VIRTUAL CAIM

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Web, API and Network Security Assessment Report

Prepared for Example Finserv Ltd. (fictional client). Customer portal, mobile API, partner gateway and back-office console.

SAMPLE REPORT - fictional engagement, sanitized

SAMPLE

Report ID	VC-SAMPLE-VAPT-2026-001
Client	Example Finserv Ltd. (fictional NBFC)
Engagement window	14 September 2026 to 9 October 2026
Report date / version	21 October 2026 / v1.0 (Final)
Classification	Confidential (sample). Fictional data throughout.
Prepared by	Virtual Caim Private Limited. This Organization is empanelled by CERT-In for providing information Security Auditing Service.

Document control

Document title	VAPT Report: Customer Portal, Mobile API, Partner Gateway, Back-office Console
Document ID	VC-SAMPLE-VAPT-2026-001
Client point of contact	Head of Information Security, Example Finserv Ltd. (fictional)
Distribution	Named Point of Contact only. Shared through an encrypted, password-protected channel from an official Virtual Caim mailbox, with the password sent by a separate channel.
Handling	Working notes, raw tool output and screenshots are retained under the client's data-handling agreement and destroyed on the agreed date.

Version history

Version	Date	Status	Description
0.1	9 Oct 2026	Draft	Interim notification of Critical and High findings issued to the Point of Contact during testing.
0.9	14 Oct 2026	Draft	Full draft for factual accuracy review by the client.
1.0	21 Oct 2026	Final	Issued after factual review. Re-test scheduled after remediation.

Tested artefacts

Asset	Environment tested	Version / build	Build hash (SHA-256)
Customer Web Portal	UAT, production-equivalent	4.12.3	`9f3a...c71e` (shortened)
Mobile API	UAT, production-equivalent	2.8.0	`41bd...07aa` (shortened)
DSA Portal	UAT	1.9.4	`c0e2...5d19` (shortened)
Back-office console	UAT (internal)	3.3.1	`7a58...e2f0` (shortened)
Partner gateway	Production (external, non-intrusive checks only)	n/a	n/a

Contents

1. Executive summary 3
2. Scope and rules of engagement 4
3. Methodology 6
4. Findings summary 8
5. Detailed findings 9
6. Informational observations 19
7. Risk matrix 20
8. Remediation roadmap 21
9. Re-test and closure policy 22
Annex A. Compliance mapping 23
Annex B. Test coverage and evidence register 25
Annex C. Glossary 26
Annex D. Sign-off 26

SAMPLE

1. Executive summary

Example Finserv Ltd. asked Virtual Caim to test its customer-facing lending platform and the supporting back-office console before the next product release. This summary is written for the Board, the CEO and the Chief Information Security Officer. It describes the risk in business terms. Technical detail is in section 5.

9
FINDINGS
plus 3 informational observations

1
CRITICAL
needs action within 7 days

3
HIGH
needs action within 15 days

5
MEDIUM AND LOW
planned release cycle

Overall risk posture

> **RATING: ELEVATED (SAMPLE)**
> The platform has a solid technical base: modern transport security on the main hosts, input validation that stops common injection, and a WAF in front of the portal. The weak spots sit in the identity and authorisation layer, where a small number of design flaws can expose customer accounts and personal data at scale. We recommend that the release is held until the Critical finding (F-01) is closed and the High findings have a dated fix plan.

What the main findings mean for the business

- **Customer accounts can be taken over.** The password-reset flow can be defeated without access to the customer's phone or email (F-01). A takeover of one account is a personal data breach. A takeover at scale is a reportable incident to CERT-In within 6 hours and a regulatory event.
- **One customer can see another customer's loan data.** Statement and preference endpoints do not check ownership (F-02). This is the kind of flaw that attracts regulator attention and customer complaints.
- **The second factor is not a real barrier.** OTP guesses are not limited (F-03).
- **Customer input can reach a privileged internal session.** A support ticket can run script in an officer's browser (F-04).

What is working well

- The portal and API hosts enforce TLS 1.2 or higher with strong cipher suites.
- Parameterised queries are used consistently; no SQL injection was found in the tested routes.
- Administrative functions are not reachable from the internet and the back-office console requires a second factor.
- File upload is restricted by type and size, and uploaded files are stored outside the web root.
- The client's security team responded to interim notifications within one working day.

Where we recommend you start

Priority	Action	Findings	Owner (suggested)	Target
1	Replace reset-token design and add throttling	F-01, F-03	Application engineering lead	7 to 15 days
2	Introduce a central ownership check for API object access	F-02	API team	15 days
3	Encode output in the console, add CSP	F-04	Back-office team	15 days
4	Session lifecycle, library, TLS and header hygiene	F-05 to F-09	Platform and DevOps	30 to 90 days
5	Add authorisation tests and SCA to the pipeline	Root cause	Engineering and security	Next quarter

SAMPLE

2. Scope and rules of engagement

2.1 Objectives

- Identify vulnerabilities in the in-scope applications and exposed infrastructure that could affect confidentiality, integrity or availability of customer data and services.
- Demonstrate realistic impact safely, without disrupting service or accessing real customer data.
- Give practical, prioritised remediation steps and a basis for a re-test.

