SECUPROS

CYBER SECURITY REPORT

Client Name:
Web Application:

Prepared By: SECUPROS
Report Date: 06-02-2026

VAPT REPORT DETAILS:

Report Release Date	06-02-2026
Type of VAPT	Web Application VAPT
Type of VAPT Report	First test report
Period	February 2026

DOCUMENT CONTROL:

Document Title	Web Application VAPT
Document ID	Secupros/VAPT/feb 2026
Document Version	V1
Prepared by	Mr. Mohammed K
Reviewed by	Mr. Rajan Kumar
Approved by	Mr. Adithya

DOCUMENT CHANGE HISTORY:

Version	Date	Remarks / Reason of Change
N/A	N/A	N/A

DOCUMENT DISTRIBUTION LIST:

S.NO	Name	Organization	Designation	Email ID
1				

TABLE OF CONTENTS

1.0 INTRODUCTION – WEB APPLICATION VAPT: 4
1.1 ENGAGEMENT SCOPE: 4
1.2 DETAILS OF THE VAPT PENTEST TEAM: 4
1.3 VAPT TEST ACTIVITIES AND TIMELINES: 5
1.4 VAPT METHODOLOGY AND CRITERIA: 5
1.5 VAPT CRITERIA: 5
2.0 TOOLS/SOFTWARE USED: 6
3.0 EXECUTIVE SUMMARY (VAPT SEVERITY ISSUES AS PER CVSS/CWE) 7
4.0 DETAILED OBSERVATIONS: 11

1.0 INTRODUCTION – WEB APPLICATION VAPT:

Web Application Vulnerability Assessment and Penetration Testing (VAPT) is a security testing process performed to identify, analyze, and validate vulnerabilities in web-based applications. It combines vulnerability assessment techniques to discover security weaknesses with penetration testing methods that simulate real-world attack scenarios to evaluate their actual impact.

The objective of this assessment is to ensure that the web application is adequately protected against threats such as unauthorized access, data breaches, and service disruption. The testing covers key areas, including authentication, session management, input validation, APIs, and server-side security, and is conducted in alignment with industry-recognized standards such as OWASP Top 10, NIST, and ISO/IEC 27001.

1.1 Engagement Scope:

S.No	Asset Description	Criticality of Asset	Internal IP Address	URL/Endpoint	Public IP Address	Hash Value (in case of applications)	Version (in case of applications)
1	Web Application –	High	N/A		N/A	N/A	N/A
2	Web Application –	High	N/A		N/A	N/A	N/A

1.2 Details of the VAPT Pentest Team:

S.NO	Name	Designation	Email ID	Certifications
1	Mohammed	Cyber Security Analyst	mohammed.kanniyakan@secupros.com	CEH
2	Upendra	Cyber Security Analyst	rapuri.upendra@secupros.com	CEH

1.3 VAPT Test Activities and Timelines:

VAPT Phase	Timeline
Scoping	29-01-2026
Kickoff	30-01-2026
Vulnerability assessment & exploitation	31-01-2026
Documentation	04-02-2026
Report generation	06-02-2026

1.4 VAPT Methodology and Criteria:

Vulnerability Assessment and Penetration Testing (VAPT) is a structured, risk-based security testing process used to identify, validate, and assess security weaknesses in applications, systems, and networks in alignment with standards such as OWASP, NIST, PTES, ISO/IEC 27001, and SOC 2. It involves defined scoping and authorization, information gathering, vulnerability identification through automated and manual techniques, controlled exploitation to confirm real-world impact, risk-based severity classification using CVSS and business impact, and comprehensive reporting with remediation recommendations, followed by re-testing to verify effective closure of identified vulnerabilities.

1.5 VAPT Criteria:

Severity Classification:

Severity	Description
⚠ Critical	Full system compromise, sensitive data exposure
⚠ High	Significant security risk, exploitable remotely
⚠ Medium	Limited exploitation, partial impact
⚠ Low	Minor issues, informational findings
ⓘ Informational	No direct risk, best-practice gaps

2.0 TOOLS/SOFTWARE USED:

S. No	Name of Tool/Software	Version
1	Nmap	7.90
2	Custom Scripts	-
3	Burp Suite Professional	2025.4
4	Nuclei	3.7.0
5	Fuff	2.1.0

3.0 EXECUTIVE SUMMARY (VAPT SEVERITY ISSUES AS PER CVSS/CWE)

Severity	**Count**
Critical	1
High	5
Medium	9
Low	5
Info	0
Total	**20**

S.NO	Affected asset	Vulnerability title	CVE/CWE	Severity	Vulnerability history
1		Application Accessible Over Insecure HTTP (HTTPS Not Enforced).	CWE-319 – Cleartext Transmission of Sensitive Information CWE-523 – Unprotected Transport of Credentials	⚠ Critical	New
2		Stored Cross-Site Scripting (XSS) in Transporter Management Fields	CWE-79 – Improper Neutralization of Input During Web Page Generation (Cross-Site Scripting) CWE-116 – Improper Encoding or Escaping of Output	⚠ High	New
3		Business Logic Flaw – Transporter Record Overwrite / Data Integrity Issue	CWE-840 – Business Logic Errors CWE-20 – Improper Input Validation	⚠ High	New
4		Business Logic Flaw – Duplicate Transporter Records Allowed	CWE-840 – Business Logic Errors CWE-20 – Improper Input Validation	⚠ High	New
5		Sensitive Information Exposure – Credentials Sent in Plain Text Within Request	CWE-319 – Cleartext Transmission of Sensitive Information CWE-522 – Insufficiently Protected Credentials	⚠ High	New
6		Sensitive Information Exposure – Credentials Sent in Plain Text Within Request	CWE-319 – Cleartext Transmission of Sensitive Information CWE-522 – Insufficiently Protected Credentials	⚠ High	New
7		IIS Management Service (Port 8172) Exposed to the Internet	CWE-284 – Improper Access Control CWE-16 – Configuration	⚠ Medium	New
8		Weak TLS Configuration on Exposed IIS Management Service (Port 8172)	CWE-326 – Inadequate Encryption Strength CWE-327 – Use of a Broken or Risky Cryptographic Algorithm	⚠ Medium	New

9		Unrestricted File Upload Allows Arbitrary File Extensions	CWE-434 – Unrestricted Upload of File with Dangerous Type CWE-20 – Improper Input Validation	⚠ Medium	New
10		Authenticated Pages Accessible via Browser Back Button After Logout	CWE-613 – Insufficient Session Expiration CWE-525 – Information Exposure Through Browser Caching	⚠ Medium	New
11		Application Accepts Common / Weak Passwords	CWE-521 – Weak Password Requirements CWE-307 – Improper Restriction of Excessive Authentication Attempts	⚠ Medium	New
12		User Status Toggle Not Reflecting Correctly After Creation	CWE-521: Weak Password Requirements CWE-307: Improper Restriction of Excessive Authentication Attempts	⚠ Medium	New
13		Unrestricted File Upload – File Type Validation Missing in Excel Upload Functionality	CWE-434 – Unrestricted Upload of File with Dangerous Type CWE-20 – Improper Input Validation	⚠ Medium	New
14		Improper Input Length Handling / Potential Application-Level DoS	CWE-20 – Improper Input Validation CWE-400 – Uncontrolled Resource Consumption	⚠ Medium	New
15		Authenticated Pages Accessible via Browser Back Button After Logout	CWE-613 – Insufficient Session Expiration CWE-525 – Information Exposure Through Browser Caching	⚠ Medium	New
16		Web Server Version Disclosure	CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor CWE-16 – Configuration	⚠ Low	New

17	[redacted]	FTP Service Exposed on Production Server	CWE-319 – Cleartext Transmission of Sensitive Information CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor	⚠ Low	New
18	[redacted]	Password Field Missing Autocomplete Attribute	CWE-524 – Use of Cache Containing Sensitive Information CWE-522 – Insufficiently Protected Credentials	⚠ Low	New
19	[redacted]	Lack of Rate Limiting on Login Endpoint for Unauthenticated Requests	CWE-799 – Improper Control of Interaction Frequency CWE-307 – Improper Restriction of Excessive Authentication Attempts	⚠ Low	New
20	[redacted]	Username Enumeration via Distinct Login Error Message	CWE-204 – Observable Response Discrepancy CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor	⚠ Low	New

4.0 DETAILED OBSERVATIONS:

VULNERABILITY ISSUE 1:	Application Accessible Over Insecure HTTP (HTTPS Not Enforced)
Affected URL:	

Description:

During testing, it was observed that the web application is accessible over unencrypted HTTP instead of enforcing HTTPS-only communication. When users access the application using http://, the server does not automatically redirect traffic to a secure https:// connection. This allows data exchanged between the client and server to be transmitted in plain text, which can be intercepted or modified by attackers on the network.

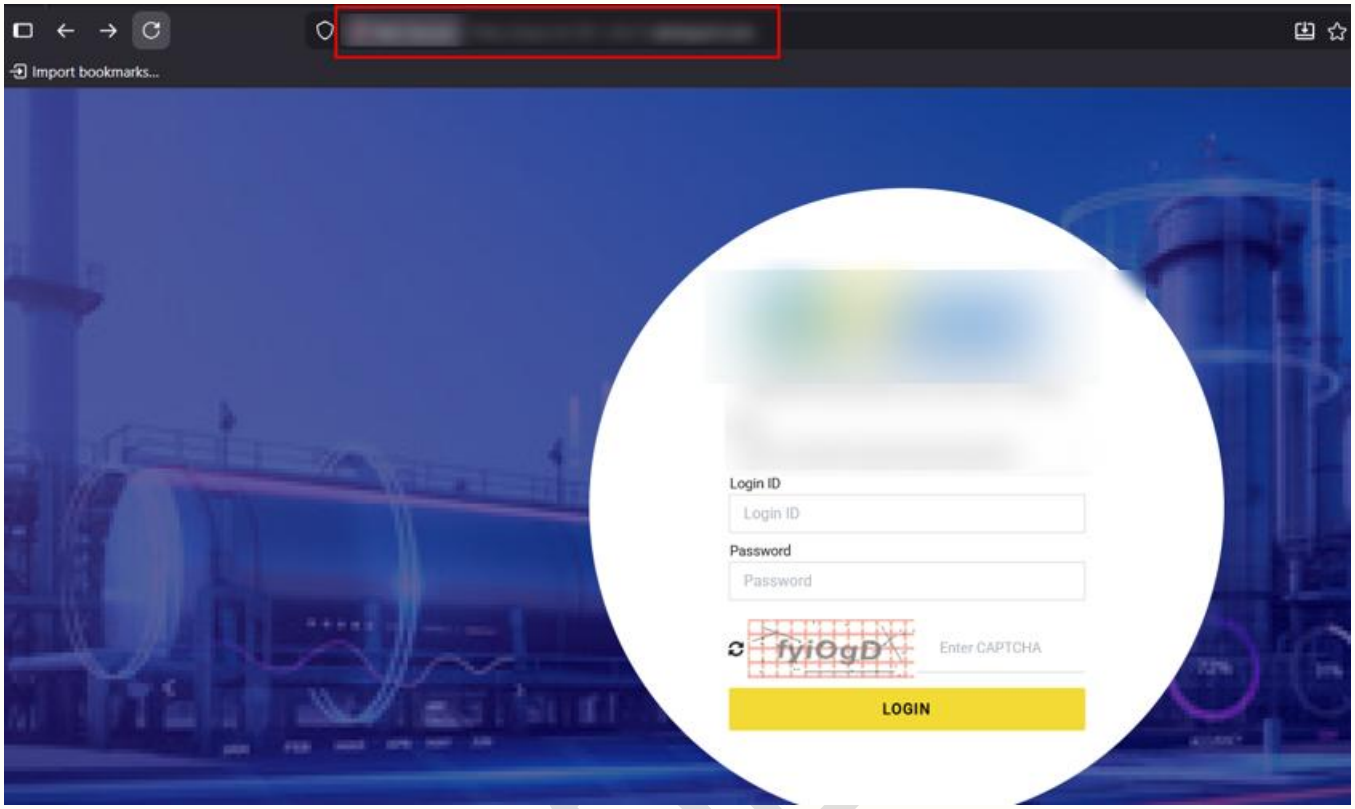
CVE/CWE:	• CWE-319 – Cleartext Transmission of Sensitive Information • CWE-523 – Unprotected Transport of Credentials
Risk Rating:	⚠ Critical
Reference:	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Impact:

- Credentials and session cookies may be exposed over the network.
- Enables Man-in-the-Middle (MITM) attacks.
- Allows attackers to intercept or modify application data.
- Reduces overall confidentiality and integrity of communications

Recommendation:	• Enforce HTTPS-only access across the entire application • Redirect all HTTP requests to HTTPS using server configuration • Ensure a valid SSL/TLS certificate is installed and maintained

Proof of Concept (POC):



VULNERABILITY ISSUE 2:	Stored Cross-Site Scripting (XSS) in Transporter Management Fields
Affected url:	

Description:

During testing of the Transporter Management → Edit Transporter functionality, it was observed that multiple input fields allow the insertion and storage of malicious JavaScript payloads. The injected script is stored in the database and executed automatically when the transporter record is viewed. The payload was observed to execute multiple times, indicating that the unsanitized input is rendered in several locations within the application interface. This confirms a Stored XSS vulnerability, which allows attackers to execute arbitrary JavaScript in the browsers of other authenticated users.

