9.a25cCc16tpXVC39.eyJpc3VzSWQiOiI0ODI0NDE1NmFjMDk4MjM0Yzg3YTQ5ZTkiLCJpYXQiOjE2NDc2Nzk0NjA1MjV4CzIgMzQCMHD.1QuoNxzB6lg0s0dbxv5
  "exp": "2025-05-16T07:11:00Z"
}
```

A red box highlights the JSON response body, and a red callout box says: "valid Credential Response".

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

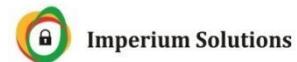


A screenshot of a web application audit tool, likely Burp Suite, showing an intercept session. The interface includes a toolbar at the top with various options like Extender, Project options, User options, Learn, 403 Bypass, Authorize, CORS*, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Composer, and Logger. Below the toolbar, tabs for Intercept, HTTP history, WebSockets history, and Options are visible. A message in the center says "Logging of out-of-scope Proxy traffic is disabled". Buttons for Forward, Drop, Intercept (which is highlighted in blue), Action, and Open Browser are present. A note below states: "When selected requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server." Buttons for "Learn more" and "Open browser" are also shown. To the right, a browser window shows a login success message ("Login successful") and an "Admin Dashboard" page with a video camera icon. Below the dashboard are two cards: "Total Bookings 10" and "Rejected Applications 10". The browser status bar indicates "Not secure" and the URL "44.209.151.89:5173/...".

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



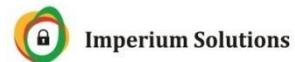
05: Captcha not Implement

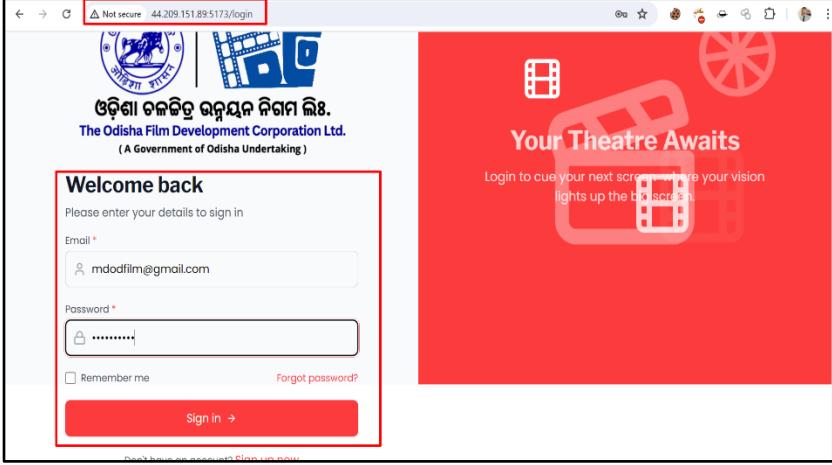
Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Failing to implement a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) on critical user input forms (e.g., login, registration, password reset) can leave the application vulnerable to automated abuse such as Brute-force login attempts Credential stuffing attacks
Detailed observation / Vulnerable point	Account takeover through automated brute-force or credential stuffing Denial of service or abuse of application features
CVE/CWE	CWE-799
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Recommendation	For better user experience, use invisible or adaptive CAPTCHA based on behavior. Complement CAPTCHA with IP-based rate limiting and lockouts.
Reference	https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-login-no-captcha-recaptcha-security-bypass-1-4-1/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



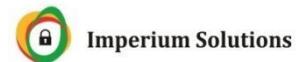
06: Configuration file Accessible

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	When sensitive configuration files (such as .env, config.php, web.config, application.yml, or .git/config) are publicly accessible over the web, attackers can retrieve them and gain access to Database credentials API keys and secrets
Detailed observation / Vulnerable point	Credential leakage (database, cloud, third-party APIs) Unauthorized access to systems
CVE/CWE	CWE-538
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Recommendation	Ensure sensitive files (e.g., .env, config.php) are not directly accessible via HTTP. Restrict read access to configuration files to only necessary system users.
Reference	https://www.acunetix.com/vulnerabilities/web/configuration-file-disclosure/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	 A screenshot of a web browser window showing the source code of a file named 'vite.config.ts'. The code imports 'defineConfig' from 'vite', 'react' from '@vitejs/plugin-react', and 'tailwindcss' from 'tailwindcss/vite'. It then defines a default export for a configuration object with a 'plugins' array containing the imported modules, a 'server' object with a host of '0.0.0.0' and port 5173, and a closing brace. A red rectangular box highlights the code area.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

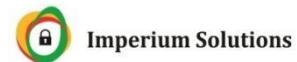


07: Sesnsitive Data not masked

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Sensitive data (e.g., credit card numbers, Social Security Numbers (SSNs), email addresses, authentication tokens, or medical records) should be masked when displayed in user interfaces, logs, debug tools, or transmitted in non-secure contexts.
Detailed observation / Vulnerable point	Privacy violations (especially under regulations like GDPR, HIPAA, PCI-DSS) Identity theft or financial fraud Reputation damage
CVE/CWE	CWE-359
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Period: Period: 14th May 2025 – 17th May 2025

Recommendation	Filter out or redact sensitive fields before writing to logs (e.g., passwords, tokens, PII). Only authorized roles should see unmasked data.