2.2 Assets in scope

#	Asset	Type	Location (sanitized)	Environment	Depth
1	Customer Web Portal	Web application	portal.examplefinserv.example	UAT	Authenticated, 2 customer roles
2	Mobile API (Android and iOS back end)	REST API	api.examplefinserv.example	UAT	Authenticated, 340 documented routes
3	DSA (agent) Portal	Web application	dsa.examplefinserv.example	UAT	Authenticated, agent role
4	Back-office console	Web application (internal)	10.20.x.x (redacted)	UAT	Authenticated, officer role
5	Partner gateway and perimeter	External network	203.0.113.0/28 (redacted)	Production	Non-intrusive, no exploitation

2.3 Out of scope

- Denial-of-service and volumetric testing.
- Social engineering and physical security.
- Third-party services (payment aggregator, SMS provider, e-KYC provider). Their integration points were tested from our side only.
- Source code review (an option for the next phase).

2.4 Timeline and effort

Phase	Dates	Effort
Kick-off, access verification, test accounts	14 to 15 Sep 2026	2 person-days
Reconnaissance and mapping	16 to 18 Sep 2026	5 person-days
Vulnerability discovery and exploitation (safe)	21 Sep to 2 Oct 2026	20 person-days
Post-exploitation analysis and impact validation	5 to 7 Oct 2026	5 person-days
Reporting and walkthrough	8 to 21 Oct 2026	4 person-days

2.5 Rules of engagement

- Testing windows: 20:00 to 06:00 IST on weekdays for UAT; non-intrusive checks on production at any time with prior notice.
- Source addresses: two static Virtual Caim IPs, shared with the client's SOC to avoid false escalations.
- Test data: only accounts created for the engagement were used. No real customer record was accessed, modified or exported.
- Stop conditions: any sign of instability, accidental exposure of real data, or a finding that suggests an active compromise causes testing to pause and the Point of Contact to be called.
- Immediate notification: Critical and High findings were reported to the Point of Contact within one working day of discovery, ahead of this report.
- Escalation contacts and out-of-hours numbers were exchanged at kick-off.

2.6 Assumptions, limitations and constraints

- Results apply to the builds and configuration recorded in the document control section at the dates tested.

SAMPLE

- Testing was time-boxed. Absence of a finding is not proof of absence of a vulnerability.
- The assessment was performed on a UAT stack and not on production, apart from the perimeter checks. Differences between UAT and production were declared by the client and not independently verified.
- Business logic coverage was limited to the loan servicing and support journeys agreed at kick-off.

2.7 Assessment team

Role	Count	Responsibility
Lead Auditor	1	Planning, quality of testing, sign-off of findings
Security testers	3	Manual testing, tooling, evidence
Independent reviewer	1	Reviews the report. Not part of the test team.

SAMPLE

3. Methodology

We follow a four-phase approach that moves from understanding the system to proving realistic impact and then to reporting. It is aligned with the Penetration Testing Execution Standard (PTES), NIST SP 800-115 (technical guide to information security testing) and the OWASP Web Security Testing Guide (WSTG v4.2) with the OWASP Application Security Verification Standard (ASVS) as the benchmark for authentication, session and access control requirements. API testing follows the OWASP API Security Top 10 (2023).

Phase	What we do	Typical output	PTES stage
1. Reconnaissance	Map the attack surface: hosts, routes, technologies, user roles, trust boundaries. Review documentation and API specifications. Passive and low-impact active discovery.	Asset and route inventory, role matrix, threat model notes	Pre-engagement, intelligence gathering, threat modelling
2. Vulnerability discovery	Manual testing guided by WSTG categories, supported by scanners for breadth. Authenticated and unauthenticated passes. Business logic walk-throughs per role.	Candidate issues with reproduction steps	Vulnerability analysis
3. Exploitation and post-exploitation	Confirm issues safely. Chain findings where it shows real impact. Assess what an attacker could reach and what could be proved with test data. No destructive actions.	Validated findings, attack paths, impact statements	Exploitation, post-exploitation
4. Reporting and walkthrough	Rate, de-duplicate, write evidence and fixes. Walk the client team through the findings, agree closure timelines, plan re-test.	This report, evidence annex, walkthrough	Reporting

3.1 Test categories applied (OWASP WSTG v4.2)

WSTG area	Example checks performed
4.1 Information gathering	Fingerprinting, entry points, application mapping, technology stack
4.2 Configuration and deployment	Platform configuration, HTTP methods, HSTS, file extensions, backup files
4.3 Identity management	Role definitions, registration, account enumeration
4.4 Authentication	Credential transport, lock-out, password reset, OTP, alternative channels
4.5 Authorisation	Path traversal, authorisation bypass, privilege escalation, object references
4.6 Session management	Cookie attributes, fixation, CSRF, logout, timeout
4.7 Input validation	Reflected and stored XSS, injection classes, file inclusion
4.8 Error handling	Error codes and stack traces
4.9 Weak cryptography	TLS configuration, padding, sensitive data over unencrypted channels
4.10 Business logic	Workflow integrity, request forging, upload of unexpected file types
4.11 Client side	DOM issues, clickjacking, CORS, web storage
4.12 API testing	GraphQL not applicable; REST routes tested per OWASP API Top 10

3.2 Tools and manual techniques

Intercepting proxy (Burp Suite Professional), network and service discovery (Nmap), TLS analysis (testssl.sh), content discovery, and custom scripts written for this engagement. Automated results were never reported without manual validation. Tools were authorised in advance in the engagement plan shared with the client.

3.3 Severity and prioritisation model

Every finding carries a CVSS v3.1 base score and vector, an EPSS probability for the likelihood of real-world exploitation where a CVE applies (or an illustrative value in this sample), a CWE identifier and, where one exists, a CVE identifier. Severity bands follow the CVSS v3.1 qualitative scale. Business context can move the remediation order, but never the score itself.