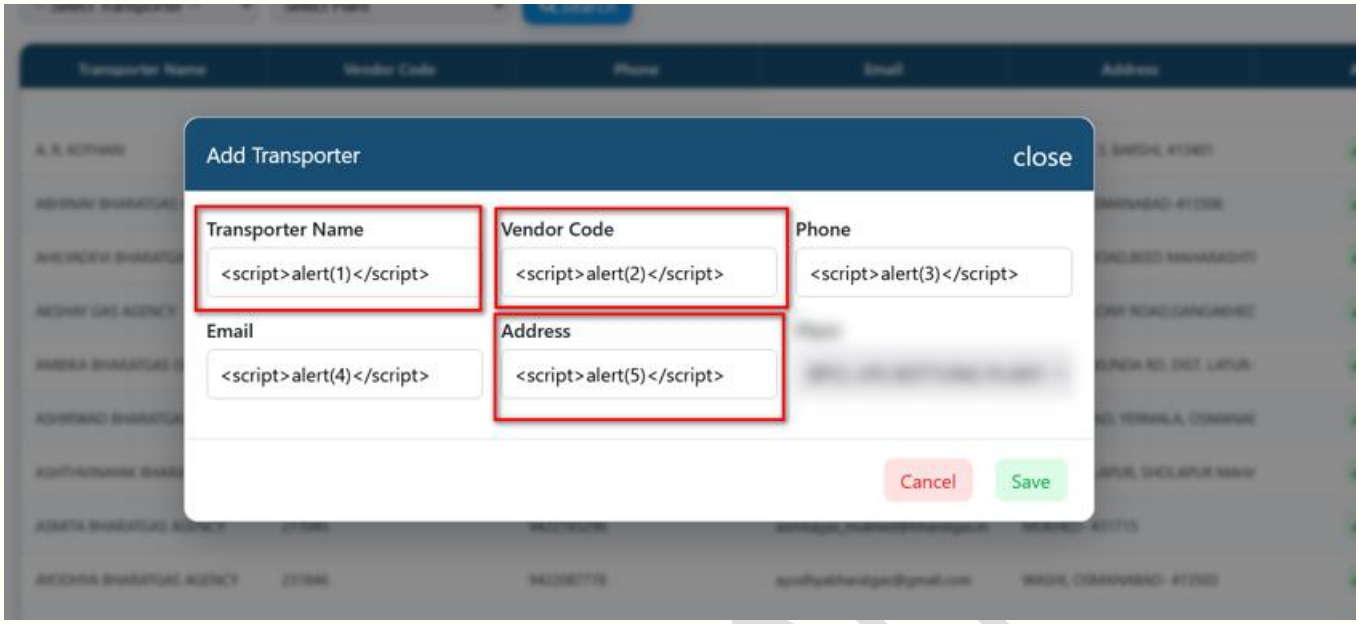
CVE/CWE:	• CWE-79 – Improper Neutralization of Input During Web Page Generation (Cross-Site Scripting) • CWE-116 – Improper Encoding or Escaping of Output
Risk Rating:	⚠ High
Reference:	https://owasp.org/Top10/A03_2021-Injection

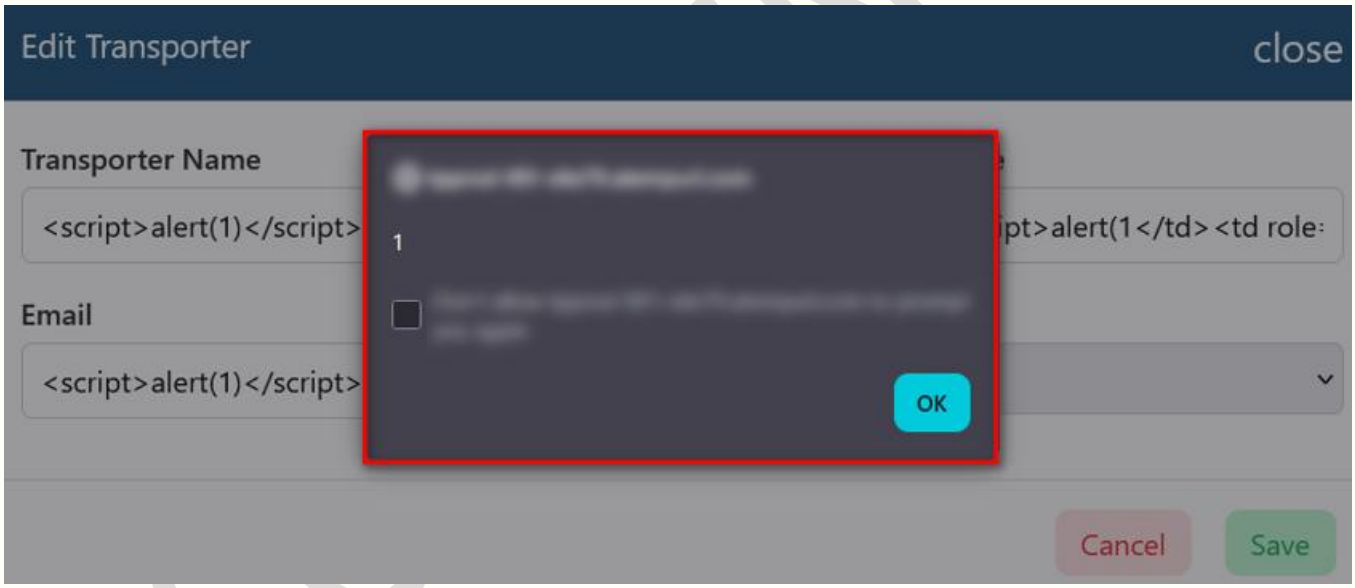
Impact:

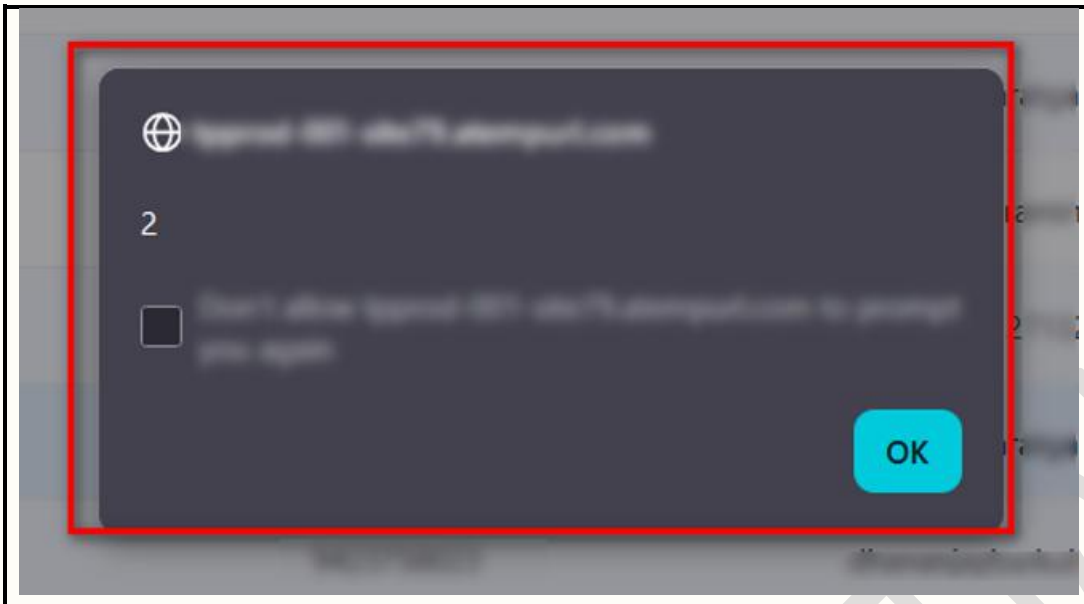
- Execution of arbitrary JavaScript in victim browsers.
- Possible session hijacking / cookie theft.
- Potential credential phishing or keylogging.
- Affects all users who view the manipulated record.
- May lead to full administrative account compromise.

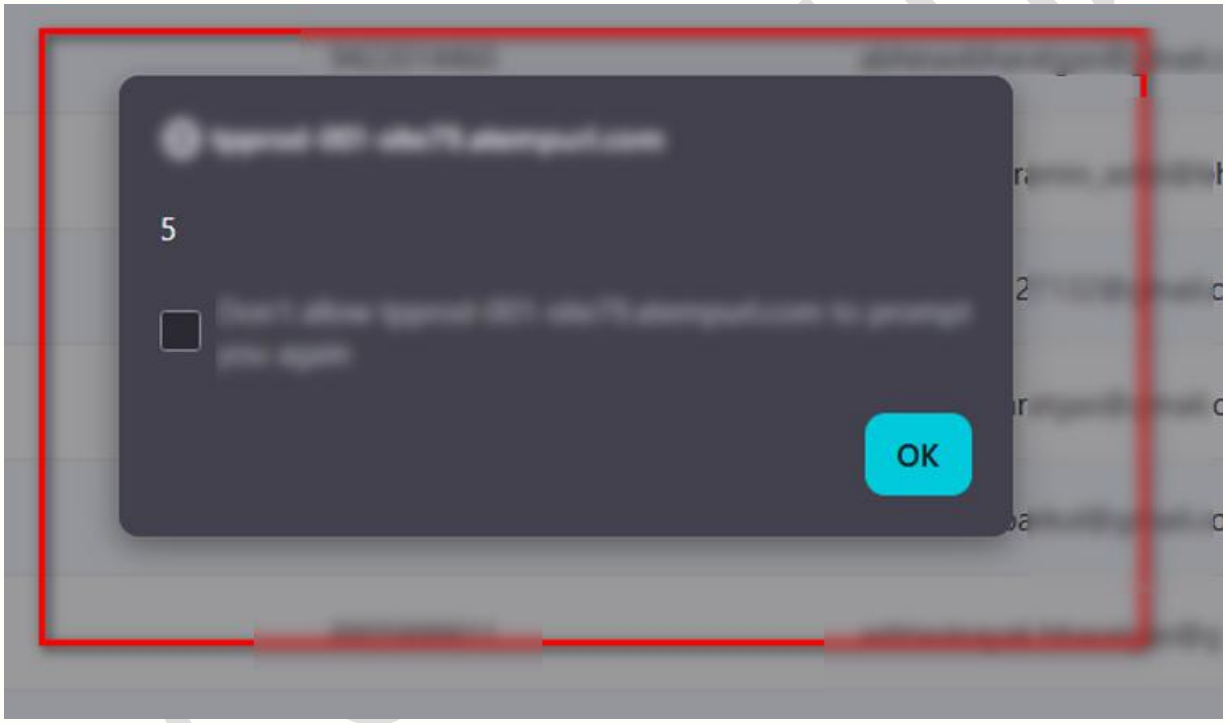
Recommendation:	• Implement server-side sanitization and encoding for all inputs • Escape dynamic content before rendering in HTML • Use allow lists for text fields (letters, numbers, limited symbols)

Proof of Concept (POC):






2
OK


5
OK

VULNERABILITY ISSUE 3:	Business Logic Flow – Transporter Record Overwrite / Data Integrity Issue
Affected Component:	

Description:

The Transporter management functionality allows creation of new transporter records without enforcing proper uniqueness validation or synchronization with existing data. When a new transporter is added, previously existing records may be overwritten, hidden, or not displayed correctly in the listing table. This indicates a failure in business logic validation and improper handling of record integrity between the UI layer and backend database.