Reference	https://cwe.mitre.org/data/definitions/200.html
New or Repeat observation	New Observation
References to evidences / Proof of Concept	<pre> Request 1 POST /api/v1/user/login HTTP/1.1 2 Host: 44.209.151.89:3000 3 Content-Length: 78 4 Accept: application/json, text/plain, */* 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Origin: http://44.209.151.89:5173 8 Referer: http://44.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US;q=0.9 11 Connection: close 12 13 { "identifier": "mdodfilm@gmail.com", "password": "QFDOadmin", "rememberMe": false } </pre> <pre> Response 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Access-Control-Allow-Origin: * 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 341 6 ETag: W/"154-a/xfgmNAdyOp9d4IHeVPTCShdc" 7 Date: Fri, 16 May 2025 07:11:00 GMT 8 Connection: close 9 10 [{ "message": "Login successful", "user": { "id": "#8243a6cc098234a8749e5", "name": "OFC", "email": "mdodfilm@gmail.com", "phoneNo": "+91912305155", "role": "ADMIN" }, "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiUiMjM0k4HjMDTyTgYtQ529L1c0pYQoCjE3Moc2s2hNjAsImV4cCI6MTw4cCIOtW0.1ou0Bxx2BQDq8s1bPv9Hs2xQ4_AqBByyySg11x02-z" }] </pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



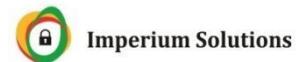
08: Session Token in Url

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Session tokens should never be included in the URL (query string) of a request. When session identifiers are passed via URLs, they may be. Stored in browser history Shared via Referer headers to third-party sites
Detailed observation / Vulnerable point	Session hijacking via leaked URLs Unauthorized access to user accounts or administrative interfaces
CVE/CWE	CWE-598
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium
Recommendation	Store session tokens in secure, HttpOnly, SameSite cookies instead of URLs. Use POST requests for login and session handling.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Reference	https://www.acunetix.com/vulnerabilities/web/session-id-in-url/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a network traffic capture tool showing a request. The URL is highlighted with a red box and contains a session ID parameter: '?token=GKnkZDwmwHrv'. The request is a GET to port 5173. Other headers include Connection: Upgrade, Pragma: no-cache, Cache-Control: no-cache, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36, Upgrade: websocket, Origin: http://44.209.151.89:5173, Sec-WebSocket-Version: 13, Accept-Encoding: gzip, deflate, Accept-Language: en-US, en;q=0.9, Sec-WebSocket-Key: lMl3frEWEalmOKhDg0o0fw==, and Sec-WebSocket-Protocol: vite-hmr.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

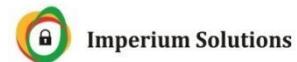


09: Json Syntax Error

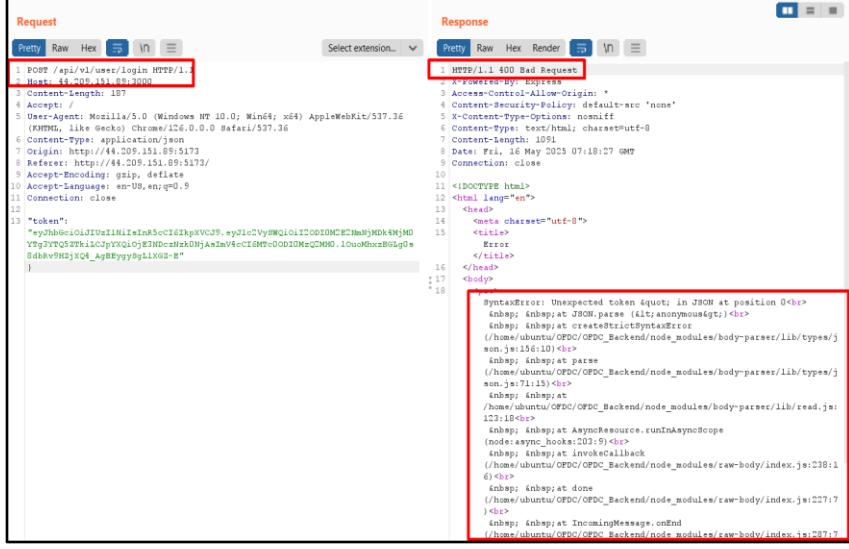
Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	A JSON Syntax Error occurs when the JSON data structure is malformed or not properly formatted, making it unreadable or improperly parsed by the server or client. Common causes include Missing commas or braces Improper escaping of quotes
Detailed observation / Vulnerable point	Service disruption or application errors Data parsing failures
CVE/CWE	CWE 693
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium
Recommendation	Use strict schema validation (e.g., using AJV in Node.js or jsonschema in Python). Reject malformed JSON before processing.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Period: Period: 14th May 2025 – 17th May 2025

Reference	https://www.invicti.com/learn/json-injection/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	 <pre> Request Pretty Raw Hex ⌂ ⌃ ⌄ ⌅ ⌆ 1 POST /api/user/login HTTP/1.1 2 Host: 44.209.151.89:3000 3 Content-Length: 187 4 Accept: / 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 6 Origin: http://44.209.151.89:5173 7 Origin: http://44.209.151.89:5173 8 Referer: http://44.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US, en;q=0.9 11 Connection: close 12 13 "token": "eyJhbGciOiJIUzI1NiIiんIn5cG16IkpxVVOj5..eyJlcCvyeWQjO1I2ODIDMCE2NmNjMDk4MjMD 14 YTY3YTG5ZTRHikJpYXNlcnE3NDc2Mzk0NjAsImV4cCI6MTc0ODIDMzQCMH0.1OusdxzBGlgs 15 Bdbkv9H2;XQ4_AgBFyggBgLlxG2-E" 16 17 18 </pre> <pre> Response Pretty Raw Hex Render ⌂ ⌃ ⌄ ⌅ ⌆ 1 HTTP/1.1 400 Bad Request 2 Error: SyntaxError: Unexpected token &quot; in JSON at position 0
 3 at JSON.parse (<anonymous>:4) 4 at Object.createStrictBytecodeError 5 at JSON.parse (/home/ubuntu/GFDC/GFDC_Backend/node_modules/body-parser/lib/types/j 6 son.js:156:10)
 7 at JSON.parse (/home/ubuntu/GFDC/GFDC_Backend/node_modules/body-parser/lib/types/j 8 son.js:71:15)
 9 at invokeCallback 10 at /home/ubuntu/GFDC/GFDC_Backend/node_modules/raw-body/index.js:238:1 11 at done 12 at AsyncResource.runInAsyncScope 13 at hooks:203:9
 14 at invokeCallback 15 at /home/ubuntu/GFDC/GFDC_Backend/node_modules/raw-body/index.js:227:7 16 at IncomingMessage.onEnd 17 at IncomingMessage._readableEnd 18 </pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

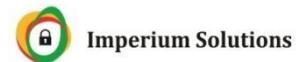


10: Improper Error Handling

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Improper error handling occurs when an application fails to properly manage or present error messages, potentially exposing sensitive information (e.g., stack traces, internal database queries, paths, server configurations) or allowing attackers to infer application logic. It can lead to Detailed error messages (e.g., SQL errors, stack traces) may reveal sensitive data such as database schema, application logic, or file paths.
Detailed observation / Vulnerable point	Exposure of sensitive information, like database credentials, file paths, or stack traces.
CVE/CWE	CWE-390
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Period: Period: 14th May 2025 – 17th May 2025

Recommendation	Ensure that error messages shown to users do not contain sensitive information. Use generic messages like "Something went wrong. Please try again later" rather than exposing technical details.
Reference	https://owasp.org/www-community/Improper_Error_Handling
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a web browser window. The address bar shows a URL starting with "Not secure 44.209.151.89:5173/all-bookings". Below the address bar, an error message "URI malformed" is displayed. The error stack trace is visible in the browser's developer tools. The page content shows a navigation menu with items like "Admin Das", "All Booking", "Payment D", and "Calender".

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



11: Improper Input Validation

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Improper Input Validation occurs when an application fails to validate input from users or external sources properly. It allows attackers to inject malicious or unexpected data that could compromise the security, integrity, or stability of the application.
Detailed observation / Vulnerable point	SQL Injection, Command Injection, Cross-Site Scripting (XSS), and other injection-based attacks. Buffer overflows leading to arbitrary code execution.
CVE/CWE	CWE-20
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium
Recommendation	Whitelisting should be used wherever possible. Only allow known, safe inputs (e.g., specific characters, length, and data types). Blacklist is

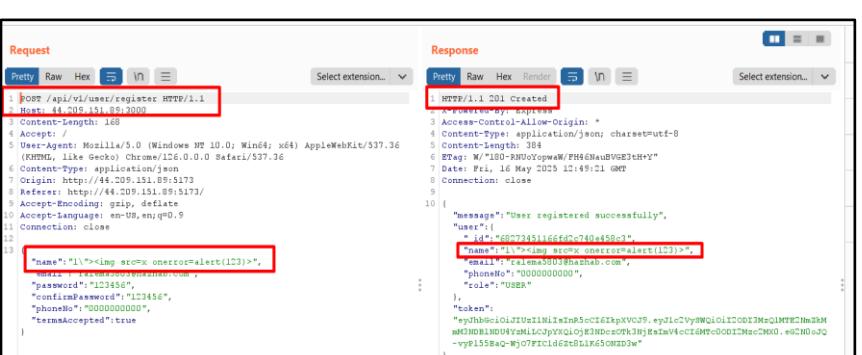
This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Imperium Solutions

Period: Period: 14th May 2025 – 17th May 2025

	generally a poor approach since attackers can craft payloads that bypass blacklist rules.