Severity	CVSS v3.1 base	Meaning	Proposed closure target
Critical	9.0 to 10.0	Direct compromise or mass data exposure with little effort	7 days
High	7.0 to 8.9	Serious weakness with a realistic path to harm	15 days
Medium	4.0 to 6.9	Needs specific conditions or chaining	30 days
Low	0.1 to 3.9	Hardening or limited impact	90 days
Informational	0.0	Observation with no direct exploitable impact	Next planned release

READING EPSS

EPSS is a probability between 0 and 1 that a vulnerability is exploited in the wild in the next 30 days. It helps to order work among findings of similar CVSS. Application-specific findings have no published EPSS, so values in this sample report are illustrative estimates and are labelled so.

SAMPLE

4. Findings summary

Findings are ordered by CVSS v3.1 base score. Status reflects the position at the date of this report.

ID	Finding	Primary asset	CVSS	Severity	EPSS*	CWE	Status
F-01	Account takeover through a predictable password-reset token	Customer Web Portal	9.1	Critical	0.31	CWE-640	Open
F-04	Stored cross-site scripting in the back-office support ticket viewer	Back-office console	7.6	High	0.07	CWE-79	Open
F-03	No effective limit on one-time password (OTP) verification attempts	Customer Web Portal and Mobile API	7.4	High	0.09	CWE-307	Open
F-02	Broken object-level authorisation on the loan statement API	Mobile API	7.1	High	0.18	CWE-639	Open
F-06	Outdated JavaScript library with known vulnerabilities (jQuery 3.4.1)	Customer Web Portal and DSA Portal	6.1	Medium	0.02	CWE-79	Open
F-05	Sessions remain valid after logout and idle timeout is too long	Customer Web Portal	5.4	Medium	0.04	CWE-613	Open
F-07	Legacy TLS protocol versions and weak cipher suites on the partner gateway	Partner gateway	5.3	Medium	0.01	CWE-326	Open
F-08	Verbose error messages and framework version disclosure	Mobile API	3.7	Low	0.01	CWE-209	Open
F-09	Missing clickjacking protection and HTTP Strict Transport Security	DSA	3.1	Low	0.01	CWE-1021	Open

* EPSS values are illustrative for this sample. CVSS vectors are given in each finding. Scores were calculated with the CVSS v3.1 equations published by FIRST.

Informational observations

ID	Observation
I-01	Permissive CORS policy on public static-asset endpoint
I-02	Application log retention declared at 90 days on the web tier
I-03	No published vulnerability disclosure contact

Distribution

1	3	3	2	3
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

Distribution by OWASP Top 10 (2021) category



5. Detailed findings

Each finding lists description, affected assets, sanitized evidence, business impact, remediation and references. In a live engagement the full reproduction steps and screenshots form a confidential annex given to the Point of Contact only. In this sample, evidence is deliberately redacted and no working exploit code appears anywhere: values that would help to repeat an attack are replaced by [REDACTED] or described in words, the way a sanitized report for external circulation is prepared.

F-01

Critical

CVSS v3.1 base 9.1

Account takeover through a predictable password-reset token

Severity / score	Critical 9.1 `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`
EPSS (illustrative)	0.31 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-640, CWE-330 | Not applicable (application logic flaw)
OWASP mapping	A07:2021 Identification and Authentication Failures | WSTG-ATHN-09
Affected assets	Customer Web Portal, Mobile API (password-reset service)
Closure target	7 days from notification (proposed, see section 9)

Description

The password-reset service issues a one-time token to the registered mobile number or email address of the customer. During testing we found that the token is built from a small numeric space and from values that an observer can estimate (the time of the request and the account sequence). The service also accepts the token without binding it to the browser or device that requested it, and it does not invalidate earlier tokens when a new one is issued.

Taken together, these design choices mean that a person who knows only a customer's registered username can, with a modest number of attempts, obtain a working reset token and set a new password. No access to the customer's phone or inbox is required.

Evidence

Token sampling (sanitized)

```
Test accounts: 3 (owned by Virtual Caim, created for this engagement)
Reset requests issued per account: 60, spaced 2 to 5 seconds apart
Observation 1: token length is fixed at 8 numeric characters
Observation 2: [REDACTED] of 180 sampled tokens fell within a window narrower than the full keyspace,
indicating non-uniform generation
Observation 3: a second request did not invalidate the first token (both remained valid until expiry)
Outcome: password of a Virtual Caim test account was changed without access to its registered phone or inbox
```

Technique and statistical findings are described at summary level. The generation analysis and the exact attempt budget are held in the confidential evidence annex handed over to the named Point of Contact only.

Business impact

An attacker can take over any customer account whose username is known or guessable, including accounts with active loans and linked bank mandates. This exposes personal and financial data, allows unauthorised changes to contact details and communication preferences, and may allow initiation of requests on behalf of the customer. Because the flaw can be automated, it scales across the whole customer base.

The event would qualify as unauthorised access to IT systems and data and as identity theft under the incident types listed in Annexure I of the CERT-In Directions dated 28 April 2022, and would trigger the 6 hour reporting duty. It would also raise questions under the security safeguards expected of a Data Fiduciary (DPDP Act, 2023, section 8(5)).

Recommended remediation

1. Generate reset tokens with a cryptographically secure random generator, with at least 128 bits of entropy, and deliver them as a single-use link rather than a short numeric code.

2. Bind each token to the originating session or device, expire it within 15 minutes and invalidate all earlier tokens on every new request.
3. Apply per-account and per-source throttling on token requests and token submission, with alerting for sustained attempts.
4. Send a notification to the registered contact on every successful reset, and force logout of all active sessions after the change.
5. Add the reset flow to the regression suite so that a change to token handling cannot be released without review.

References

OWASP WSTG-ATHN-09 (Testing for Weak Password Change or Reset Functionalities); OWASP Forgot Password Cheat Sheet; CWE-640; NIST SP 800-63B, section on look-up secrets and out-of-band authenticators.