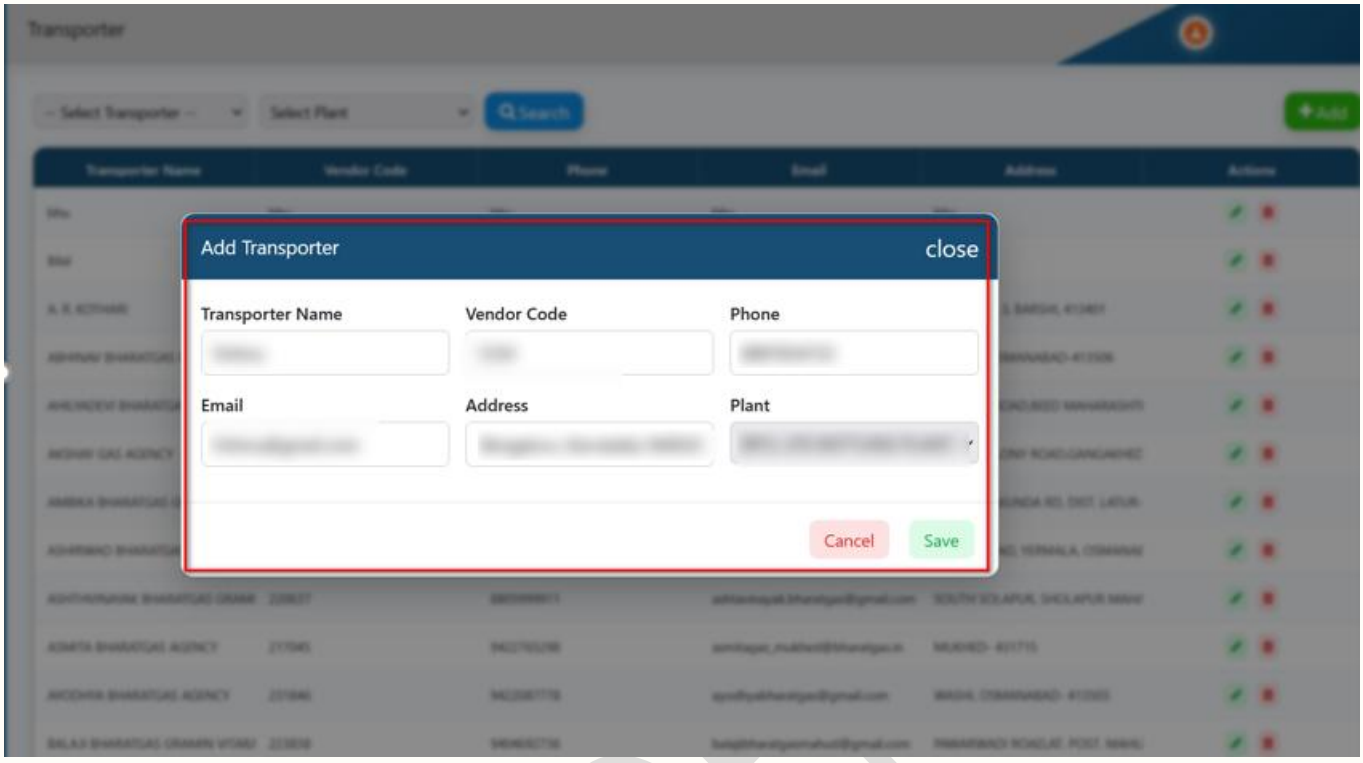
CVE/CWE:	• CWE-840 – Business Logic Errors • CWE-20 – Improper Input Validation
Risk Rating:	⚠ High
Reference:	https://owasp.org/Top10/A04_2021-Insecure_Design

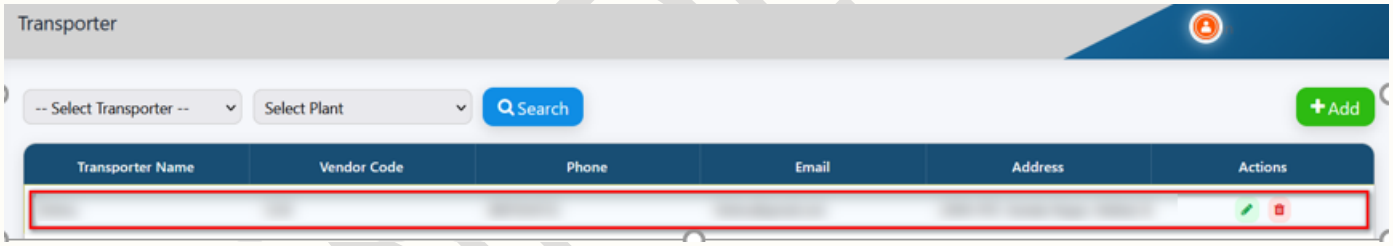
Impact:

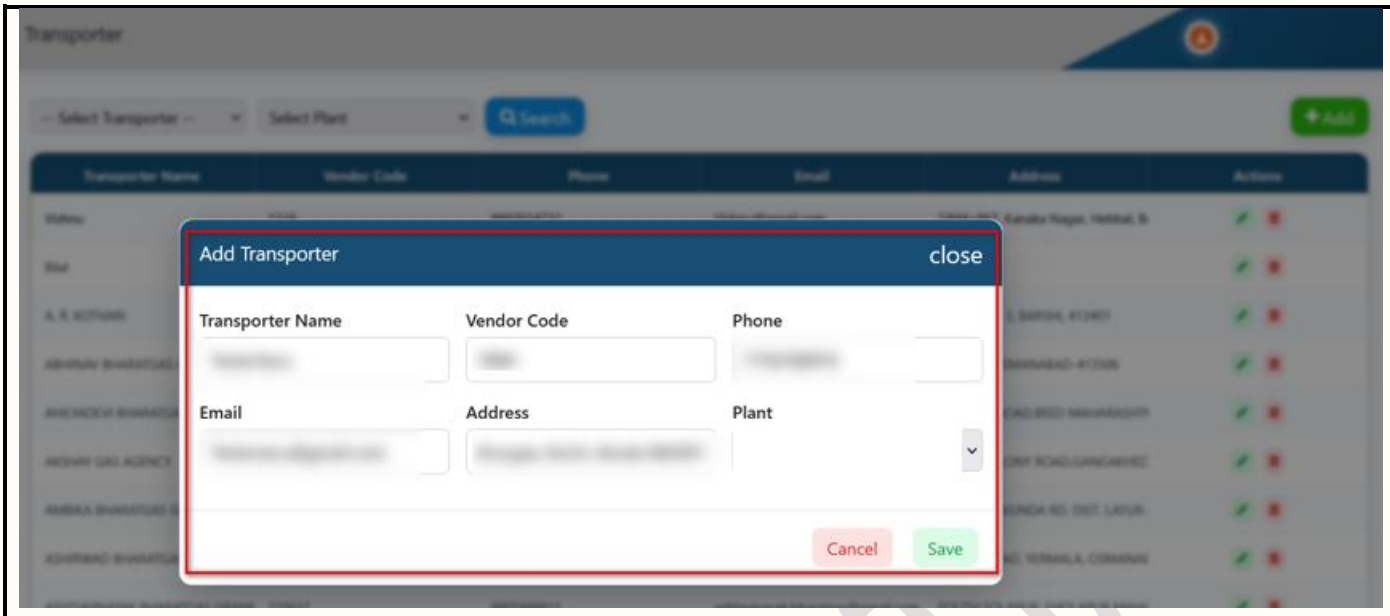
- Loss or corruption of business-critical transporter data.
- Inaccurate operational records and reporting.
- Potential compliance and Test issues due to unreliable data storage.
- Reduced trust in system reliability and data accuracy.

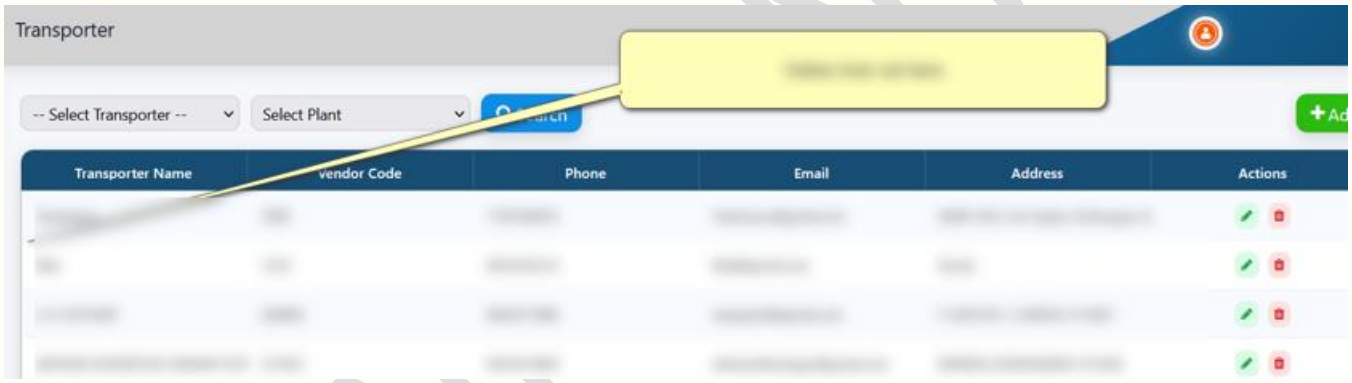
Recommendation:	• Enforce unique constraints on key identifiers such as Vendor Code, Email, or Transporter ID at the database level. • Implement server-side validation to prevent duplicate or conflicting entries. • Ensure proper UI-backend synchronization and refresh logic after save operations. • Add transaction handling and rollback mechanisms to prevent unintended overwrites.

Proof of Concept (POC):









VULNERABILITY ISSUE 4:	Business Logic Flaw – Duplicate Transporter Records Allowed
Affected Component:	

Description:

The Transporter module fails to enforce uniqueness validation on critical fields such as Vendor Code, Phone Number, and Email Address. The system allows multiple transporter records to be created with identical values for these fields, resulting in duplicate entries within the database. This indicates missing or improper business logic validation and weak data integrity controls.

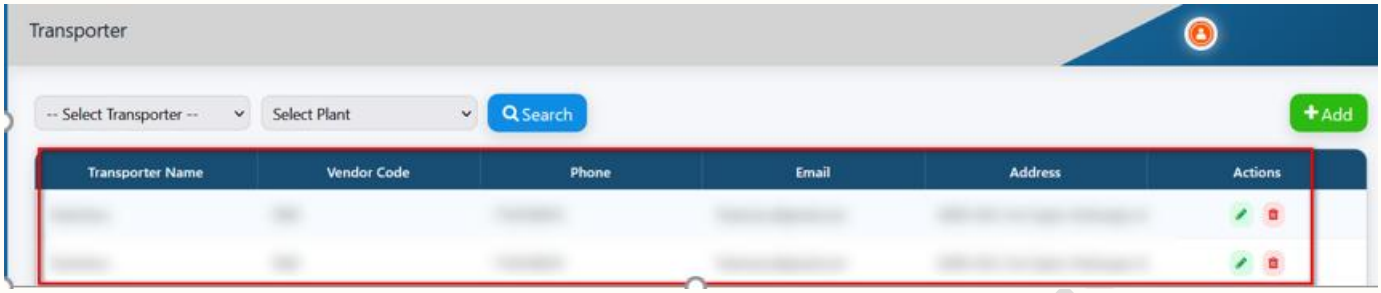
CVE/CWE:	• CWE-840 – Business Logic Errors • CWE-20 – Improper Input Validation
Risk Rating:	⚠ High
Reference:	https://cwe.mitre.org/data/definitions/1287.html

Impact:

- Data integrity compromise due to redundant or conflicting records.
- Reporting and operational inaccuracies.
- Difficulty in identifying legitimate transporter information.
- Increased risk of fraud or misuse of duplicated vendor identities.
- Administrative and Test complications.

Recommendation:	• Implement database-level unique constraints on Vendor Code, Phone Number, and Email fields. • Enforce server-side validation to prevent duplicate submissions regardless of client-side controls. • Display clear user validation messages when duplicates are detected.

Proof of Concept (POC):



VULNERABILITY ISSUE 5:	Sensitive Information Exposure – Credentials Sent in Plain Text Within Request
Affected Component:	

Description:

During the authentication process, the application sends the username and password as plain text parameters in the HTTP request body (e.g., LoginUserName and LoginPassword). This means the raw password value is directly included in the request payload and could be exposed if transport security is downgraded, misconfigured, terminated at an intermediary, or logged by proxies, servers, or monitoring tools.

CVE/CWE:	• CWE-319 – Cleartext Transmission of Sensitive Information • CWE-522 – Insufficiently Protected Credentials
Risk Rating:	⚠ High
Reference:	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

Impact:

- Exposure of credentials in browser history, debugging tools, or proxy logs.
- Increased risk if TLS is terminated at load balancers or inspection gateways.
- Potential leakage through application/server logging or monitoring systems.