Reference	https://cwe.mitre.org/data/definitions/20.html
New or Repeat observation	New Observation
References to evidences / Proof of Concept	 <pre> Request Pretty Raw Hex ⌂ ⌃ ⌄ ⌅ Select extension... ⌋ 1 POST /api/v1/user/register HTTP/1.1 2 Host: 44.209.151.0:3000 3 Content-Length: 168 4 Accept: / 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Origin: http://44.209.151.0:5173 8 Referer: http://44.209.151.0:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US,en;q=0.9 11 Connection: close 12 13 14 "name": "\\\'>"} 15 "email": "testuser0000000000@gmail.com", 16 "password": "123456", 17 "confirmPassword": "123456", 18 "phoneNo": "0000000000", 19 "termsAccepted": true 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 179 180 181 182 183 184 185 186 187 188 189 189 190 191 192 193 194 195 196 197 198 199 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 219 220 221 222 223 224 225 226 227 228 229 229 230 231 232 233 234 235 236 237 238 239 239 240 241 242 243 244 245 246 247 248 249 249 250 251 252 253 254 255 256 257 258 259 259 260 261 262 263 264 265 266 267 268 269 269 270 271 272 273 274 275 275 276 277 278 279 279 280 281 282 283 284 285 285 286 287 288 289 289 290 291 292 293 294 295 295 296 297 298 299 299 300 301 302 303 304 305 305 306 307 308 309 309 310 311 312 313 313 314 315 316 316 317 318 319 319 320 321 322 323 323 324 325 325 326 327 327 328 329 329 330 331 331 332 333 333 334 335 335 336 337 337 338 339 339 340 341 341 342 343 343 344 345 345 346 347 347 348 349 349 350 351 351 352 353 353 354 355 355 356 357 357 358 359 359 360 361 361 362 363 363 364 365 365 366 367 367 368 369 369 370 371 371 372 373 373 374 375 375 376 377 377 378 379 379 380 381 381 382 383 383 384 385 385 386 387 387 388 389 389 390 391 391 392 393 393 394 395 395 396 397 397 398 399 399 400 401 401 402 403 403 404 405 405 406 407 407 408 409 409 410 411 411 412 413 413 414 415 415 416 417 417 418 419 419 420 421 421 422 423 423 424 425 425 426 427 427 428 429 429 430 431 431 432 433 433 434 435 435 436 437 437 438 439 439 440 441 441 442 443 443 444 445 445 446 447 447 448 449 449 450 451 451 452 453 453 454 455 455 456 457 457 458 459 459 460 461 461 462 463 463 464 465 465 466 467 467 468 469 469 470 471 471 472 473 473 474 475 475 476 477 477 478 479 479 480 481 481 482 483 483 484 485 485 486 487 487 488 489 489 490 491 491 492 493 493 494 495 495 496 497 497 498 499 499 500 501 501 502 503 503 504 505 505 506 507 507 508 509 509 510 511 511 512 513 513 514 515 515 516 517 517 518 519 519 520 521 521 522 523 523 524 525 525 526 527 527 528 529 529 530 531 531 532 533 533 534 535 535 536 537 537 538 539 539 540 541 541 542 543 543 544 545 545 546 547 547 548 549 549 550 551 551 552 553 553 554 555 555 556 557 557 558 559 559 560 561 561 562 563 563 564 565 565 566 567 567 568 569 569 570 571 571 572 573 573 574 575 575 576 577 577 578 579 579 580 581 581 582 583 583 584 585 585 586 587 587 588 589 589 590 591 591 592 593 593 594 595 595 596 597 597 598 599 599 600 601 601 602 603 603 604 605 605 606 607 607 608 609 609 610 611 611 612 613 613 614 615 615 616 617 617 618 619 619 620 621 621 622 623 623 624 625 625 626 627 627 628 629 629 630 631 631 632 633 633 634 635 635 636 637 637 638 639 639 640 641 641 642 643 643 644 645 645 646 647 647 648 649 649 650 651 651 652 653 653 654 655 655 656 657 657 658 659 659 660 661 661 662 663 663 664 665 665 666 667 667 668 669 669 670 671 671 672 673 673 674 675 675 676 677 677 678 679 679 680 681 681 682 683 683 684 685 685 686 687 687 688 689 689 690 691 691 692 693 693 694 695 695 696 697 697 698 699 699 700 701 701 702 703 703 704 705 705 706 707 707 708 709 709 710 711 711 712 713 713 714 715 715 716 717 717 718 719 719 720 721 721 722 723 723 724 725 725 726 727 727 728 729 729 730 731 731 732 733 733 734 735 735 736 737 737 738 739 739 740 741 741 742 743 743 744 745 745 746 747 747 748 749 749 750 751 751 752 753 753 754 755 755 756 757 757 758 759 759 760 761 761 762 763 763 764 765 765 766 767 767 768 769 769 770 771 771 772 773 773 774 775 775 776 777 777 778 779 779 780 781 781 782 783 783 784 785 785 786 787 787 788 789 789 790 791 791 792 793 793 794 795 795 796 797 797 798 799 799 800 801 801 802 803 803 804 805 805 806 807 807 808 809 809 810 811 811 812 813 813 814 815 815 816 817 817 818 819 819 820 821 821 822 823 823 824 825 825 826 827 827 828 829 829 830 831 831 832 833 833 834 835 835 836 837 837 838 839 839 840 841 841 842 843 843 844 845 845 846 847 847 848 849 849 850 851 851 852 853 853 854 855 855 856 857 857 858 859 859 860 861 861 862 863 863 864 865 865 866 867 867 868 869 869 870 871 871 872 873 873 874 875 875 876 877 877 878 879 879 880 881 881 882 883 883 884 885 885 886 887 887 888 889 889 890 891 891 892 893 893 894 895 895 896 897 897 898 899 899 900 901 901 902 903 903 904 905 905 906 907 907 908 909 909 910 911 911 912 913 913 914 915 915 916 917 917 918 919 919 920 921 921 922 923 923 924 925 925 926 927 927 928 929 929 930 931 931 932 933 933 934 935 935 936 937 937 938 939 939 940 941 941 942 943 943 944 945 945 946 947 947 948 949 949 950 951 951 952 953 953 954 955 955 956 957 957 958 959 959 960 961 961 962 963 963 964 965 965 966 967 967 968 969 969 970 971 971 972 973 973 974 975 975 976 977 977 978 979 979 980 981 981 982 983 983 984 985 985 986 987 987 988 989 989 990 991 991 992 993 993 994 995 995 996 997 997 998 999 999 1000 1000 1001 1002 1002 1003 1004 1004 1005 1006 1006 1007 1008 1008 1009 10010 10010 10011 10011 10012 10012 10013 10013 10014 10014 10015 10015 10016 10016 10017 10017 10018 10018 10019 10019 10020 10020 10021 10021 10022 10022 10023 10023 10024 10024 10025 10025 10026 10026 10027 10027 10028 10028 10029 10029 10030 10030 10031 10031 10032 10032 10033 10033 10034 10034 10035 10035 10036 10036 10037 10037 10038 10038 10039 10039 10040 10040 10041 10041 10042 10042 10043 10043 10044 10044 10045 10045 10046 10046 10047 10047 10048 10048 10049 10049 10050 10050 10051 10051 10052 10052 10053 10053 10054 10054 10055 10055 10056 10056 10057 10057 10058 10058 10059 10059 10060 10060 10061 10061 10062 10062 10063 10063 10064 10064 10065 10065 10066 10066 10067 10067 10068 10068 10069 10069 10070 10070 10071 10071 10072 10072 10073 10073 10074 10074 10075 10075 10076 10076 10077 10077 10078 10078 10079 10079 10080 10080 10081 10081 10082 10082 10083 10083 10084 10084 10085 10085 10086 10086 