SAMPLE

F-02

High

CVSS v3.1 base 7.1

Broken object-level authorisation on the loan statement API

Severity / score	High 7.1 `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N`
EPSS (illustrative)	0.18 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-639, CWE-284 | Not applicable (application logic flaw)
OWASP mapping	A01:2021 Broken Access Control; API1:2023 Broken Object Level Authorization | WSTG-ATHZ-04
Affected assets	Mobile API: /api/v2/loans/{id}/statements and /api/v2/loans/{id}/preferences
Closure target	15 days from notification (proposed, see section 9)

Description

The loan statement and preference endpoints accept a loan identifier in the request path. The service confirms that the caller is logged in but does not confirm that the loan belongs to the caller. A logged-in customer can therefore request statements, and change communication preferences, for loans belonging to other customers by changing the identifier.

Loan identifiers are sequential, which removes the practical barrier of guessing. The mobile application and the web portal share this API, so both are affected.

Evidence

Cross-account read (sanitized)

```
Caller: test customer A (session token [REDACTED])
Request : GET /api/v2/loans/[loan ID belonging to test customer B]/statements/2026-08
Result  : HTTP 200, statement for test customer B returned (name, address, EMI schedule, masked account number)
Control : same request without a session token returned HTTP 401, confirming authentication is enforced but
ownership is not
Scope of testing: two Virtual Caim test customers only; no real customer record was requested
```

Only data of accounts created for the engagement was accessed. Identifiers in this extract are fictional.

Business impact

Any registered customer can read the loan statements and personal details of other customers and alter their communication preferences, which could be misused to suppress alerts before a fraud attempt. At the volume of a typical retail lending book, this is a reportable personal data breach scenario and a direct regulatory concern for an NBFC.

Recommended remediation

1. Enforce ownership checks on the server for every object reference: derive the customer from the authenticated session and compare it to the owner of the requested loan before any data is returned or changed.
2. Replace sequential identifiers with non-guessable identifiers as a defence in depth step. This is not a substitute for the ownership check.
3. Centralise authorisation in a shared policy layer or middleware so that new endpoints inherit the check by default.
4. Add automated authorisation tests (two users, cross-access attempts) to the CI pipeline for every API route that takes an object identifier.
5. Log denied cross-account attempts and alert on repeated denials from one session.

References

OWASP API Security Top 10 (2023) API1; OWASP WSTG-ATHZ-04 (Testing for Insecure Direct Object References); OWASP Authorization Cheat Sheet; CWE-639.

F-03

High

CVSS v3.1 base 7.4

No effective limit on one-time password (OTP) verification attempts

Severity / score	High 7.4 `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N`
EPSS (illustrative)	0.09 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-307, CWE-799 | Not applicable (application logic flaw)
OWASP mapping	A07:2021 Identification and Authentication Failures; API4:2023 Unrestricted Resource Consumption | WSTG-ATHN-03
Affected assets	Customer Web Portal and Mobile API (login OTP and transaction OTP verification)
Closure target	15 days from notification (proposed, see section 9)

Description

The OTP verification step for login and for sensitive profile changes accepts repeated incorrect values without locking the OTP, the account or the source. The six-digit code has a short validity, but within that window the number of attempts was not restricted by the service. The edge protection (WAF) applies a generic request-rate rule, but the rule is per IP address and was not triggered by a low, steady request rate.

Evidence

Attempt handling (sanitized)

```
Test account: Virtual Caim test customer 2
Attempts sent within a single OTP validity window: [REDACTED] (well above the limit expected by policy)
Responses: uniform HTTP 400 with a generic message; no lock-out, no CAPTCHA, no delay, no alert to the account holder
WAF behaviour: no block observed at the tested request rate
Environment note: test performed on the UAT stack with production-equivalent configuration, as agreed
```

The number of attempts and the timing profile are redacted in this sample.

Business impact

Where an attacker already holds the first factor (for example from a credential leak), the second factor can be defeated by repeated guessing. Weak OTP handling also undermines transaction authorisation for profile changes. Industry practice and regulator expectations on authentication for financial services are based on the second factor being a real barrier.

Recommended remediation

1. Allow no more than 3 to 5 incorrect OTP submissions per issued OTP, then invalidate it and require a new one.
2. Add progressive delay and temporary account lock after repeated failed verifications, with notification to the customer.
3. Key rate limits on account and device as well as on IP address, so that distributed attempts are covered.
4. Tune WAF rules for the authentication endpoints and forward the events to the monitoring platform with a dedicated alert.

References

OWASP WSTG-ATHN-03 (Testing for Weak Lock Out Mechanism); OWASP API Security Top 10 (2023) API4; CWE-307.

F-04

High

CVSS v3.1 base 7.6

Stored cross-site scripting in the back-office support ticket viewer

Severity / score	High 7.6 `CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N`
EPSS (illustrative)	0.07 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-79 | Not applicable (application specific)
OWASP mapping	A03:2021 Injection | WSTG-INPV-02
Affected assets	Back-office console: Support > Tickets (subject and description fields, rendered in the officer view)
Closure target	15 days from notification (proposed, see section 9)

Description

Text submitted by a customer in a support ticket is stored and later displayed to the back-office officer in the console. The subject field is encoded correctly in the list view, but the ticket detail view renders part of the description as HTML without output encoding. Content with active markup therefore executes in the officer's browser, with the officer's privileges, when the ticket is opened.

The console sits on a different internal origin, so this is a cross-boundary flaw: input from the internet-facing portal affects a privileged internal session.