Recommendation:	• Client-Side Password Hashing / Encryption
	  ○ Hash or encrypt the password in the browser before sending it to the server.
	  ○ Use strong algorithms such as:
	  ○ SHA-256 / SHA-512 (with salt)
	  ○ RSA encryption (public key)

Proof of Concept (POC):

VULNERABILITY ISSUE 6:	Sensitive Information Exposure – Credentials Sent in Plain Text Within Request
Affected Component:	

Description:

During the authentication process, the application sends the username and password as plain text parameters in the HTTP request body (e.g., LoginUserName and LoginPassword). This means the raw password value is directly included in the request payload and could be exposed if transport security is downgraded, misconfigured, terminated at an intermediary, or logged by proxies, servers, or monitoring tools.

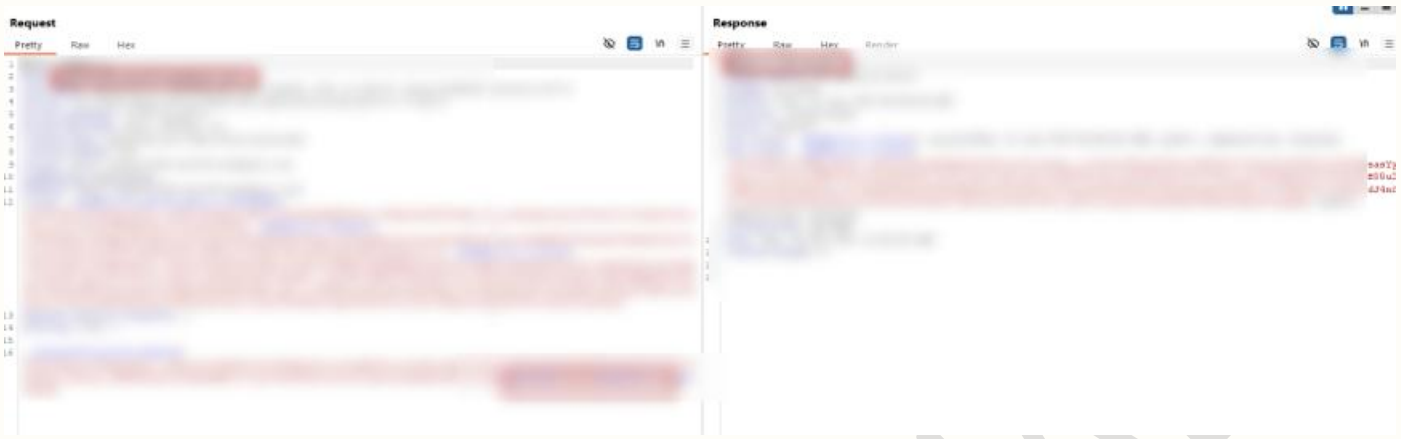
CVE/CWE:	• CWE-319 – Cleartext Transmission of Sensitive Information • CWE-522 – Insufficiently Protected Credentials
Risk Rating:	⚠ High
Reference:	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

Impact:

- Exposure of credentials in browser history, debugging tools, or proxy logs.
- Increased risk if TLS is terminated at load balancers or inspection gateways.
- Potential leakage through application/server logging or monitoring systems.

Recommendation:	• Client-Side Password Hashing / Encryption
	  ○ Hash or encrypt the password in the browser before sending it to the server.
	  ○ Use strong algorithms such as:
	  ○ SHA-256 / SHA-512 (with salt)
	  ○ RSA encryption (public key)

Proof of Concept (POC):



VULNERABILITY ISSUE 7:	IIS Management Service (Port 8172) Exposed to the Internet
Affected Component:	

Description:

During network-level testing, it was observed that port 8172/TCP is open and accessible from the internet. This port is associated with the Microsoft IIS Management Service (WMSvc), which is used for remote administration and deployment of IIS applications. Management services such as WMSvc are not intended to be publicly exposed. Even when authentication is enabled, exposing administrative interfaces to the internet significantly increases the risk of unauthorized access through brute-force attacks, credential compromise, or service misconfigurations.

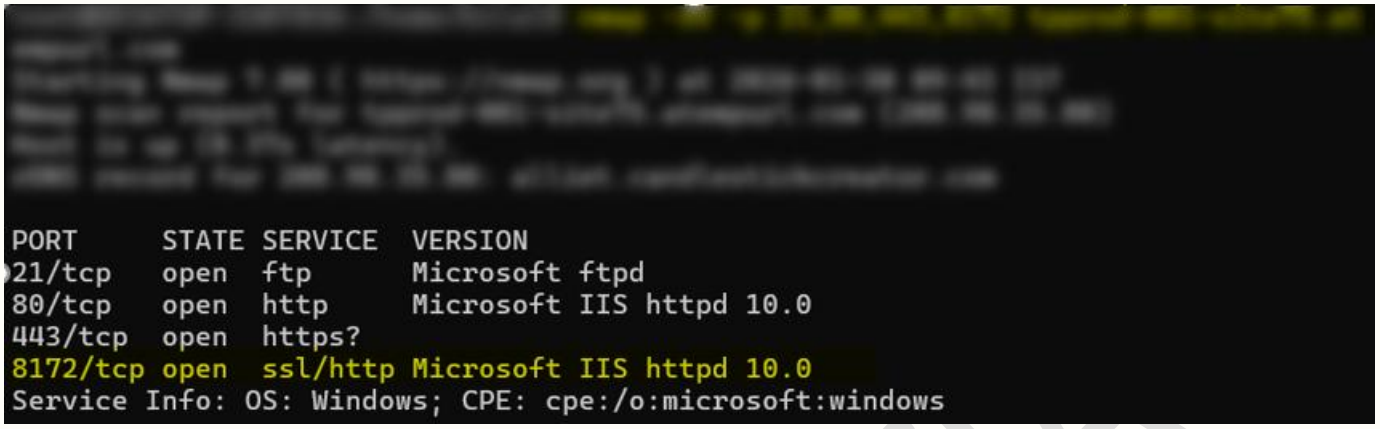
CVE/CWE:	• CWE-284 – Improper Access Control • CWE-16 – Configuration
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A05_2021-Security_Misconfiguration

Impact:

- Exposes a remote administrative service to the internet
- Increases risk of: Brute-force or credential-stuffing attacks, Unauthorized IIS configuration changes, Application deployment or file manipulation
- Management interfaces are high-value targets for attackers

Recommendation:	• Disable the IIS Management Service if it is not required • Restrict access to port 8172 using firewall rules or IP allowlisting • Ensure the service is accessible only from trusted internal networks • Enforce strong authentication and monitor access logs if the service must remain enabled

Proof of Concept (POC):



VULNERABILITY ISSUE 8:	Weak TLS Configuration on Exposed IIS Management Service (Port 8172)
Affected Component:	

Description:

During security testing, it was observed that the IIS Management Service (WMSvc) running on port 8172/TCP is publicly accessible and configured with weak TLS settings. Port 8172 is used for remote IIS administration and Web Deploy operations and is not intended to be exposed to untrusted networks. The risk is further increased by the presence of legacy TLS protocols (TLS 1.0 and TLS 1.1) and weak cipher suites (3DES). While the use of weak TLS settings alone may pose a moderate risk on standard web services, their presence on a publicly exposed administrative interface significantly increases the likelihood and impact of potential attacks.

CVE/CWE:	• CWE-326 – Inadequate Encryption Strength • CWE-327 – Use of a Broken or Risky Cryptographic Algorithm
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A02_2021-Cryptographic_Failures

Impact:

- Exposes a remote administrative service to the internet
- Legacy TLS protocols and weak ciphers increase susceptibility to: Cryptographic downgrade attacks, Traffic decryption under certain conditions
- Administrative interfaces are high-value targets and should be strongly protected
- Compromise of this service could lead to unauthorized IIS configuration changes or deployment actions.

Recommendation:	• Restrict access to port 8172 to trusted internal networks or specific IP addresses • Disable TLS 1.0 and TLS 1.1, and enforce TLS 1.3 or higher • Remove weak cipher suites such as 3DES • Disable the IIS Management Service if remote administration is not required • Monitor and log all administrative access attempts

Proof of Concept (POC):

VULNERABILITY ISSUE 9:	Unrestricted File Upload Allows Arbitrary File Extensions
Affected Component:	

Description:

During testing of the user management functionality, it was observed that the application allows file uploads in the Signature field without enforcing proper file type validation. The application accepts files with any extension, including non-image and potentially dangerous file types, instead of restricting uploads to expected image formats only. This indicates a lack of server-side validation on uploaded files. Unrestricted file upload vulnerabilities can be abused to upload malicious files, which may lead to further attacks depending on how and where the uploaded files are stored and accessed.

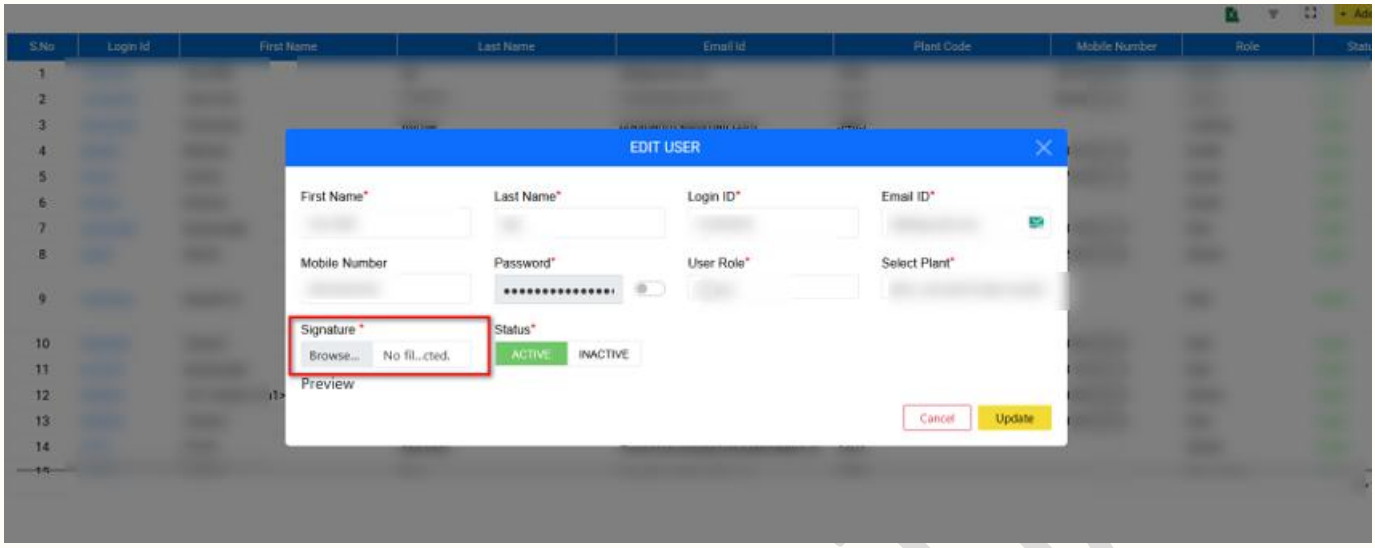
CVE/CWE:	• CWE-434 – Unrestricted Upload of File with Dangerous Type • CWE-20 – Improper Input Validation
Risk Rating:	⚠ Medium
Reference:	https://mas.owasp.org/MASVS/controls/MASVS-PLATFORM/