10087 10087 10088 10088 10089 10089 10090 10090 10091 10091 10092 10092 10093 10093 10094 10094 10095 10095 10096 10096 10097 10097 10098 10098 10099 10099 100100 100100 100101 100101 100102 100102 100103 100103 100104 100104 100105 100105 100106 100106 100107 100107 100108 100108 100109 100109 100110 100110 100111 100111 100112 100112 100113 100113 100114 100114 100115 100115 100116 100116 100117 100117 100118 100118 100119 100119 100120 100120 100121 100121 100122 100122 100123 100123 100124 100124 100125 100125 100126 100126 100127 100127 100128 100128 100129 100129 100130 100130 100131 100131 100132 100132 100133 100133 100134 100134 100135 100135 100136 100136 100137 100137 100138 100138 100139 100139 100140 100140 100141 100141 100142 100142 100143 100143 100144 100144 100145 100145 100146 100146 100147 100147 100148 100148 100149 100149 100150 100150 100151 100151 100152 100152 100153 100153 100154 100154 100155 100155 100156 100156 100157 100157 100158 100158 100159 100159 100160 100160 100161 100161 100162 100162 100163 100163 100164 100164 100165 100165 100166 100166 100167 100167 100168 100168 100169 100169 100170 100170 100171 100171 100172 100172 100173 100173 100174 100174 100175 100175 100176 100176 100177 100177 100178 100178 100179 100179 100180 100180 100181 100181 100182 100182 100183 100183 100184 100184 100185 100185 100186 100186 100187 100187 100188 100188 100189 100189 100190 100190 100191 100191 100192 100192 100193 100193 100194 100194 100195 100195 100196 100196 100197 100197 100198 100198 100199 100199 100200 100200 100201 100201 100202 100202 100203 100203 100204 100204 100205 100205 100206 100206 100207 100207 100208 100208 100209 100209 100210 100210 100211 100211 100212 100212 100213 100213 100214 100214 100215 100215 100216 100216 100217 100217 100218 100218 100219 100219 100220 100220 100221 100221 100222 100222 100223 100223 100224 100224 100225 100225 100226 100226 100227 100227 100228 100228 100229 100229 100230 100230 100231 100231 100232 100232 100233 100233 100234 100234 100235 100235 100236 100236 100237 100237 100238 100238 100239 100239 100240 100240 100241 100241 100242 100242 100243 100243 100244 100244 100245 100245 100246 100246 100247 100247 100248 100248 100249 100249 100250 100250 100251 100251 100252 100252 100253 100253 100254 100254 100255 100255 100256 100256 100257 100257 100258 100258 100259 100259 100260 100260 100261 100261 100262 100262 100263 100263 100264 100264 100265 100265 100266 100266 100267 100267 100268 100268 100269 100269 100270 100270 100271 100271 100272 100272 100273 100273 100274 100274 100275 100275 100276 100276 100277 100277 100278 100278 100279 100279 100280 100280 100281 100281 100282 100282 100283 100283 100284 100284 100285 100285 100286 100286 100287 100287 100288 100288 100289 100289 100290 100290 100291 100291 100292 100292 100293 100293 100294 100294 100295 100295 100296 100296 100297 100297 100298 100298 100299 100299 100300 100300 100301 100301 100302 100302 100303 100303 100304 100304 100305 100305 100306 100306 100307 100307 100308 100308 100309 100309 100310 100310 100311 100311 100312 100312 100313 100313 100314 100314 100315 100315 100316 100316 100317 100317 100318 100318 100319 100319 100320 100320 100321 100321 100322 100322 100323 100323 100324 100324 100325 100325 100326 100326 100327 100327 100328 100328 100329 100329 100330 100330 100331 100331 100332 100332 100333 100333 100334 100334 100335 100335 100336 100336 100337 100337 100338 100338 100339 100339 100340 100340 100341 100341 100342 100342 100343 100343 100344 100344 100345 100345 100346 100346 100347 100347 100348 100348 100349 100349 100350 100350 100351 100351 100352 100352 100353 100353 100354 100354 100355 100355 100356 100356 100357 100357 100358 100358 100359 100359 100360 100360 100361 100361 100362 100362 100363 100363 100364 100364 100365 100365 100366 100366 100367 100367 100368 100368 100369 100369 100370 100370 100371 100371 100372 100372 100373 100373 100374 100374 100375 100375 100376 100376 100377 100377 100378 100378 100379 100379 100380 100380 100381 100381 100382 100382 100383 100383 100384 100384 100385 100385 100386 100386 100387 100387 100388 100388 100389 100389 100390 100390 100391 100391 100392 100392 100393 100393 100394 100394 100395 100395 100396 100396 100397 100397 100398 100398 100399 100399 100400 100400 100401 100401 100402 100402 100403 100403 100404 100404 100405 100405 100406 100406 100407 100407 100408 100408 100409 100409 100410 100410 100411 100411 100412 100412 100413 100413 100414 100414 100415 100415 100416 100416 100417 100417 100418 100418 100419 100419 100420 100420 100421 100421 100422 100422 100423 100423 100424 100424 100425 100425 100426 100426 100427 100427 100428 100428 100429 100429 100430 100430 100431 100431 100432 100432 100433 100433 100434 100434 100435 100435 100436 100436 100437 100437 100438 100438 100439 100439 100440 100440 100441 100441 100442 100442 100443 100443 100444 100444 100445 100445 100446 100446 100447 100447 100448 100448 100449 100449 100450 100450 100451 100451 100452 100452 100453 100453 100454 100454 100455 100455 100456 100456 100457 100457 100458 100458 100459 100459 100460 100460 100461 100461 100462 100462 100463 100463 100464 100464 100465 100465 100466 100466 100467 100467 100468 100468 100469 100469 100470 100470 100471 100471 100472 100472 1004</pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

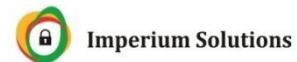


12: Weak Password Policy

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	A Weak Password Policy is a security vulnerability that arises when a system allows the creation of passwords that are too simple, too short, or easily guessable. This can make it easier for attackers to gain unauthorized access to user accounts through methods like brute force, dictionary attacks, or social engineering.
Detailed observation / Vulnerable point	Attackers can easily guess or brute-force weak passwords. Attackers gaining access to sensitive user data, internal systems, or administrative accounts.
CVE/CWE	CWE-521
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



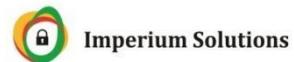
Period: Period: 14th May 2025 – 17th May 2025

Recommendation	Require passwords to be at least 12 characters long. Encourage or require the use of a combination of uppercase letters, lowercase letters, numbers, and special characters.