Evidence

Non-executing proof marker (sanitized)

```
Customer-side input : benign marker string containing HTML metacharacters [payload withheld]
Officer-side result : marker rendered as markup instead of text in the ticket detail view (confirmed in DOM
inspection)
Execution context   : back-office console origin; session cookie flagged HttpOnly, so direct cookie theft not
possible,
                      but actions in the officer's session (approve, reassign, export) are reachable from
script
Test limits         : executed only against a test officer account; no data was read, changed or exported
```

Only a harmless marker was used. No working payload is reproduced in this report.

Business impact

A customer, or an attacker posing as one, can run actions inside an officer's authenticated session. Depending on the officer's role this may include viewing other customers' records, changing ticket status, or exporting data. The change of security scope (internet user to internal privileged session) is why the score is High despite the need for the officer to open the ticket.

Recommended remediation

1. Apply context-aware output encoding to every field rendered in the console, using the framework's default escaping instead of raw HTML insertion.
2. If rich text is a business requirement, sanitise with a maintained allow-list sanitiser on the server and render in a sandboxed container.
3. Add a restrictive Content Security Policy to the console (no inline script, restricted sources) as a second layer.
4. Review other places where customer-supplied text reaches the console (feedback forms, KYC remarks, chat transcripts) using the same test.

References

OWASP WSTG-INPV-02 (Testing for Stored Cross Site Scripting); OWASP XSS Prevention Cheat Sheet; CWE-79.

F-05

Medium

CVSS v3.1 base 5.4

Sessions remain valid after logout and idle timeout is too long

Severity / score	Medium 5.4 `CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:N`
EPSS (illustrative)	0.04 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-613 | Not applicable (application logic flaw)
OWASP mapping	A07:2021 Identification and Authentication Failures | WSTG-SESS-06, WSTG-SESS-07
Affected assets	Customer Web Portal
Closure target	30 days from notification (proposed, see section 9)

Description

Logging out of the portal removes the session cookie from the browser but does not invalidate the session on the server. A copy of the session identifier, if captured earlier, continues to work. The idle timeout is configured at 12 hours, and the absolute session lifetime is not enforced.

Evidence

Session lifecycle check (sanitized)

```
Step 1: log in as test customer; note session identifier (value redacted)
Step 2: perform Logout in the UI; browser cookie cleared
Step 3: replay a saved request with the old session identifier
Result: HTTP 200 and authenticated content returned; session still active 40 minutes after logout
Idle timeout observed: no expiry within 6 hours of inactivity (configuration review shows 12 hours)
```

Timing values are from the UAT stack.

Business impact

Customers using shared or public devices, and anyone whose session identifier is exposed through a log, proxy or malware, remain exposed after they believe they have signed out. The risk is moderate on its own, but it increases the impact of other findings (for example F-04).

Recommended remediation

1. Invalidate the server-side session record on logout and on password change.
2. Reduce idle timeout to 10 to 15 minutes for authenticated financial screens and set an absolute lifetime (for example 8 hours).
3. Rotate the session identifier after login and privilege change.
4. Confirm that session cookies carry Secure, HttpOnly and SameSite attributes on all environments.

References

OWASP WSTG-SESS-06 and SESS-07; OWASP Session Management Cheat Sheet; CWE-613.

SAMPLE

F-06

Medium

CVSS v3.1 base 6.1

Outdated JavaScript library with known vulnerabilities (jQuery 3.4.1)

Severity / score	Medium 6.1 `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N`
EPSS (illustrative)	0.02 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-79 | CVE-2020-11022, CVE-2020-11023
OWASP mapping	A06:2021 Vulnerable and Outdated Components | WSTG-INFO-08
Affected assets	Customer Web Portal and DSA Portal (static script bundle)
Closure target	30 days from notification (proposed, see section 9)

Description

The front-end bundle includes jQuery version 3.4.1. Versions before 3.5.0 are affected by publicly documented cross-site scripting issues in HTML handling (CVE-2020-11022 and CVE-2020-11023). Identification was version-based. We reviewed the application code paths that pass data to the affected functions and found no confirmed reachable path in the tested release, so the practical exploitability is low today, but the component remains a latent risk for any future code change.

Evidence

Component identification (sanitized)

```
Asset   : portal static bundle, vendor script
Version : 3.4.1 (from file header and runtime version property)
Advisory: public CVE entries cited above; fixed in 3.5.0 and later
Code-path review: no confirmed reachable use of the affected functions with user-controlled input in the tested release
```

Score shown is the CVSS base score of the published advisory, adjusted to this context only where stated.

Business impact

If a developer later passes user-controlled content to the affected functions, the library will not protect the application. Unpatched third-party components are also flagged by most due-diligence questionnaires from regulators and partners.

Recommended remediation

1. Upgrade jQuery to the current maintained release and run the front-end regression suite.
2. Introduce software composition analysis in the build pipeline with a policy to fail the build on known high-severity advisories.
3. Maintain an inventory of front-end libraries with owners and update intervals.

References

NVD entries for CVE-2020-11022 and CVE-2020-11023; jQuery 3.5.0 release notes; OWASP Top 10 (2021) A06.

SAMPLE

F-07

Medium

CVSS v3.1 base 5.3

Legacy TLS protocol versions and weak cipher suites on the partner gateway

Severity / score	Medium 5.3 `CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N`
EPSS (illustrative)	0.01 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-326, CWE-327 | Not applicable (configuration weakness)
OWASP mapping	A02:2021 Cryptographic Failures | WSTG-CRYP-01
Affected assets	Partner gateway (external IP, redacted range 203.0.113.0/28, HTTPS service)
Closure target	30 days from notification (proposed, see section 9)

Description

The partner-facing HTTPS gateway still negotiates TLS 1.0 and TLS 1.1 and offers cipher suites that use CBC mode with SHA-1 and 3DES. The portal and API hosts are configured correctly (TLS 1.2 and 1.3 only). The gateway appears to carry a legacy compatibility profile that was kept for older partner integrations.