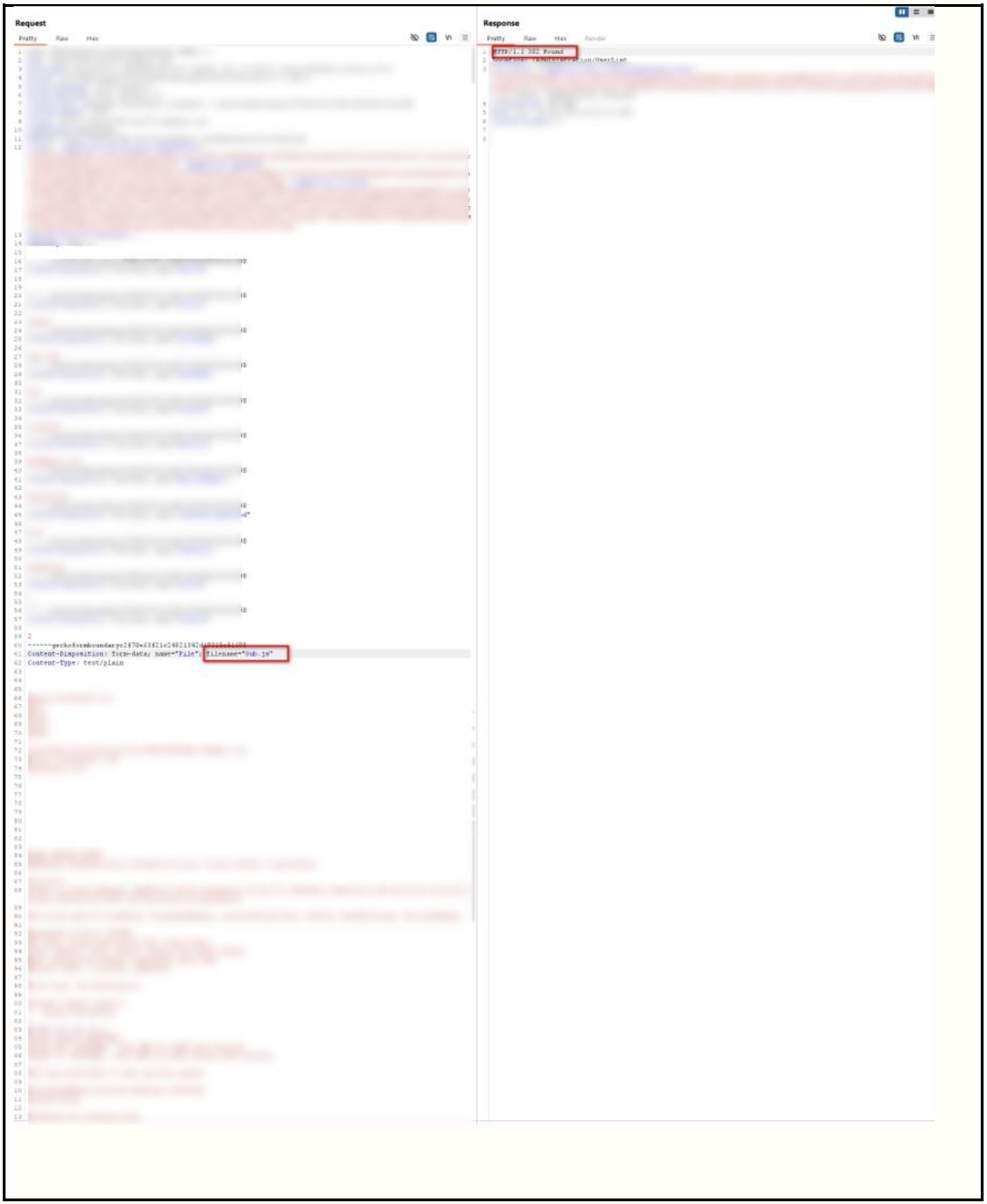
Impact:

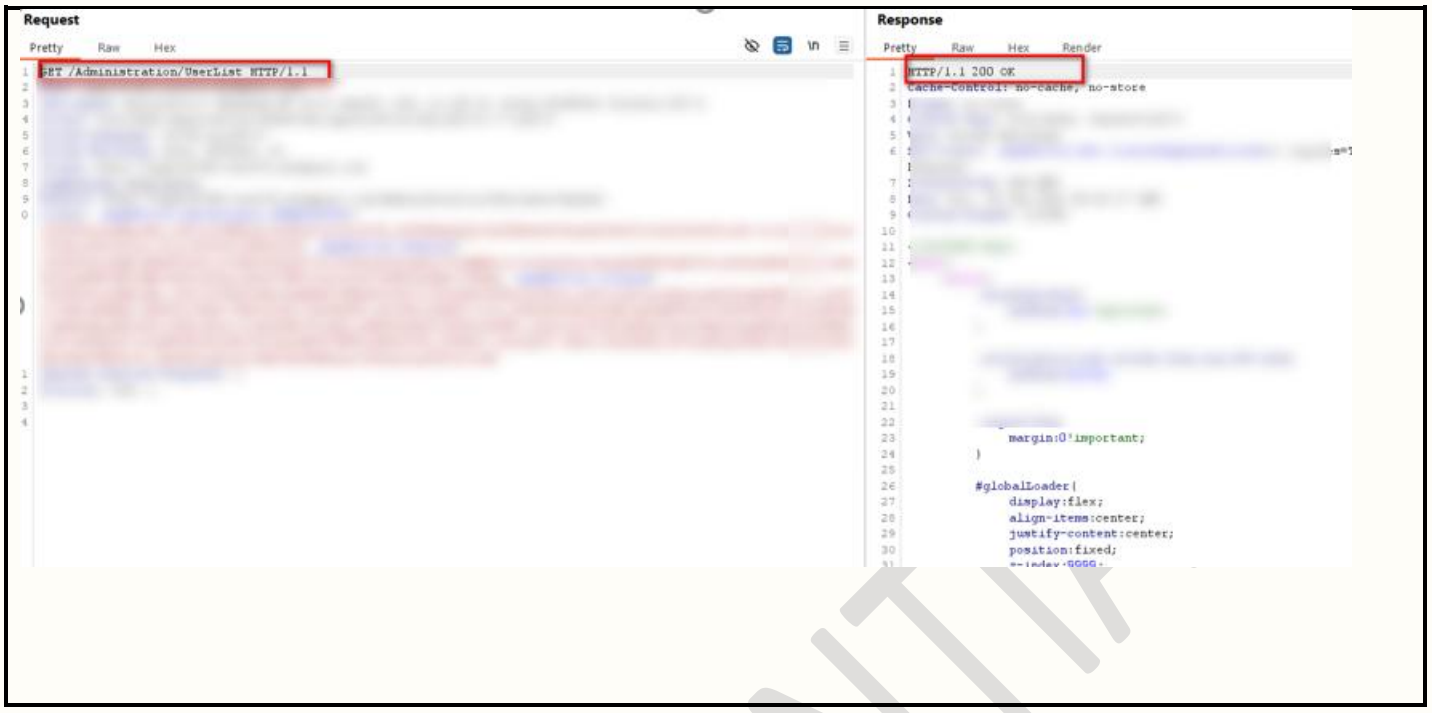
- Storage of malicious files on the server
- Abuse of uploaded content if files are accessible
- Increased attack surface for further exploitation

Recommendation:	• Validate uploaded files using:
	  ○ File extension allow listing
	  ○ MIME type validation
	  ○ File signature (magic byte) checks

Proof of Concept (POC):




Request
Response
HTTP/1.1 302 Found
Content-Disposition: form-data; name="File"; filename="Sub.js"
Content-Type: text/plain



VULNERABILITY ISSUE 10:	Authenticated Pages Accessible via Browser Back Button After Logout
Affected Component:	

Description:

During testing, it was observed that after a user logs out of the application, previously accessed authenticated pages remain accessible through the browser back button without requiring re-authentication.

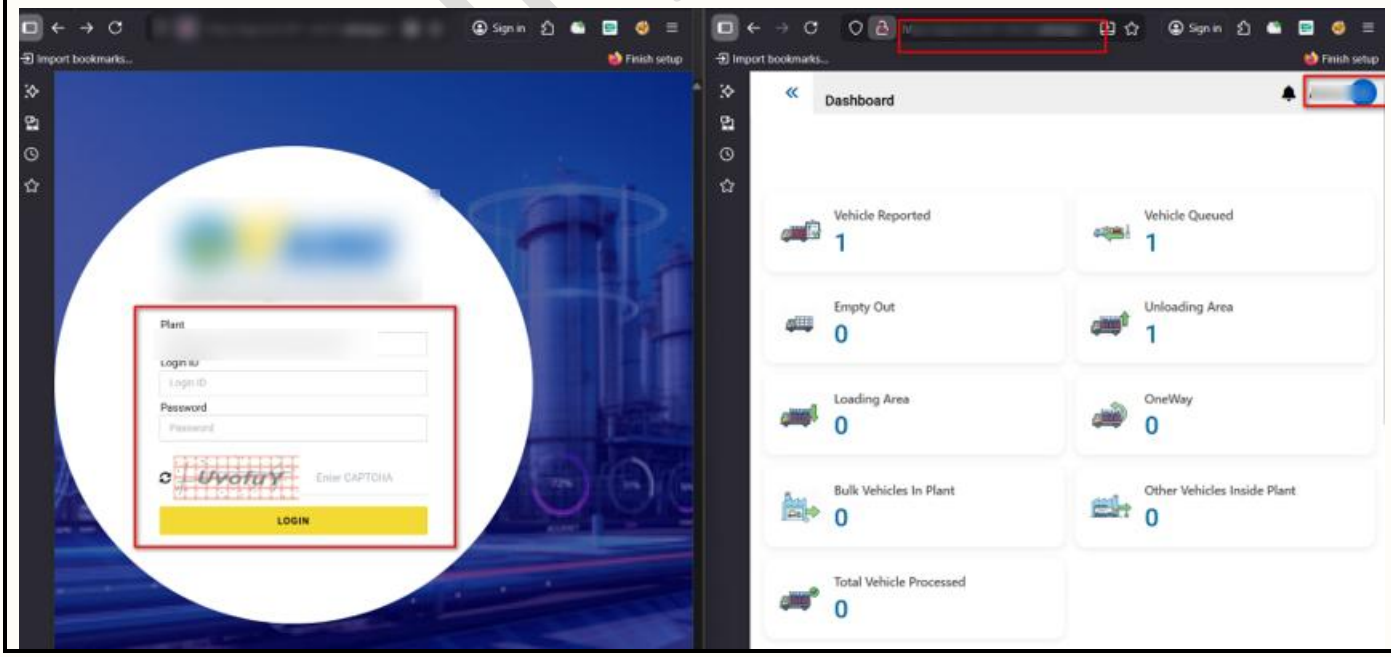
CVE/CWE:	• CWE-613 – Insufficient Session Expiration • CWE-525 – Information Exposure Through Browser Caching
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

Impact:

- Sensitive information may remain visible after logout
- Increased risk on shared or public computers

Recommendation:	• Validate session tokens on every protected request • Force redirection to the login page when session is invalid

Proof of Concept (POC):



VULNERABILITY ISSUE 11:	Application Accepts Common / Weak Passwords
Affected URL:	

Description:

During testing of the Change Password functionality, it was observed that the application accepts commonly used and easily guessable passwords despite displaying a password policy message. Although a policy banner indicates minimum complexity requirements, the system does not effectively prevent the use of widely known weak passwords, which reduces overall account security and increases susceptibility to brute-force or credential-stuffing attacks.

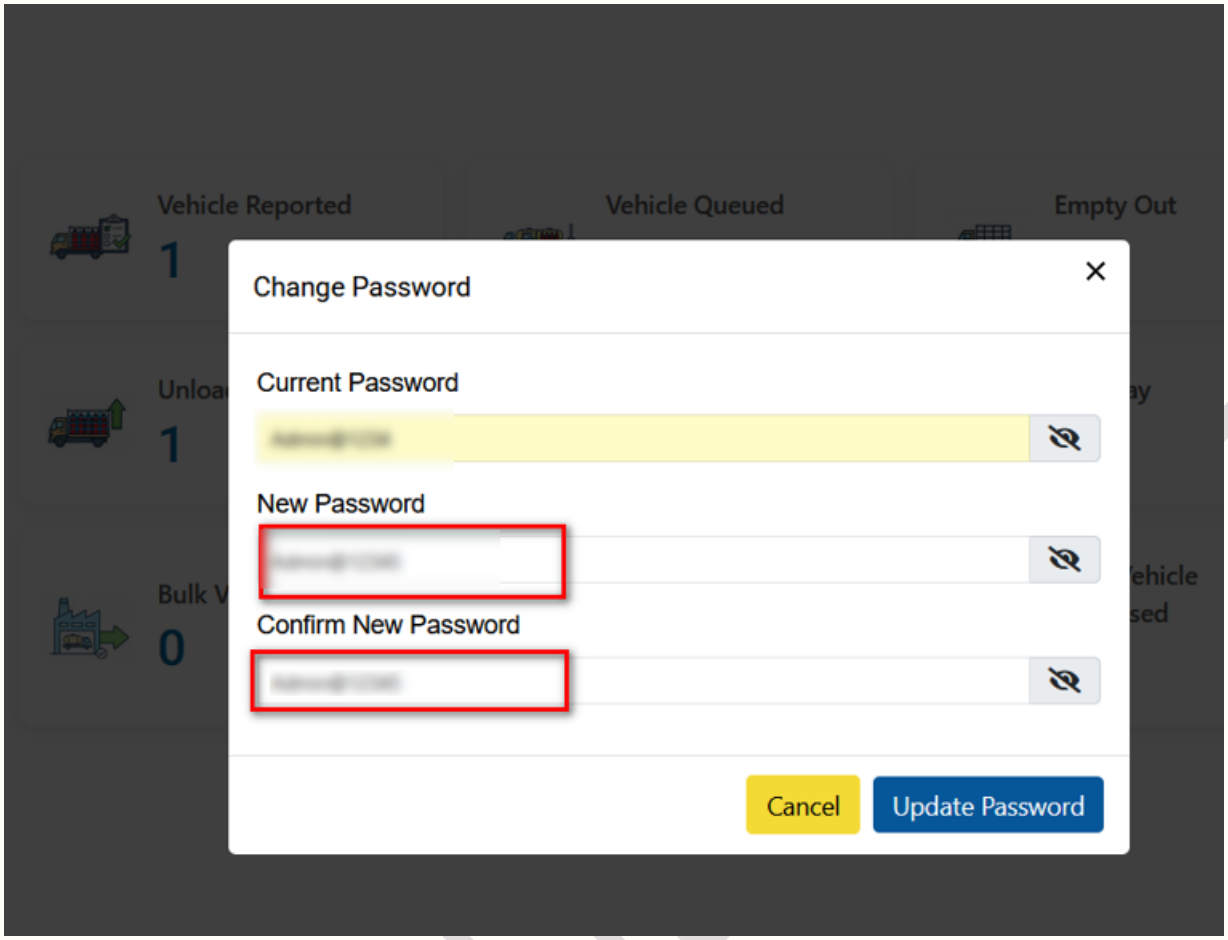
CVE/CWE:	• CWE-521 – Weak Password Requirements • CWE-307 – Improper Restriction of Excessive Authentication Attempts
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