Reference	https://www.acunetix.com/vulnerabilities/web/weak-password/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	<p>The screenshot shows a POST request to '/api/v1/user/register' with the following JSON payload:</p> <pre> 1 POST /api/v1/user/register HTTP/1.1 2 Host: 44.209.151.89:3000 3 Content-Length: 108 4 Accept: application/json, text/plain, */* 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Origin: http://44.209.151.89:5173 8 Referer: http://44.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US, en;q=0.9 11 Connection: close 12 13 { "name": "1">"> "email": "e1234567890@shahab.com", "password": "1234567", "confirmPassword": "1234567", "phoneNo": "0000000000", "termsAccepted": true } </pre> <p>The response is a 201 Created status with the following JSON data:</p> <pre> HTTP/1.1 201 Created X-Powered-By: Express Access-Control-Allow-Origin: * Content-Type: application/json; charset=utf-8 Content-Length: 384 Date: Fri, 16 May 2025 12:49:21 GMT Connection: close { "message": "User registered successfully", "user": { "id": "62723451166fd7740e458c3", "name": "1">", "email": "e1234567890@shahab.com", "phoneNo": "0000000000", "role": "USER" }, "token": "eyJhbGciOiJIUzI1NiwiTech5cI6IkpxVVOjS...eyJlc2VybmQoIiIzODI3MeQ1MT82Nw3AM...zGDN81ND04YwMILC0pxyfQ1OjE3Ndc0T3H3ExInW4cCI0Rtc0CDEZMsc2M00..eGDN0OjQ...vyP155RaQ-Wj07fICld62te8Lk65GN2D3w" } </pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



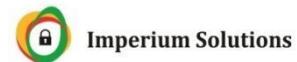
13: Unencrypted Communication

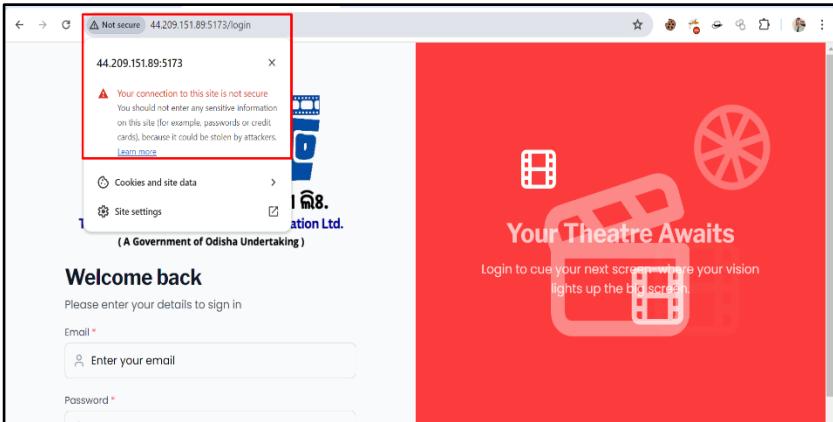
Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Unencrypted communication occurs when sensitive data, such as passwords, personal details, or payment information, is transmitted over the network without encryption. This means the data is sent in plaintext and can be intercepted and read by malicious actors.
Detailed observation / Vulnerable point	Attackers can read sensitive data transmitted over the network, including passwords, personal details, financial data, or authentication tokens.
CVE/CWE	CWE-320
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Medium

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

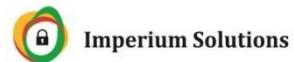


Recommendation	Ensure that all web traffic is encrypted with TLS (Transport Layer Security), previously known as SSL. Configure web servers to force HTTPS and redirect all HTTP traffic to HTTPS.
Reference	https://www.acunetix.com/vulnerabilities/web/ssl-tls-not-implemented/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	 <p>The screenshot shows a browser window with a red box highlighting the 'Not secure' warning in the address bar. The address bar displays '44.209.151.89:5173'. The warning message reads: 'Your connection to this site is not secure. You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.' Below the address bar, there are buttons for 'Cookies and site data' and 'Site settings'. The main content area shows a login form with fields for 'Email' and 'Password'. To the right of the login form, there is a red banner with the text 'Your Theatre Awaits' and 'Login to cue your next screen where your vision lights up the big screen!'. The banner features icons of a film reel and a camera.</p>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



14: Missing Security Headers

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Missing Security Headers is a common web application misconfiguration where the server response does not include HTTP headers that instruct browsers to behave securely. These headers help prevent a range of attacks including cross-site scripting (XSS), clickjacking, content sniffing, and data interception.
Detailed observation / Vulnerable point	Without Content-Security-Policy, attackers may inject malicious scripts into web pages.
CVE/CWE	CWE-693
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

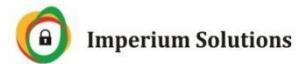


Recommendation	<p>Implement Security Headers, Add recommended security headers to your web server configuration or application response.</p> <p>Missing Content Security Policy (CSP) Header: default-src 'self'; script-src 'self' https://trusted.cdn.com</p> <p>Missing HTTP Strict-Transport-Security (HSTS) Header: max-age=31536000</p> <p>Missing Permissions-Policy Header: geolocation=(self), microphone=(), camera=(), Fullscreen=(self)</p> <p>Missing Referrer-Policy Header: no-referrer</p> <p>Missing X-Content-Type-Options Header: no sniff</p> <p>Missing X-Frame-Options Header: SAMEORIGIN or DENY</p> <p>Missing X-Permitted-Cross-Domain-Policies: none or master-only or by-content-type</p>
Reference	<p>https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html</p>
New or Repeat observation	New Observation

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



References to evidences / Proof of Concept

A screenshot of the Postman application interface. On the left, under 'Request', there is a red box highlighting a POST request to '/api/v1/user/login' with the URL 'http://44.209.151.89:3000'. The response on the right shows a red box around the status code 'HTTP/1.1 200 OK'. The response body is a JSON object containing a message, user details (id, name, email, phone), tokens, and a role.

```
HTTP/1.1 200 OK
{
  "message": "Login successful",
  "user": {
    "id": "62c242a6cc0086234a7a49e9",
    "name": "Oded",
    "email": "odedfilm@gmail.com",
    "phone": "+972305169",
    "role": "ADMIN"
  },
  "tokens": [
    "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiUi4NCjEwODk4MmNjMDk4MjM0Yjg3YTZCOTkxIiwiZWQIj0jEM3Oca3uX0NjAsImV4cCI6MTc0ODI0MsQCM80.10us0NxwBG1gD8dahv9nDjQd_AgBByyygLiXGz-e"
  ]
}
```

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



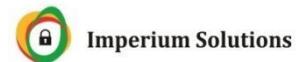
15. Concurrent Login

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173/
Observation/ Vulnerability title	Concurrent login vulnerabilities arise when a system allows a user to be logged in from multiple devices or sessions simultaneously without any restrictions or proper controls. While some applications may require users to log out from one device before logging in from another, systems without restrictions on concurrent logins may introduce a variety of security issues.
Detailed observation / Vulnerable point	Multiple devices or sessions might allow attackers to gain persistent access even if one session is closed.
CVE/CWE	CWE-693
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

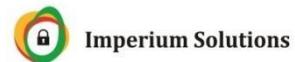


Recommendation	Implement a policy to allow only a single active session per user at a time (or a limited number of sessions). This can help prevent multiple logins and control access to the user account more securely.