Evidence

Protocol and cipher review (sanitized)

```
Service  : partner gateway, port 443
Enabled  : TLS 1.0, TLS 1.1, TLS 1.2 (TLS 1.3 not offered)
Weak     : 3DES-based and SHA-1 CBC suites offered
Forward secrecy: available on TLS 1.2 suites, not enforced
Certificate: valid, 2048-bit RSA, chain complete
```

Scan output summarised. Host names are fictional.

Business impact

Exploiting legacy protocol weaknesses is difficult and needs a network position between the partner and the gateway, which is why the likelihood is limited. The finding still matters because PCI DSS, RBI expectations and most partner security reviews call for modern TLS, and because the traffic includes partner credentials and customer data.

Recommended remediation

1. Disable TLS 1.0 and 1.1 and remove 3DES and SHA-1 CBC suites. Enable TLS 1.3.
2. Agree a cut-off date with the partners that still use legacy clients, and publish the supported configuration.
3. Add a TLS scan to the monthly external hygiene check and track results.

References

OWASP WSTG-CRYP-01; RFC 8996 (deprecating TLS 1.0 and 1.1); NIST SP 800-52 Rev. 2; CWE-326.

F-08

Low

Verbose error messages and framework version disclosure

CVSS v3.1 base 3.7

Severity / score	Low 3.7 `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N`
EPSS (illustrative)	0.01 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-209, CWE-200 | Not applicable (information exposure)
OWASP mapping	A05:2021 Security Misconfiguration | WSTG-ERRH-01, WSTG-INFO-02
Affected assets	Mobile API (malformed request handling), Customer Web Portal (HTTP response headers)
Closure target	90 days from notification (proposed, see section 9)

Description

Malformed input to two API routes returns a stack trace that names internal class paths and the framework version. HTTP response headers on the portal also disclose the web server and framework version. This helps an attacker to select known issues for the exact version, although it does not give access on its own.

Evidence

Error handling (sanitized)

```
Route    : POST /api/v2/support/feedback with malformed JSON body
Response : HTTP 500 with trace containing internal package names and framework version [REDACTED]
Header   : Server and X-Powered-By headers present on portal responses
```

Class names and versions are redacted in this sample.

Business impact

Low direct impact. It shortens the reconnaissance effort of an attacker and can make a later finding easier to exploit.

Recommended remediation

1. Return a generic error body with a correlation identifier and log the details server-side.
2. Remove or neutralise version-revealing headers at the web server and the reverse proxy.
3. Set the framework to production mode for all internet-facing environments.

References

OWASP WSTG-ERRH-01; OWASP Error Handling Cheat Sheet; CWE-209.

SAMPLE

F-09

Low

CVSS v3.1 base 3.1

Missing clickjacking protection and HTTP Strict Transport Security

Severity / score	Low 3.1 `CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N`
EPSS (illustrative)	0.01 probability of exploitation in 30 days (sample value)
CWE / CVE	CWE-1021, CWE-319 | Not applicable (configuration weakness)
OWASP mapping	A05:2021 Security Misconfiguration | WSTG-CLNT-09, WSTG-CONF-07
Affected assets	DSA (agent) Portal
Closure target	90 days from notification (proposed, see section 9)

Description

The DSA portal can be loaded inside a frame on another origin because neither a frame-ancestors policy nor X-Frame-Options is returned. The portal also does not send the Strict-Transport-Security header, so a first visit over plain HTTP can be downgraded in a hostile network.

Evidence

Header review (sanitized)

```
Response headers on authenticated pages: Content-Security-Policy (frame-ancestors) absent, X-Frame-Options absent, Strict-Transport-Security absent
Frame test: portal login page rendered inside a frame on a Virtual Caim test origin
```

Test origin belongs to Virtual Caim.

Business impact

Low. A deceptive overlay could trick an agent into clicking on a hidden control, and a network attacker could downgrade a first connection. Both need user interaction and a favourable position.

Recommended remediation

1. Send Content-Security-Policy: frame-ancestors 'self' (and X-Frame-Options: DENY for older browsers).
2. Send Strict-Transport-Security with a max-age of at least 12 months and consider preload after verifying all subdomains.
3. Add the headers at the reverse proxy so that every application inherits them.

References

OWASP WSTG-CLNT-09 and CONF-07; OWASP Secure Headers Project; CWE-1021.

SAMPLE

6. Informational observations

These items do not carry a CVSS score. They are included for completeness and for regulatory alignment.

ID	Observation	Detail and recommendation
I-01	Permissive CORS policy on public static-asset endpoint	No sensitive data is served from the endpoint. Recommend restricting to known origins during the next release.
I-02	Application log retention declared at 90 days on the web tier	Declared by the client and not independently verified. CERT-In Directions (28 April 2022), direction (iv), require logs of ICT systems to be kept for a rolling 180 days within Indian jurisdiction. Recommend aligning retention and confirming storage location.
I-03	No published vulnerability disclosure contact	Recommend a security.txt file and a monitored mailbox so that external researchers have a route to report issues.