Impact:

- Increases risk of account compromise through password-guessing attacks
- Reduces effectiveness of password complexity policies

Recommendation:	• Implement a weak password blacklist (e.g., “password”, “admin”, “welcome”, etc.) • Enforce minimum password entropy/strength checks

Proof of Concept (POC):



VULNERABILITY ISSUE 12:	User Status Toggle Not Reflecting Correctly After Creation
Affected Component:	

Description:

During testing of the User Management → Add New User functionality, it was observed that the Status toggle value is not saved correctly. When creating a new user and selecting the Inactive status, the application saves the user but displays the status as Active in the user list. This indicates a mismatch between the selected status in the form and the value stored or rendered by the system.

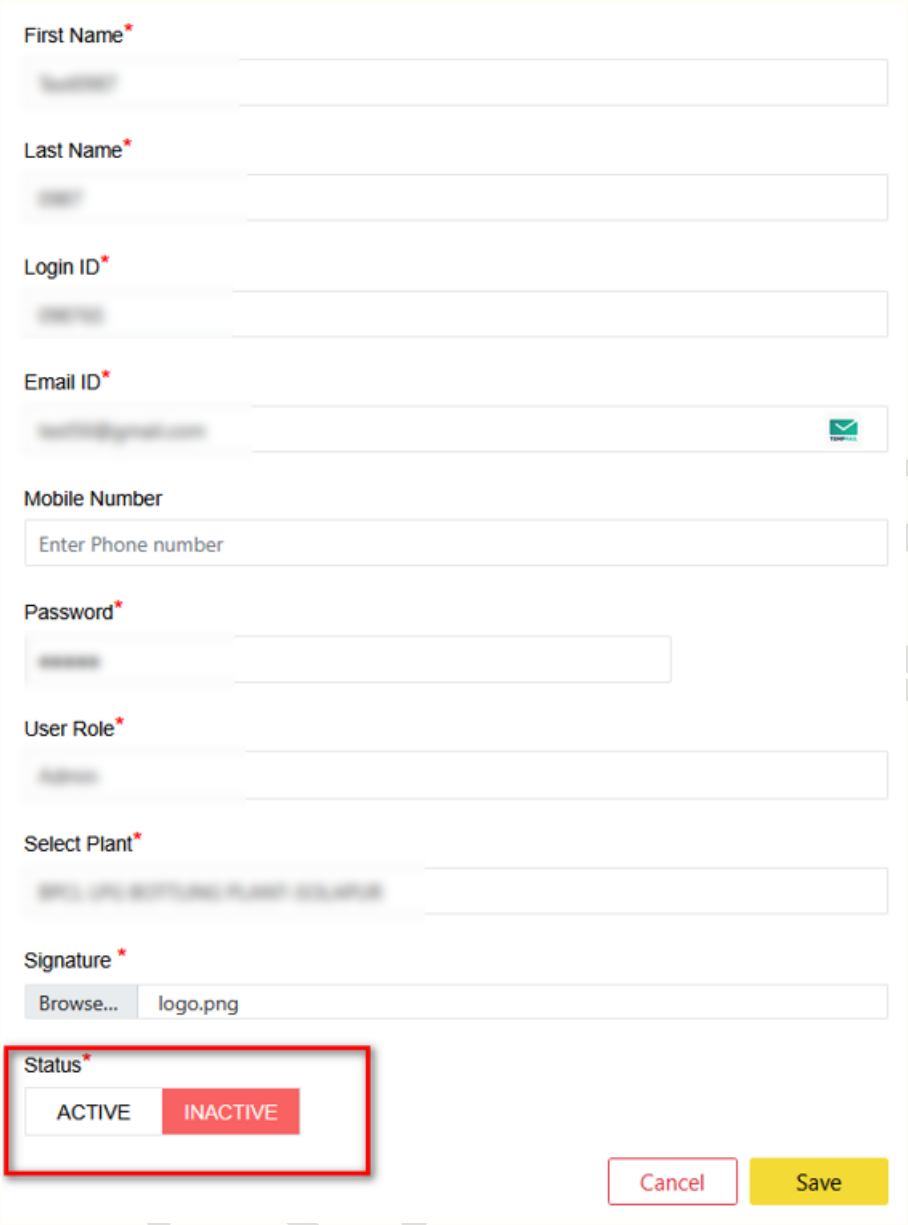
CVE/CWE:	• CWE-521: Weak Password Requirements • CWE-307: Improper Restriction of Excessive Authentication Attempts
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

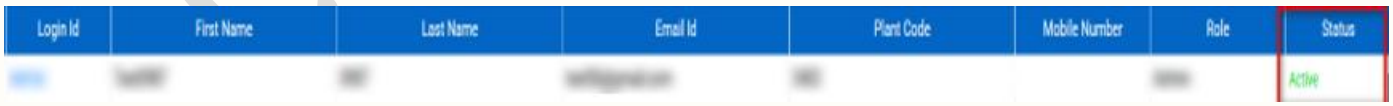
Impact:

- Users intended to be inactive may remain active
- Risk of unauthorized or unintended access
- Administrative control over user lifecycle becomes unreliable

Recommendation:	• Validate that the status field value is correctly passed in the request payload • Ensure backend logic respects the provided status instead of applying defaults • Implement server-side validation and confirmation response

Proof of Concept (POC):





VULNERABILITY ISSUE 13:	Unrestricted File Upload – File Type Validation Missing in Excel Upload Functionality
Affected URL:	

Description:

During testing of the Customer Registration → Upload Excel File functionality, it was observed that the application does not enforce file type validation. Although the interface indicates that only Excel files should be uploaded, the server accepts files with arbitrary extensions such as .php, .js, and .sh without restriction. This indicates missing or insufficient server-side validation of uploaded file types.

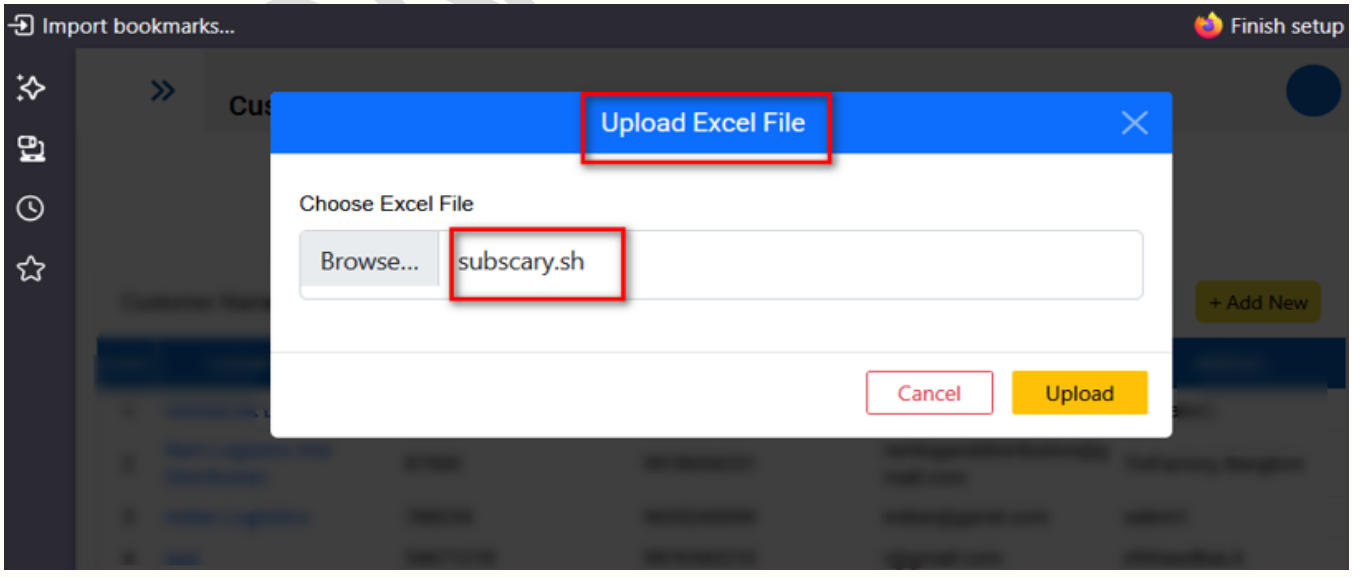
CVE/CWE:	• CWE-434 – Unrestricted Upload of File with Dangerous Type • CWE-20 – Improper Input Validation
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

Impact:

- Allows upload of potentially malicious files
- Increases risk of remote code execution if files are stored in executable directories
- May enable storage of harmful scripts or unauthorized content

Recommendation:	• Enforce server-side allow listing for file extensions (.xls, .xlsx only) • Validate MIME type and file signature (magic bytes)

Proof of Concept (POC):



VULNERABILITY ISSUE 14:	Improper Input Length Handling / Potential Application-Level DoS
Affected Component:	

Description:

During testing of the Customer Registration → Add Customer functionality, it was observed that multiple input fields do not enforce a maximum character length restriction. Extremely long input values are accepted without validation or truncation. Allowing unrestricted input lengths may lead to performance degradation, excessive memory usage, UI rendering issues, or potential denial-of-service conditions depending on backend processing and storage logic.

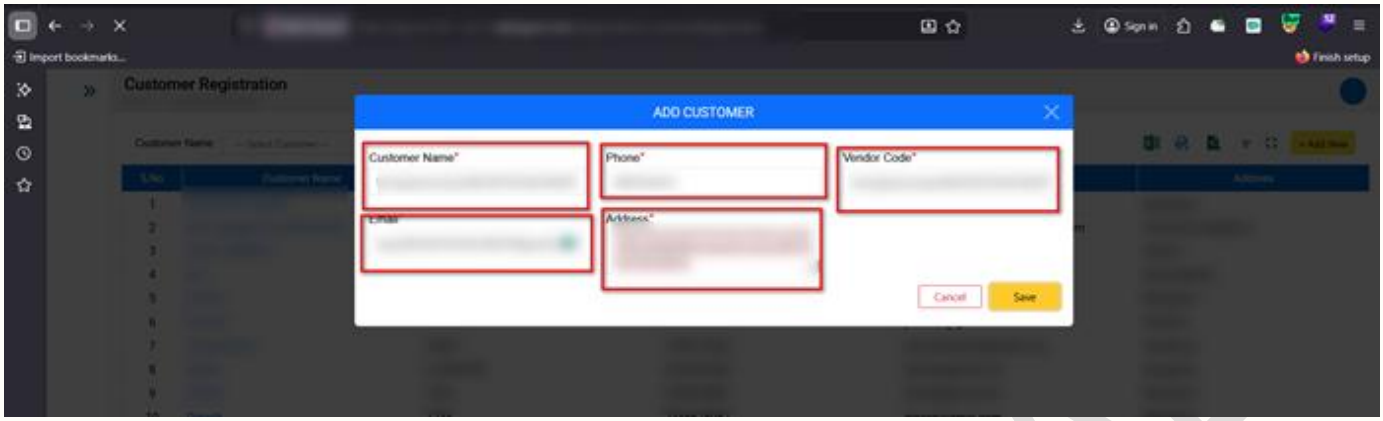
CVE/CWE:	• CWE-20 – Improper Input Validation • CWE-400 – Uncontrolled Resource Consumption
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

Impact:

- Potential UI distortion or rendering issues
- Increased database storage and memory consumption
- Possible backend processing delays
- Risk of application-level resource exhaustion in extreme scenarios

Recommendation:	• Define and enforce maximum character limits per field • Apply server-side validation in addition to client-side checks • Implement database column size constraints

Proof of Concept (POC):



VULNERABILITY ISSUE 15:	Authenticated Pages Accessible via Browser Back Button After Logout
Affected URL:	

Description:

During testing, it was observed that after a user logs out of the application, previously accessed authenticated pages can still be viewed by using the browser back button without requiring re-authentication.