Reference	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web Application Security Testing/06-Session Management Testing/11-Testing for Concurrent Sessions
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a web browser displaying two identical instances of an 'Admin Dashboard' page. The URL in the address bar is '44.209.151.89:5173/admin-dashboard' and both instances are marked as 'Not secure'. The dashboard features a film reel background. It shows summary statistics: 'Total Bookings 10' in a blue box and 'Rejected Applications 10' in a red box. There are also links for 'All Bookings', 'Payment Details', and 'Calender'. A red box highlights the URL in the address bar of both windows. Another red box highlights the 'Not secure' message in the browser's status bar.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

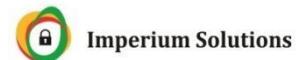


16: Lack of Phone number Verification

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	Lack of phone number verification occurs when an application or system does not validate or confirm the phone number provided by the user during account registration, account recovery, or other processes. This verification typically involves sending a one-time passcode (OTP) or verification code to the phone number to confirm its ownership.
Detailed observation / Vulnerable point	Attackers can create fake or fraudulent accounts or bypass account recovery processes if they can guess or manipulate the phone number.
CVE/CWE	CWE-284
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Period: Period: 14th May 2025 – 17th May 2025

Recommendation	When users enter a phone number, send a one-time passcode (OTP) to that number. The user must then enter the correct OTP to verify ownership of the phone number.
Reference	https://cwe.mitre.org/data/definitions/345.html
New or Repeat observation	New Observation
References to evidences / Proof of Concept	<p>The screenshot shows a POST request to '/api/v1/user/register' with the following JSON body:</p> <pre> 1 POST /api/v1/user/register HTTP/1.1 2 Host: 44.209.151.89:5173 3 Content-Length: 100 4 Accept: / 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Origin: http://44.209.151.89:5173 8 Referer: http://44.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US, en;q=0.9 11 Connection: close 12 13 { "name": "\\\\">\", "email": "xalem5003@ahashab.com", "password": "123456", "termsAccepted": true, "phoneNo": "0000000000" } </pre> <p>The response is a 201 Created status with the following JSON data:</p> <pre> 1 : HTTP/1.1 201 Created 2 3 Access-Control-Allow-Origin: * 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 384 6 ETag: W/"100-8MUVOpewW/FH6NaubVgE3tH+Y" 7 Date: Fri, 16 May 2025 13:49:31 GMT 8 Connection: close 9 10 { "message": "User registered successfully", "user": { "_id": "6fb73734511e54d0c740e458c3", "name": "\\\\">\", "email": "xalem5003@ahashab.com", "phoneNo": "0000000000", "date": "2025-05-16T13:49:31.000Z" }, "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleCiywQjOiz2c0t3Meq1NWE2NmXK eHCUd1mUy7mLcijpYXQlclK3HbDzso2k3NjKalev4cc1SMt0001CMsc2MK0..esGhoJQ -vyp155BaQ-WjOFIC1d62t8L1X65CH2D3w" } </pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



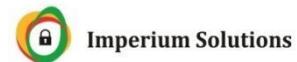
17: Clickjacking Attack

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	In a clickjacking attack, the attacker embeds a transparent frame (iframe) or element over a legitimate page. The user might think they are clicking a button or link on the page, but in reality, they are interacting with the transparent, hidden element underneath. The attacker can then perform malicious actions on behalf of the user without their knowledge.
Detailed observation / Vulnerable point	Users might unknowingly perform harmful actions, such as liking or sharing something on social media, making purchases, or sending sensitive information.
CVE/CWE	CWE-1021
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

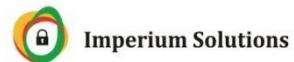


Recommendation	The X-Frame-Options HTTP header prevents your content from being embedded into an iframe. This can block clickjacking attacks by disallowing your page from being embedded on malicious sites.
Reference	https://owasp.org/www-community/attacks/Clickjacking
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a web browser window. The address bar shows a warning: "Not secure 44.209.151.89:5173/login". The main content area displays the login page for "Odisha Film Development Corporation Ltd." (A Government of Odisha Undertaking). Overlaid on this is a smaller window titled "Clickjacking Test v1.0" which also features the same logo and text. The entire screenshot is set against a large red background.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



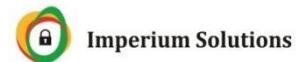
18: Exposed Directory File

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	When the server is misconfigured and reveals a list of files within a directory without restrictions, allowing attackers to browse and potentially download files.
Detailed observation / Vulnerable point	Attackers can view and download sensitive files, potentially gaining access to critical application configurations, database information, or source code.
CVE/CWE	CWE-548
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low
Recommendation	Disable directory listing on the web server (e.g., Apache, Nginx). This prevents attackers from viewing the contents of directories that do not have an index file (e.g., index.html, index.php).

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Reference	https://www.acunetix.com/vulnerabilities/web/directory-listings/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a web browser displaying a receipt. The header reads "The Orissa Film Development Corporation Ltd." with an address "CHALACHITRA BHAWAN, BUXI BAZAR, CUTTACK-753 001". It shows a reference number "M.R. No. 2517451744" and a date "Date : 14/05/2025". The body of the receipt states: "RECEIVED with thanks from M/s. Koustav Dream works Pvt Ltd of Bhubaneswar a sum of Rupees Eleven Thousand Eight Hundred only, Ref. No 2517451744 Dated on 14/05/2025 against / our Bill Letter No. od/22/321212/ on behalf of BANK OF BARODA Bank in Full on account of CBFC SCREENING OF GHAMAGHOT (Corporation Ltd undertaking)." Below this, it says "Rs. 11800/-" and includes a note: "** This is a computer generated receipt and does not require any signature **".

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



19: Outdated Component Used

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	An Outdated Component Used vulnerability occurs when an application relies on outdated software libraries, frameworks, or components that no longer receive security patches or updates. These components might contain known vulnerabilities that attackers can exploit, and using them can leave an application exposed to attacks.
Detailed observation / Vulnerable point	Attackers can exploit known vulnerabilities in outdated components to gain unauthorized access, execute arbitrary code, or perform other malicious activities.
CVE/CWE	CWE-1104
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



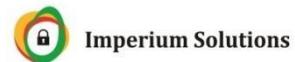
Period: Period: 14th May 2025 – 17th May 2025

Recommendation	Ensure that all components (e.g., libraries, frameworks, APIs) are updated to the latest stable version that has received security patches.