Controls that held up under testing

Area	Result
SQL injection	Not found in 60 routes tested with parameterised input and manual probing
File upload	Type and size enforcement effective; content stored outside web root
Back-office authentication	Second factor enforced; no default credentials
Transport security (portal, API)	TLS 1.2 and 1.3 only, strong suites, valid certificate chain
Cross-site request forgery	Anti-forgery tokens present on state-changing requests
Admin exposure	No administrative interface reachable from the internet

SAMPLE

7. Risk matrix

The matrix places each finding by likelihood (how easy and how probable exploitation is, informed by EPSS and attacker effort) and impact (data, financial and regulatory consequence). It is a planning aid for management and sits alongside, not instead of, the CVSS score.

Likelihood / Impact	Minor	Moderate	Major	Severe
Very likely				F-01
Likely			F-02, F-03	
Possible		F-05, F-06	F-04	
Unlikely	F-08, F-09	F-07		

Reading the matrix

- F-01 sits alone in the highest cell: easy to exploit, severe consequence, and not dependent on user mistakes.
- F-02 and F-03 are likely to be found by any motivated user or attacker of the platform. Both feed the same outcome as F-01 (unauthorised access to customer data).
- F-04 needs an officer to open a ticket, which lowers likelihood but not the impact on a privileged session.
- F-05 to F-09 are hygiene items that matter mainly in combination with the items above.

Attack path view

The three findings F-01, F-03 and F-05 form a realistic chain. An attacker who obtains a reset token (F-01) takes control of an account. If the customer later notices and logs out of an old session, that session can persist (F-05). Where a second factor is in place, F-03 weakens it. Closing F-01 and F-03 breaks the chain even before F-05 is fixed.

SAMPLE

8. Remediation roadmap

The roadmap sequences work by risk and by dependency. Dates are counted from the issue of this report (21 October 2026).

Wave	Window	Items	Outcome	Suggested owner
0. Contain	Days 0 to 7	F-01 (fix or temporary compensating control: disable self-service reset for high-value accounts, add throttling at WAF)	Account takeover path closed	Engineering lead, SOC
1. Fix	Days 8 to 15	F-02, F-03, F-04	Authorisation, OTP and console encoding corrected	API team, back-office team
2. Strengthen	Days 16 to 30	F-05, F-06, F-07	Session lifecycle, library upgrade, TLS profile	Platform and DevOps
3. Harden	Days 31 to 90	F-08, F-09, I-01 to I-03	Error handling, headers, CORS, retention, disclosure contact	Platform, GRC
4. Prevent	Quarter after	Authorisation test suite, SCA in CI, secure coding refresher, periodic re-test	Root causes addressed, fewer repeat findings	CISO, Engineering

Root-cause themes

- **Authorisation by convention, not by design.** Ownership checks are written per endpoint. A central policy layer prevents omissions.
- **Security controls without negative tests.** Rate limits and token rules exist on paper but are not tested for abuse.
- **Dependency and configuration drift.** Libraries and TLS profiles are not on a regular review cycle.

Estimated effort (indicative)

Item	Engineering effort	Dependency
F-01 and F-03	6 to 10 person-days	Product sign-off on reset journey
F-02	5 to 8 person-days	Shared authorisation middleware
F-04	2 to 4 person-days	Template review
F-05 to F-09	6 to 9 person-days	Release calendar, partner notice for TLS

SAMPLE

9. Re-test and closure policy

A finding is closed only when it has been verified by the assessment team. The report is not treated as final until the follow-up verification is complete for the in-scope production system, and a limited-scope statement is issued if only staging was tested.

Step	What happens	Who
1. Fix notification	Client informs the Lead Auditor which findings are fixed, with the build version and hash.	Client Point of Contact
2. Re-test window	Targeted re-test of each fixed finding and of closely related routes. Typically within 5 working days of the request.	Virtual Caim
3. Outcome per finding	Closed, Partially closed (with residual risk noted) or Open.	Virtual Caim
4. Closure report	Issued with updated status, evidence and the tested build hash. A closure statement is signed by the Lead Auditor and the Head of the auditing organisation.	Virtual Caim
5. Further rounds	Number of re-test rounds and chargeability are agreed in the engagement terms (sample: two included).	Both

> **VALIDITY**
> A report describes the state of security at the point in time of testing. Any significant change to code, infrastructure or configuration after the tested build calls for a new or delta assessment. For regulated entities, the frequency of VAPT is set by the board-approved policy and the applicable regulator.

Closure status template

ID	Reported	Fix claimed	Re-test date	Status	Residual risk
F-01	21 Oct 2026	-	-	Open	-
F-02	21 Oct 2026	-	-	Open	-
F-03	21 Oct 2026	-	-	Open	-
F-04	21 Oct 2026	-	-	Open	-
...					

SAMPLE

Annex A. Compliance mapping

This annex relates the findings to external requirements. It is a mapping for planning and is not a legal opinion or a certification.

A.1 CERT-In Directions, 28 April 2022 (section 70B(6), IT Act, 2000)

Direction	Requirement (summary)	Relevance to this assessment
(i)	Synchronise ICT system clocks with NIC or NPL NTP servers, or sources traceable to them	Time source not in scope. Recommended check during log retention review (I-02).
(ii)	Report listed cyber incidents to CERT-In within 6 hours of noticing them (Annexure I lists 20 incident types)	F-01, F-02, F-04 describe conditions that would be reportable if exploited (unauthorised access, identity theft, data breach, attacks on applications).
(iii)	Designate a Point of Contact to interface with CERT-In	Client confirmed a designated Point of Contact exists (not independently verified).
(iv)	Enable and maintain logs of all ICT systems for a rolling 180 days, within Indian jurisdiction	I-02: declared 90 day retention on the web tier.