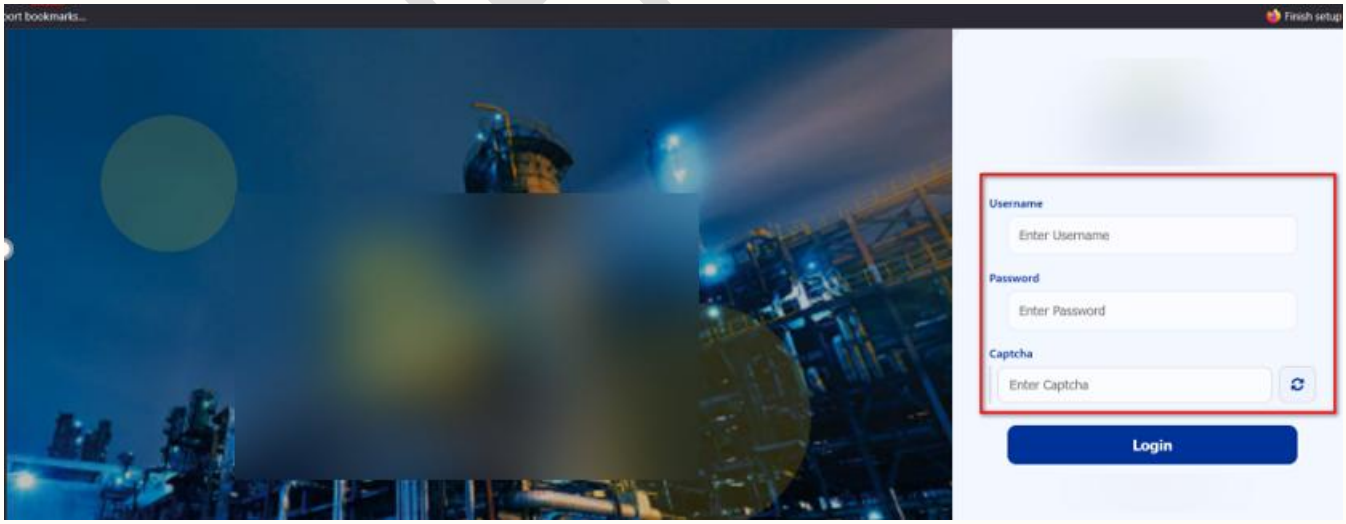
CVE/CWE:	• CWE-613 – Insufficient Session Expiration • CWE-525 – Information Exposure Through Browser Caching
Risk Rating:	⚠ Medium
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

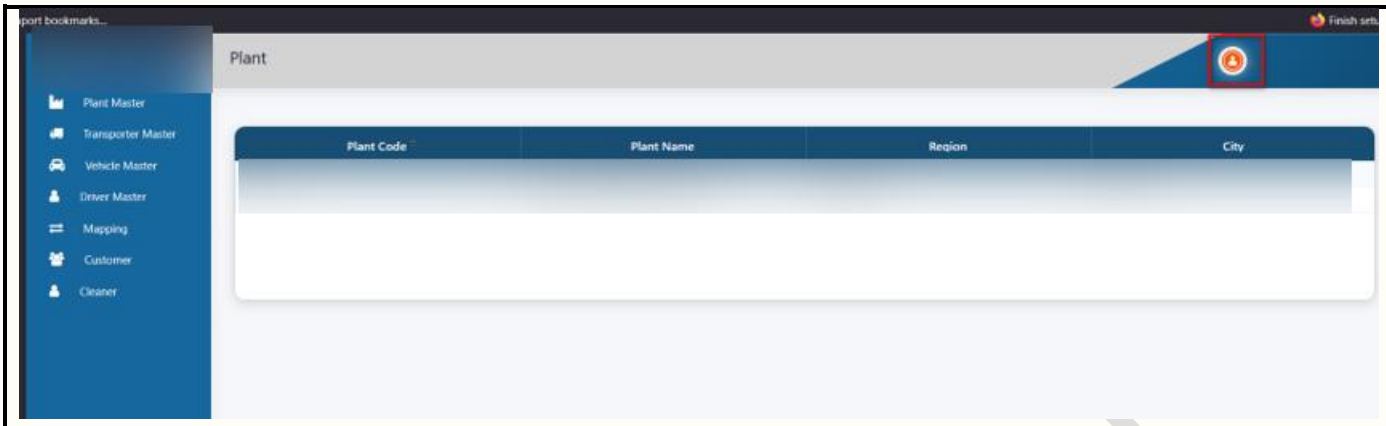
Impact:

- Sensitive information may remain visible after logout
- Risk increases on shared or public computers

Recommendation:	• Ensure complete session invalidation on logout (server-side) • Redirect users to the login page when accessing protected routes after logout

Proof of Concept (POC):





VULNERABILITY ISSUE 16:	Web Server Version Disclosure
Affected URL:	

Description:

The web server reveals detailed version and operating system information through service banners, aiding attackers during reconnaissance.

CVE/CWE:	• CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor • CWE-16 – Configuration
Risk Rating:	⚠ Low
Reference:	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Impact:

Disclosed server details can be leveraged to identify known vulnerabilities and plan targeted attacks, increasing overall risk exposure.

Recommendation:	• Remove or suppress HTTP response headers that disclose server information (such as Server and X-Powered-By). • Configure the web server to display custom error pages instead of detailed system error messages. • Avoid exposing framework or platform version details to unauthenticated users. • Ensure the web server is kept up to date with the latest vendor-recommended patches.

Proof of Concept (POC):

VULNERABILITY ISSUE 17:	FTP Service Exposed on Production Server
Affected URL:	

Description:

During network-level reconnaissance, it was observed that the FTP service (port 21/TCP) is exposed on the production server hosting the web application. FTP is an outdated protocol that transmits data, including credentials, in clear text by default. Even when not actively used, an exposed FTP service increases the attack surface and may be targeted for unauthorized access, brute-force attacks, or misconfiguration abuse.

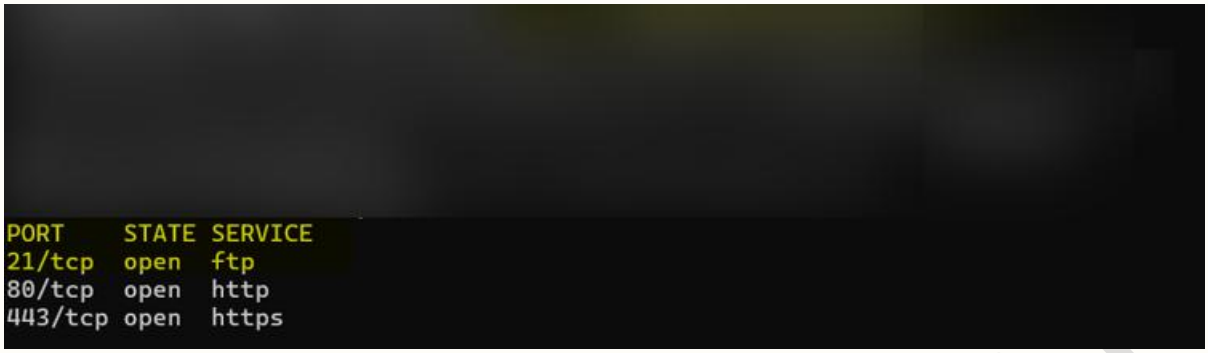
CVE/CWE:	• CWE-319 – Cleartext Transmission of Sensitive Information • CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor
Risk Rating:	⚠ **Low**
Reference:	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Impact:

- Increases the exposed attack surface of the production server
- May allow brute-force or credential-stuffing attacks if authentication is enabled
- FTP traffic can be intercepted if accessed over untrusted networks
- Could lead to unauthorized file access if misconfigured

Recommendation:	• Disable the FTP service if it is not required for application functionality • If file transfer is needed, replace FTP with a secure alternative such as SFTP or FTPS • Restrict access to FTP using firewall rules or IP allow listing • Ensure strong authentication and logging are enabled if the service must remain exposed

Proof of Concept (POC):



VULNERABILITY ISSUE 18:	Password Field Missing Autocomplete Attribute
Affected URL:	

Description:

It was observed that the password input field on the login page does not explicitly define the autocomplete attribute. When the autocomplete attribute is not set, browsers and password managers may handle stored credentials inconsistently. This can result in unintended password storage, autofill behaviour, or exposure of credentials on shared or public systems.

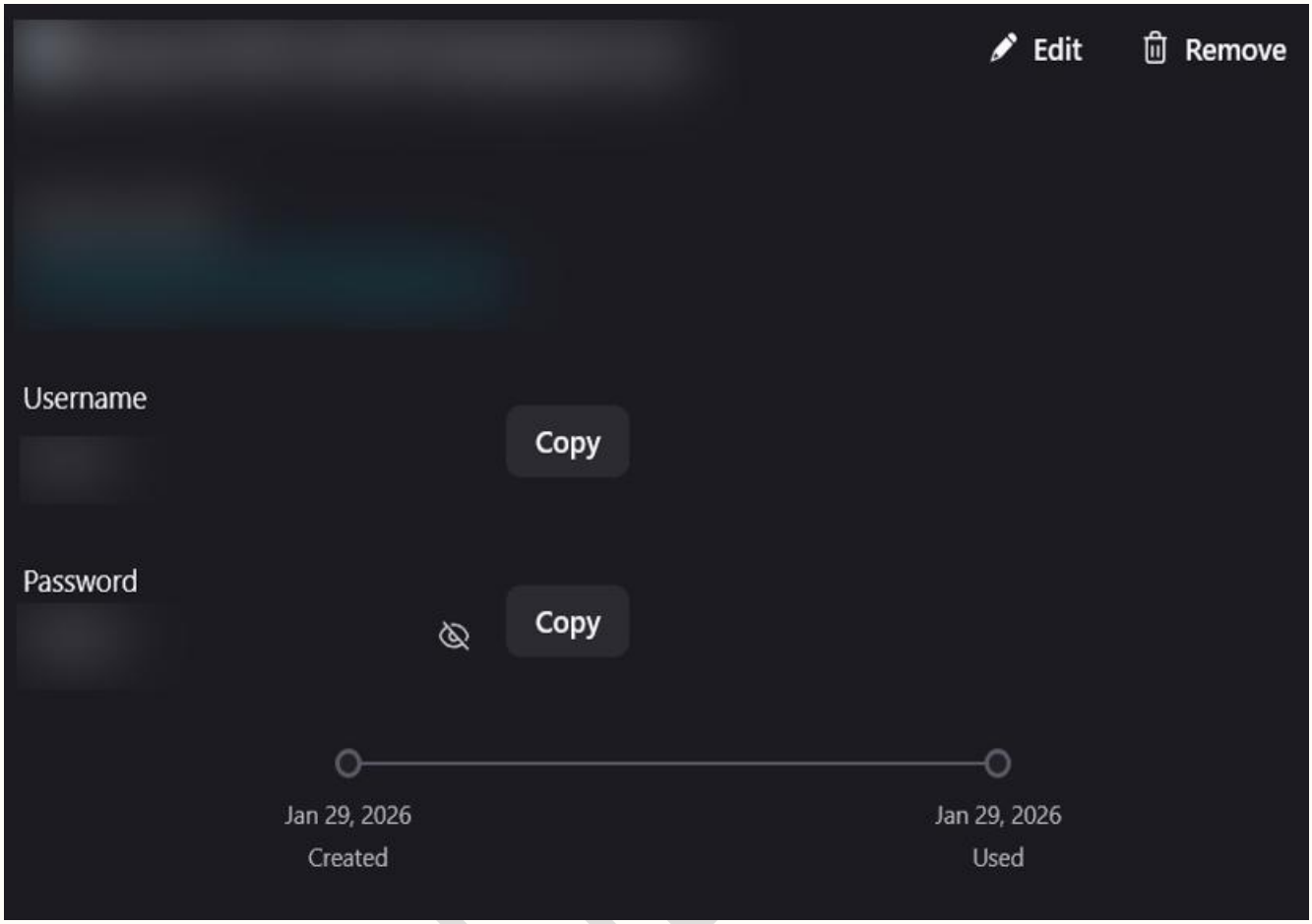
CVE/CWE:	• CWE-524 – Use of Cache Containing Sensitive Information • CWE-522 – Insufficiently Protected Credentials
Risk Rating:	⚠ **Low**
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