Reference	<p>https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/</p>
New or Repeat observation	New Observation
References to evidences / Proof of Concept	<pre> nmap -sC -sV -T4 -O ec2-44-209-151-89.compute-1.amazonaws.com (44.209.151.89) Nmap scan report for ec2-44-209-151-89.compute-1.amazonaws.com (44.209.151.89) Host is up (0.25s latency). Not shown: 996 filtered ports (no-response) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.9.1p1 Ubuntu 3ubuntu1.11 (Ubuntu Linux; protocol 2.0) vulners: _ cpe:/a:openbsd:openssh:7.9.1p1: 52E696B4-DBD6-57FA-BF6E-D9B2219D827A 9.8 https://vulners.com/githubexploit/52E696B4-DBD6-57FA-BF6E-D9B2219D827A *EXPLOIT* 33DE23F7-98E0-57F5-80FA-81AA66D1340 9.8 https://vulners.com/githubexploit/33DE23F7-98E0-57F5-80FA-81AA66D1340 *EXPLOIT* PACKETSTORM:190587 8.1 https://vulners.com/packetstorm/PACKETSTORM:190587 *EXPLOIT* PACKETSTORM:179290 8.1 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT* F9E589E9-5E4C-5350-A159-625B2E803F 8.1 https://vulners.com/githubexploit/F9E589E9-5E4C-5350-A159-625B2E803F *EXPLOIT* F9391437-9287-5869-93F1-657DF1CE59 8.1 https://vulners.com/githubexploit/F9391437-9287-5869-93F1-657DF1CE59 *EXPLOIT* F58A5C82-2174-586F-9CA9-4C47F0F1085B 8.1 https://vulners.com/githubexploit/F58A5C82-2174-586F-9CA9-4C47F0F1085B *EXPLOIT* EFD615F0-8F17-5471-AA83-0F491FD497AF 8.1 https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF *EXPLOIT* EC20B9C2-6857-5848-846A-A9F430D13EB 8.1 https://vulners.com/githubexploit/EC20B9C2-6857-5848-846A-A9F430D13EB *EXPLOIT* E813CB06-BC93-5F14-A210-A0C85A1D8572 8.1 https://vulners.com/githubexploit/E813CB06-BC93-5F14-A210-A0C85A1D8572 *EXPLOIT* E660E1AF-7A87-57E2-AEEF-C41E41FF7CD 8.1 https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-C41E41FF7CD *EXPLOIT* E543E274-C20A-582A-8F8E-F8E3F381C345 8.1 https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345 *EXPLOIT* E34FC0CD-236B-5A4C-901C-BE83E557 8.1 https://vulners.com/githubexploit/E34FC0CD-236B-5A4C-901C-BE83E557 *EXPLOIT* E508060A-9080-5845-BE15-27795E 8.1 https://vulners.com/githubexploit/E508060A-9080-5845-BE15-27795E *EXPLOIT* DC473889-B477-57F4-B016-00780540B89 8.1 https://vulners.com/githubexploit/DC473889-B477-57F4-B016-00780540B89 *EXPLOIT* DC473885-F54C-5F74-BADF-0175A480C01D 8.1 https://vulners.com/githubexploit/DC473885-F54C-5F74-BADF-0175A480C01D *EXPLOIT* D85F0898-DB96-5585-B8D2-2201980F3360 8.1 https://vulners.com/githubexploit/D85F0898-DB96-5585-B8D2-2201980F3360 *EXPLOIT* D572250A-BE94-501D-90C4-14A6C9C0AC47 8.1 https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0AC47 *EXPLOIT* D1E049F1-393B-552D-80D1-675022B26911 8.1 https://vulners.com/githubexploit/D1E049F1-393B-552D-80D1-675022B26911 *EXPLOIT* CVE-2024-6387 8.1 https://vulners.com/cve/CVE-2024-6387 CFEBF7AF-651A-5302-80B8-F8146D5B33A6 8.1 https://vulners.com/githubexploit/CFEBF7AF-651A-5302-80B8-F8146D5B33A6 *EXPLOIT* </pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



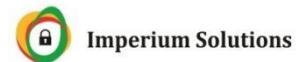
20: Functionality Not Working

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	A clickable element like a button or link doesn't trigger the expected action. A series of processes or steps in an application do not proceed as expected.
Detailed observation / Vulnerable point	When key functionality does not work, users may get frustrated, leading to a poor user experience. Non-functional features can directly impact business processes, such as losing the ability to process transactions or sign up users.
CVE/CWE	CWE-802
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

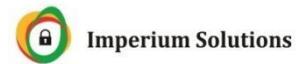


Recommendation	Conduct unit testing, integration testing, and user acceptance testing (UAT) to ensure that all features are functioning as expected in different environments and scenarios.
Reference	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/classification/cwe-22/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	A screenshot of a web browser displaying the login page for The Odisha Film Development Corporation Ltd. The page features the Odisha state emblem and the text "ଓଡିଶା ଚଳିତ୍ ରମ୍ୟନ ନିଗମ ଲିୟ." (The Odisha Film Development Corporation Ltd.) and "(A Government of Odisha Undertaking)". The login form includes fields for "Email" and "Password", a "Remember me" checkbox, and a "Sign in" button. A red box highlights the "Not secure" warning in the address bar. To the right of the login form is a red banner with the text "Your Theatre Awaits" and "Login to cue your next screen where your vision lights up the big screen".

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

A screenshot of a web browser displaying the "Contact Us" page of the Odisha Film Development Corporation website. The URL in the address bar is "Not secure 44.209.151.89:5173/contact-us". The page contains three input fields: the first has the value ">", the second has "coo2@mail.com", and the third has "<script>alert(xss)</script>". Below these fields is a red button labeled "Send Message". To the right of the form is a map of a city area with several locations marked, including "Chalachitra Bhawan" and "Mission Shakti Cafe". A callout box for "Chalachitra Bhawan" provides address details: "PVR#461 Buxi Bazaar, Cuttack, Odisha 753001" and a rating of "3.8 ★★★★ ★ 17 reviews".

Contact Us

I'>

coo2@mail.com

<script>alert(xss)</script>

Send Message

Chalachitra Bhawan
PVR#461 Buxi Bazaar, Cuttack,
Odisha 753001
3.8 ★★★★ ★ 17 reviews
View larger map

Directions

Mission Shakti Cafe

Buxi Bazar Shish Mahal

Stewart School

Gopabandhu Park

RT E COLLEGE

Pata Pata Rd

Mission Rd 4

Mission Rd

Babu Bazar Rd

Dron Lin

nisha's

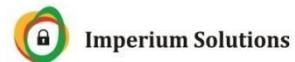
Anand Sports

Chalachitra Bhawan

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

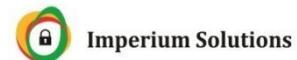


21 : Allow origin Allow origin Misconfiguration

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	The Allow-Origin Misconfiguration vulnerability is typically caused by an incorrect configuration of the CORS (Cross-Origin Resource Sharing) policy in web applications. CORS is a security feature implemented by web browsers to restrict web pages from making requests to domains different from the one that served the web page. It's a mechanism that allows a server to specify which domains can access its resources.
Detailed observation / Vulnerable point	Malicious websites can access sensitive user data (e.g., authentication tokens, user information) from the vulnerable web application, leading to data theft or information leakage.
CVE/CWE	CWE-693
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report



Period: Period: 14th May 2025 – 17th May 2025

Recommendation	Avoid using the wildcard (*) for the Access-Control-Allow-Origin header. If the origin must be dynamic (i.e., vary based on the request), implement logic to check the Origin header and ensure it matches a whitelist of trusted origins.