A.2 ISO/IEC 27001:2022, Annex A controls

Control	Title	Findings
A.5.15	Access control	F-02
A.5.17	Authentication information	F-01, F-03
A.8.3	Information access restriction	F-02
A.8.5	Secure authentication	F-01, F-03, F-05
A.8.8	Management of technical vulnerabilities	F-06, F-07
A.8.9	Configuration management	F-07, F-08, F-09
A.8.15	Logging	I-02
A.8.24	Use of cryptography	F-07
A.8.26	Application security requirements	F-01 to F-04
A.8.28	Secure coding	F-04, F-08
A.8.29	Security testing in development and acceptance	All (this assessment is evidence)

A.3 RBI expectations for regulated entities

Source	Expectation (summary)	Relevance
RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023)	Board-approved IT and cyber security policy, risk-based controls, periodic independent assurance including vulnerability assessment and penetration testing, and incident reporting to the regulator	This assessment is a form of periodic assurance. Findings F-01 to F-04 should be tracked in the IT risk register with owners. Applicability depends on the entity's regulatory layer and should be confirmed by the client's compliance team.

A.4 Data protection

Source	Provision	Relevance
DPDP Act, 2023, section 8(5)	Data Fiduciary to protect personal data with reasonable security safeguards	F-01, F-02, F-04 bear on this duty.
DPDP Act, 2023, section 8(6)	Intimation of a personal data breach to the Data Protection Board and affected Data Principals	Incident response should cover the scenarios in F-01 and F-02.
DPDP Act, 2023, section 33 and Schedule	Monetary penalties after inquiry, with a ceiling of Rs 250 crore for failure to take reasonable security safeguards	Shows the scale of exposure. Penalty is imposed by the Board after inquiry.

Source	Provision	Relevance
IT Act, 2000, section 43A and SPDI Rules, 2011	Reasonable security practices for sensitive personal data, until the DPDP provisions replace them on commencement	Interim relevance for current operations.

The DPDP Rules, 2025 were notified in November 2025 with phased commencement (most obligations, including security safeguards and breach intimation procedure, from May 2027). Clients should confirm the current commencement position before relying on a date.

SAMPLE

Annex B. Test coverage and evidence register

B.1 Coverage by asset

Asset	Routes or hosts tested	Roles used	Manual hours (approx.)	Findings
Customer Web Portal	86 pages and flows	Customer (2)	78	F-01, F-03, F-05, F-06, F-08
Mobile API	340 routes	Customer (2)	92	F-02, F-03, F-08
DSA Portal	41 pages	Agent (1)	30	F-06, F-09
Back-office console	58 pages	Officer (1)	36	F-04
Partner gateway	3 hosts	None	8	F-07

B.2 Evidence register

Ref	Type	Related finding	Held in
E-001	Token sampling dataset (summary statistics)	F-01	Confidential annex
E-002	Request and response pairs, redacted	F-02	Confidential annex
E-003	Attempt log summary	F-03	Confidential annex
E-004	DOM inspection capture	F-04	Confidential annex
E-005	Session lifecycle notes	F-05	Confidential annex
E-006	TLS scan report	F-07	Confidential annex
E-007	Header capture	F-08, F-09	Confidential annex

HANDLING OF AUDIT DATA

Raw evidence is stored encrypted, shared only with the named Point of Contact, and disposed of on the date agreed in the engagement terms. Reports are sent from an official mailbox, password protected, with the password sent separately.

SAMPLE

Annex C. Glossary

Term	Meaning
API	Application programming interface.
ASVS	OWASP Application Security Verification Standard.
BOLA	Broken object-level authorisation: access to an object the user does not own.
CERT-In	Indian Computer Emergency Response Team, under MeitY.
CIA	Confidentiality, integrity, availability.
CORS	Cross-origin resource sharing.
CSP	Content Security Policy, a browser-enforced allow-list for content sources.
CVE	Common Vulnerabilities and Exposures identifier.
CVSS	Common Vulnerability Scoring System, version 3.1 used here.
CWE	Common Weakness Enumeration.
DPDP	Digital Personal Data Protection Act, 2023.
DSA	Direct selling agent.
EPSS	Exploit Prediction Scoring System.
HSTS	HTTP Strict Transport Security.
IDOR	Insecure direct object reference, an older name for BOLA.
MFA	Multi-factor authentication.
NBFC	Non-banking financial company.
OTP	One-time password.
PoC	Point of Contact (also proof of concept, where stated).
PTES	Penetration Testing Execution Standard.
SCA	Software composition analysis.
SPDI	Sensitive personal data or information.
TLS	Transport Layer Security.
UAT	User acceptance testing environment.
VAPT	Vulnerability assessment and penetration testing.
WAF	Web application firewall.
WSTG	OWASP Web Security Testing Guide.

CVSS v3.1 vector key

AV: attack vector (N network, A adjacent, L local, P physical). AC: attack complexity (L low, H high). PR: privileges required (N none, L low, H high). UI: user interaction (N none, R required). S: scope (U unchanged, C changed). C, I, A: impact on confidentiality, integrity, availability (H high, L low, N none).

Annex D. Sign-off

The report is signed by the auditors who performed the assessment, reviewed and signed by a designated reviewer who was not part of the test team, and authorised by the head of the auditing organisation. Signature blocks below are shown for format only; this is a sample and carries no signatures.

Auditor(s)	Independent reviewer	Head of auditing organisation
Name, ID, date (sample)	Name, designation, date (sample)	Name, designation, date (sample)

FICTIONAL ENGAGEMENT

Example Finserv Ltd., its systems, people, addresses, hosts, findings and scores are invented for illustration. Any resemblance to a real organisation is unintended. Virtual Caim prepares real reports on this structure for real clients, with scope, evidence and sign-off specific to the engagement.

SAMPLE