Impact:

- May allow browsers to store or autofill passwords unintentionally
- Increases risk on shared or public systems
- Does not directly lead to exploitation, but weakens credential handling controls

Recommendation:	• Explicitly define the autocomplete attribute for password fields • Use recommended values based on the context (e.g., login vs registration)

Proof of Concept (POC):



VULNERABILITY ISSUE 19:	Lack of Rate Limiting on Login Endpoint for Unauthenticated Requests
Affected URL:	

Description:

It was observed that the application does not enforce rate limiting or request throttling on unauthenticated requests to the login endpoint. Multiple sequential requests were sent in a short period without any restriction, delay, or blocking mechanism being applied. The absence of rate limiting allows repeated requests to be processed continuously, which may be abused for automated activities

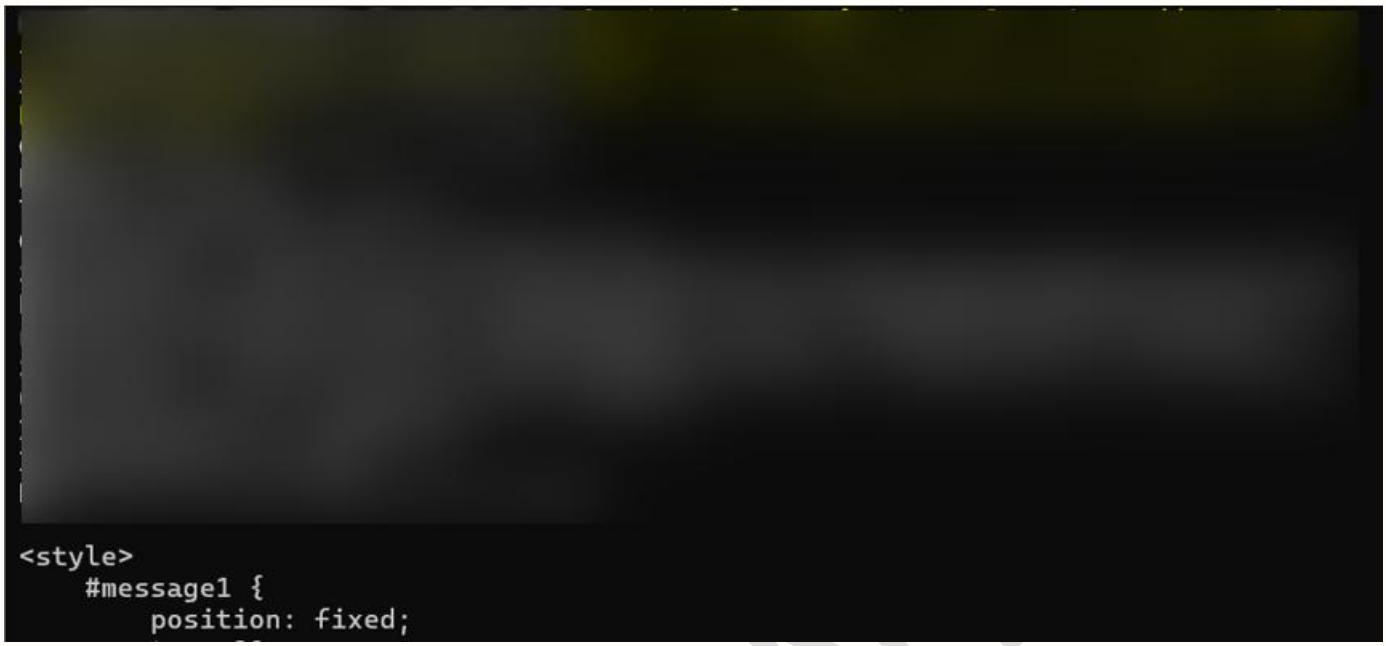
CVE/CWE:	• CWE-799 – Improper Control of Interaction Frequency • CWE-307 – Improper Restriction of Excessive Authentication Attempts
Risk Rating:	⚠ **Low**
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures

Impact:

- Allows automated, high-frequency requests without restriction
- May facilitate reconnaissance or preparatory attacks such as credential stuffing
- Can contribute to unnecessary server load and increased attack surface

Recommendation:	• Implement rate limiting or request throttling on the login endpoint • Enforce request limits based on IP address or request patterns • Return appropriate responses such as HTTP 429 when limits are exceeded • Monitor repeated failed or high-frequency login attempt

Proof of Concept (POC):



VULNERABILITY ISSUE 20:	Username Enumeration via Distinct Login Error Message
Affected URL:	

Description:

During testing of the login functionality, it was observed that the application returns a specific error message when an invalid username is supplied, even when a valid password is used.
The application responds with the message “Invalid user. Please check and try again.”, which allows an attacker to distinguish between non-existent usernames and other authentication failures. This behavior enables username enumeration, which can be leveraged in further attacks.

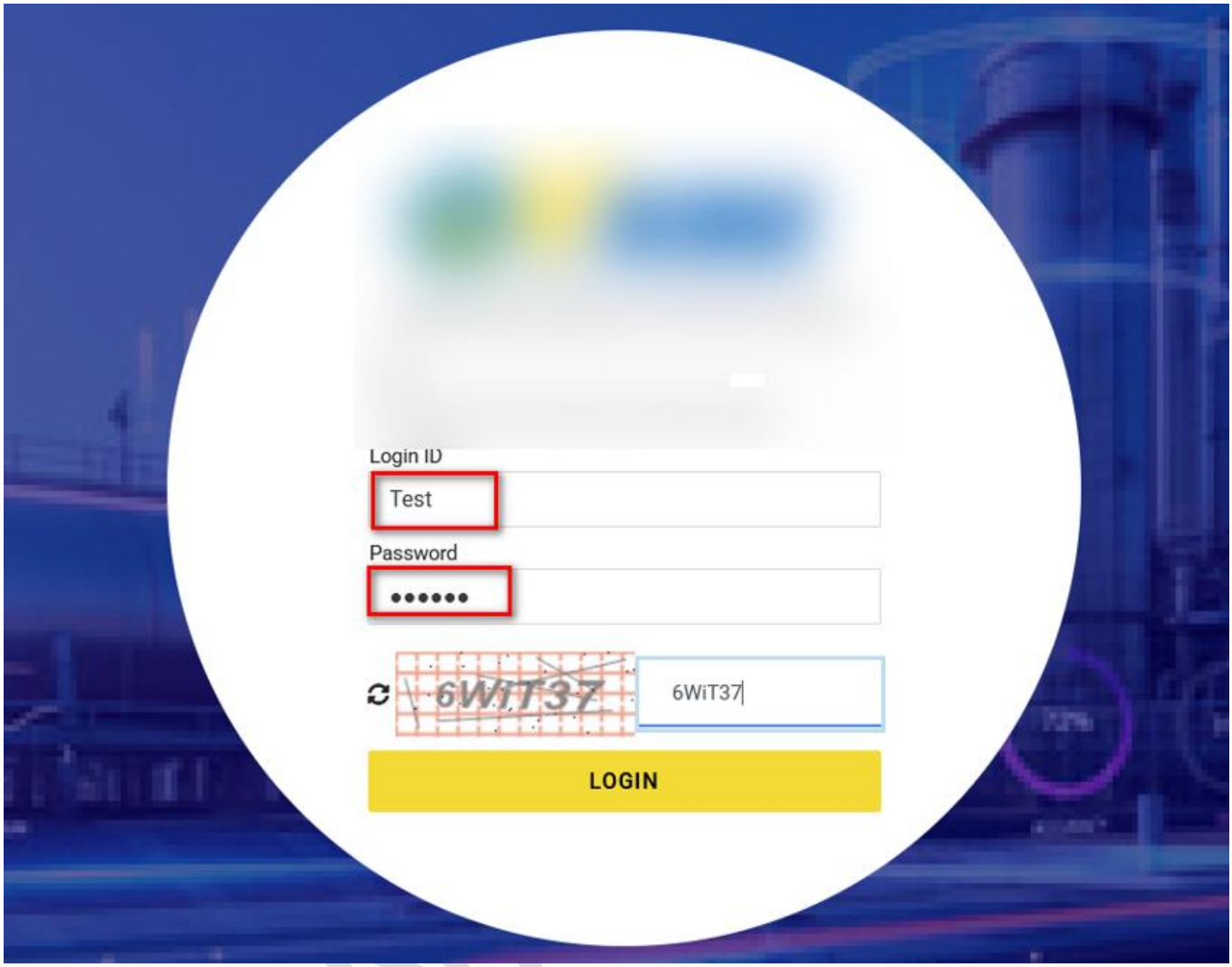
CVE/CWE:	• CWE-204 – Observable Response Discrepancy • CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor
Risk Rating:	⚠ **Low**
Reference:	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

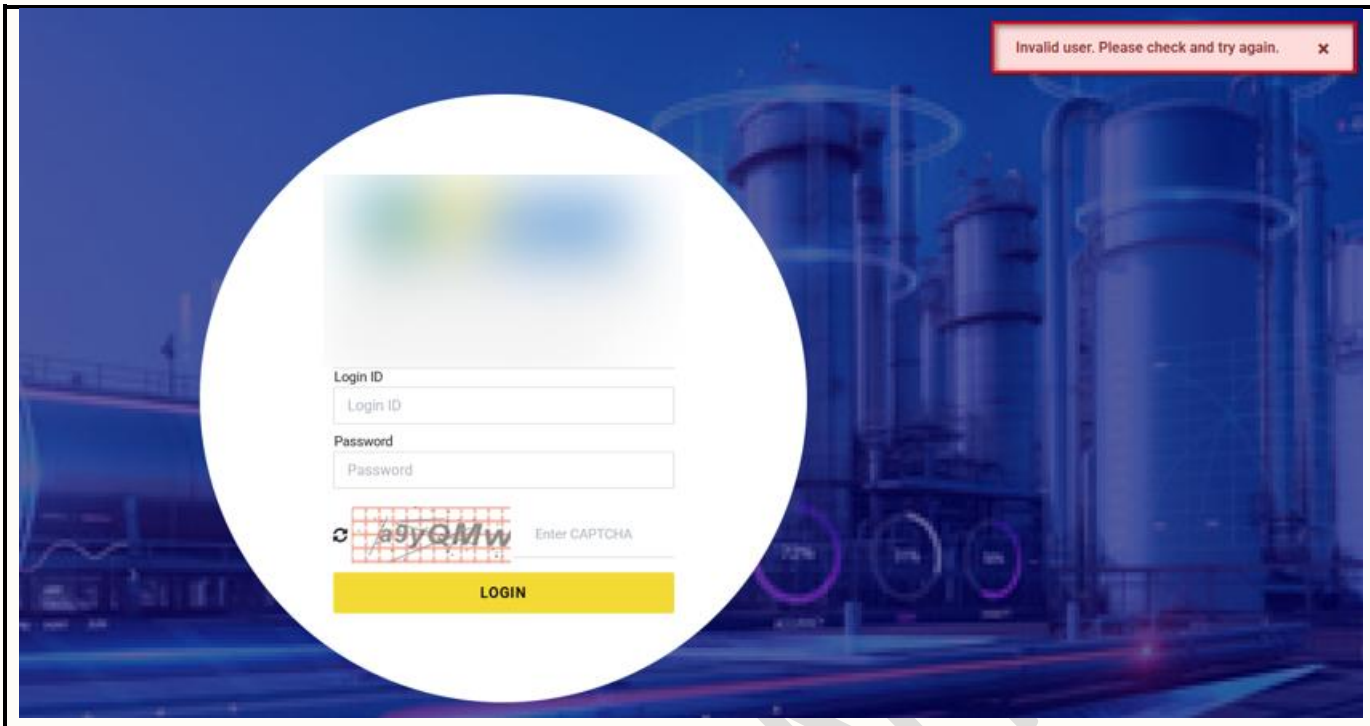
Impact:

- Allows attackers to identify valid and invalid usernames
- Facilitates targeted brute-force or credential-stuffing attacks
- Reduces attack complexity by confirming account existence

Recommendation:	• Use a generic error message for all authentication failures ○ Example: “Invalid username or password” • Ensure identical responses (message, status code, and timing) for all failed login attempts • Log detailed authentication failure reasons internally for monitoring

Proof of Concept (POC):




Invalid user. Please check and try again.
Login ID
Login ID
Password
Password
a9yQMw
Enter CAPTCHA
LOGIN