Reference	https://www.acunetix.com/vulnerabilities/web/misconfigured-access-control-allow-origin-header/
New or Repeat observation	New Observation
References to evidences / Proof of Concept	<pre> Request Pretty Raw Hex ⌂ ⓘ ⓘ ⓘ 1 POST /api/v1/user/login HTTP/1.1 2 Host: 144.209.151.89:3000 3 Content-Length: 78 4 Accept: / 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Origin: http://144.209.151.89:5173 8 Referer: http://144.209.151.89:5173/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US,en;q=0.9 11 Connection: close 12 13 { 14 "identifier": "mdodofil@gmail.com", 15 "password": "OPDC@admin", 16 "rememberMe": false 17 } Response Pretty Raw Hex Render ⌂ ⓘ ⓘ ⓘ 1 HTTP/1.1 200 OK 2 Date: Fri, 16 May 2025 07:11:00 GMT 3 Access-Control-Allow-Origin: * 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 340 6 ETag: W/"154-a/x6GnMadgOp66nHsVrTC9h4c" 7 Date: Fri, 16 May 2025 07:11:00 GMT 8 Connection: close 9 10 { 11 "message": "Login successful", 12 "user": { 13 "id": "80C43ad6cc098234a87a49e9", 14 "name": "cerce", 15 "email": "mdodofil@gmail.com", 16 "phoneNo": "+712305165", 17 "role": "ADMIN" 18 }, 19 "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVOJB...ey3le2V9WQjOliODIDMCE3N8jMDA4MjM0Y2gjYX5029LIC0jyXQLojE3NcGnsxK0NjAsImV4cCI6MjcyODI0MsQCM8D.1ouuMhszBGZgOs8ahbv9B2jXQ4_AgBByyy8gLLXGZ-B" 20 } </pre>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



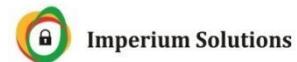
22 : Old Password Set as New Password

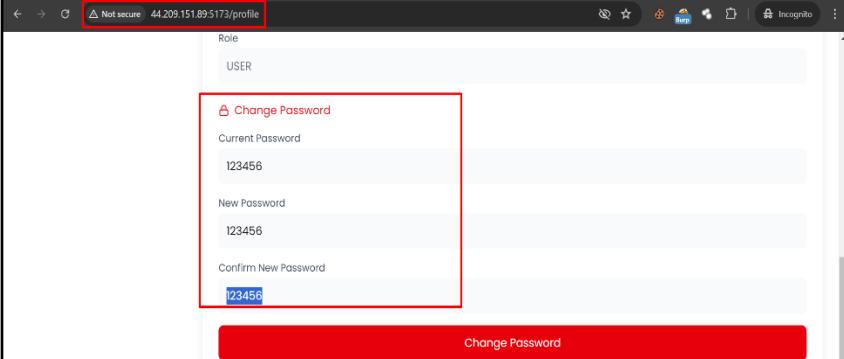
Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	The Old Password Set as New Password vulnerability occurs when a user can set their old password as their new password during the password change process. This happens because the application does not properly validate that the new password is different from the current password, which allows the user to essentially keep their old password.
Detailed observation / Vulnerable point	An attacker who gains access to an account will not be forced to change the password if they exploit this vulnerability. They could retain full control of the account, even if the user or the system attempts to enforce a password change.
CVE/CWE	CWE-640
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025

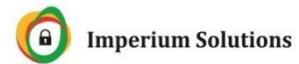


Recommendation	When users attempt to change their password, ensure that the new password is different from the old password. This is a simple yet crucial validation check.
Reference	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web Application Security Testing/04-Authentication Testing/09-Testing for Weak Password Change or Reset Functionalities
New or Repeat observation	New Observation
References to evidences / Proof of Concept	

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

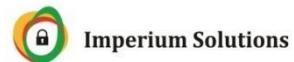
Period: Period: 14th May 2025 – 17th May 2025

A screenshot of a web browser window showing a password change interface. The URL bar at the top indicates the site is not secure (44.209.151.89:5173/profile). The page itself shows a "Role" dropdown set to "USER". Below it is a "Change Password" section with fields for "Current Password" (containing "123456") and "New Password" (containing four dots). A "Confirm New Password" field below it also contains four dots. At the bottom of the form are two red buttons: "Change Password" and "Save Changes". A green success message box is visible in the upper right corner stating "Password changed successfully." with a checkmark icon.

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



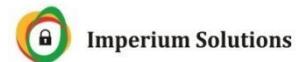
23: Unwanted http Method Enable

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	The Unwanted HTTP Methods Enabled vulnerability occurs when an application or web server is configured to accept HTTP methods that are unnecessary or unsafe, such as DELETE, PUT, TRACE, or OPTIONS, for endpoints that should only support GET or POST. This misconfiguration can expose the application to a variety of attacks.
Detailed observation / Vulnerable point	If a server accepts HTTP methods that should not be available to the public, attackers could modify or delete sensitive resources. For example, if an attacker sends a DELETE request to a vulnerable resource endpoint, they might be able to remove critical data.
CVE/CWE	CWE-444
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



Recommendation	Review the HTTP methods allowed by your web server and application, and disable any that are unnecessary for the functioning of the application.
Reference	<p>https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/06-Test_HTTP_Methods</p>
New or Repeat observation	New Observation
References to evidences / Proof of Concept	<p>The screenshot shows a browser developer tools Network tab with two panels: Request and Response. The Request panel shows a PUT request to 'PUT /api/v1/user/updateUser HTTP/1.1' with various headers. The Response panel shows a successful response (HTTP/1.1 200 OK) with headers like 'X-Powered-By: Express', 'Access-Control-Allow-Origin: *', and 'Content-Type: application/json; charset=utf-8'. The response body is a JSON object containing success: true, message: "User updated successfully", user: {id: 60273451166fd7c740e45b0c1, name: "test user", email: "telma5803@hashab.com", profilePic: "000000000000", profilePicUrl: "https://example.com/default-profile.png", createdAt: "2025-05-16T12:49:21.516Z", updatedAt: "2025-05-16T14:44:05.914Z", v: 0}.</p>

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



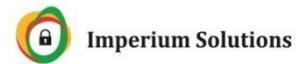
24 : Open port

Affected Asset i.e. IP / URL / Application etc.	http://44.209.151.89:5173//
Observation/ Vulnerability title	An Open Port vulnerability occurs when unnecessary or unsecured network ports are left open on a system, device, or server. These open ports can be exploited by attackers to gain unauthorized access to the system, steal sensitive data, or perform malicious activities.
Detailed observation / Vulnerable point	If an attacker can exploit an open port, they might gain unauthorized access to the system, bypassing security controls. For example, an open SSH port might allow an attacker to brute force a login and gain access to a server.
CVE/CWE	CWE-200
Control Objective	NA
Control Name	NA
Audit Requirement	NA
Severity	Low
Recommendation	Identify and close any open ports that are not needed for legitimate purposes. This includes ports related to unused services, outdated

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.

Web Application Audit Report

Period: Period: 14th May 2025 – 17th May 2025



	protocols, or any service that does not need to be exposed to the internet.																									
Reference	https://mas.owasp.org/MASWE/MASVS-NETWORK/MASWE-0051/																									
New or Repeat observation	New Observation																									
References to evidences / Proof of Concept	A screenshot of a NetworkMiner tool interface. On the left, there's a tree view with 'OS' and 'Host' expanded, showing 'ec2-44-209-15'. On the right, a table displays network traffic details: <table border="1"><thead><tr><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr></thead><tbody><tr><td>22</td><td>tcp</td><td>open</td><td>ssh</td><td>OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)</td></tr><tr><td>80</td><td>tcp</td><td>closed</td><td>http</td><td></td></tr><tr><td>443</td><td>tcp</td><td>closed</td><td>https</td><td></td></tr><tr><td>3000</td><td>tcp</td><td>open</td><td>http</td><td>Node.js Express framework</td></tr></tbody></table>	Port	Protocol	State	Service	Version	22	tcp	open	ssh	OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)	80	tcp	closed	http		443	tcp	closed	https		3000	tcp	open	http	Node.js Express framework
Port	Protocol	State	Service	Version																						
22	tcp	open	ssh	OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)																						
80	tcp	closed	http																							
443	tcp	closed	https																							
3000	tcp	open	http	Node.js Express framework																						

This document and the information contained within generated by Imperium Solutions, are intended for the use of Client personnel only. The information contained herein is confidential and is for use by the assigned personnel only. General circulation and reproduction in any form by unauthorized personnel or firm is prohibited.