Bachao.AI

BACHAO.AI · SECURITY ASSESSMENT REPORT

At***** — Production Security Assessment (Sample · Client Identity Redacted)

Vulnerability Assessment & Penetration Test — Verification Platform (Black-box + Grey-box)

Sample deliverable — a real Bachao.AI engagement with the client name, domains and IP addresses redacted (shown as asterisks). eKYC / identity-verification platform — public APIs, application and customer dashboard.

TLP:AMBER · Confidential

Prepared for: **At*****

Prepared by: **Bachao.AI — Dhisattva AI Pvt Ltd (DPIIT-Recognised Startup)**

Assessment: **15 August 2026**

Certificate No.: **BVPT-SAMPLE-2026-0005** · Classification: **TLP:AMBER — Confidential**

✔ No Critical or High severity findings

7 findings identified (0 Critical · 0 High · 1 Medium · 4 Low · 2 Informational). Remediation guidance and a path to the all-green certificate are provided.

Sample deliverable — do not scan

This is a masked demonstration report; the certificate reference is **not a live verification**. Real client certificates carry a scannable, OTP-authenticated QR at **bachao.ai/verify**.

Contents

The report is organised as follows.

1 Document Control

Report title	At***** — Production Security Assessment (Sample · Client Identity Redacted)
Client	Pe******** IQ Solutions Private Limited
Certificate / Reference No.	BVPT-SAMPLE-2026-0005

Engagement	Vulnerability Assessment & Penetration Test — Verification Platform (Black-box + Grey-box)
Assessment type	Black-box + Authenticated Grey-box
Assessment window	15 August 2026
Report version	1.0 — Final
Classification	CONFIDENTIAL — restricted to At***** & Bachao.AI
Assessor	Bachao.AI — Dhisattva AI Pvt Ltd (DPIIT-Recognised Startup)
Standards	CERT-In-aligned · ISO/IEC 27001:2022 · SOC 2 · GDPR · DPDP · OWASP · CVSS v3.1
Lead assessor	Shouvik Mukherjee — Lead Security Assessor
Verification	sample deliverable — reference not live

2 About This Assessment

Bachao.AI (Dhisattva AI Pvt Ltd) is a DPIIT-recognised cybersecurity and fraud-prevention company. This engagement was an authorised Vulnerability Assessment & Penetration Test (VAPT) of At*****'s internet-facing production surface, with prioritised remediation guidance. Testing combined unauthenticated black-box probing with authenticated grey-box testing (capture-and-replay of the application's real API calls under a valid session). The assessment was conducted to a **CERT-In-aligned methodology** and its findings are mapped to **ISO/IEC 27001:2022, SOC 2, GDPR and the DPDP Act 2023** control frameworks, following the **OWASP** Top 10 and API Security Top 10 testing standards and scored with **CVSS v3.1** — meeting Indian and international security-assessment benchmarks.

This report is confidential and intended for At*****. It may be shared with the client's customers, investors, auditors and regulators as independent evidence of the security testing performed.

3 Executive Summary

This is a sample deliverable: a real Bachao.AI engagement with the client name, domains and IP addresses redacted (shown as asterisks) to protect confidentiality — the findings, evidence and structure are the genuine report. Bachao.AI performed a black-box and authenticated grey-box VAPT of the At***** production platform — the verification APIs, the onboarding application and the customer dashboard. The platform processes PAN, Aadhaar, GST, bank and biometric data for banks and NBFCs, so testing was weighted to API authorization, verification-result integrity, tenant isolation and personal-data exposure, and every automated result was manually verified before inclusion. No Critical or High severity vulnerability was confirmed: authentication is enforced, and cross-origin theft of authenticated data is blocked. The findings are a single Medium CORS misconfiguration (with currently-capped impact) and a set of Low / Informational hardening items. Several high-severity automated signals — notably five SQL-injection flags — were verified as false positives and are documented in the annex. Notably, the customer-facing app and dashboard sit behind edge protection that actively rate-limited even our authorised testing — a genuine defensive control that we credit as positive assurance rather than a gap (see Coverage note).

0	0	1	4	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Posture: no Critical or High severity vulnerabilities were confirmed. The residual items are addressed with concrete remediation and a defined path to the all-green certificate (remediation + one re-test).

4 Scope of Work

The following assets were in scope. Testing was non-destructive and read-only: no data was deleted or altered, no active denial-of-service or load testing was performed, and no real personal data was exfiltrated. All activity is recorded in a timestamped forensic log.

HOST	ROLE	RESOLVES TO	STATUS
`api.at*****.com`	Production API (verification endpoints)	`13.***.***.***`	In scope
`app.at*****.com`	Candidate/guest onboarding application (Netlify)	—	In scope
`dashboard.at*****.com`	Customer console (Next.js, Netlify)	—	In scope

Authenticated testing. Grey-box testing used a client-provided Admin dashboard session (httpOnly cookie). Authenticated API behaviour was exercised to confirm access enforcement and that cross-origin data theft is blocked.

Coverage note: api.at*****.com (AWS) was scanned fully and cleanly. The customer-facing app.at*****.com and dashboard.at*****.com sit behind Netlify edge protection that rate-limits and blocks aggressive automated traffic — it throttled even our authorised, deliberately-gentle (sequential, low-rate) testing. We treat this as a POSITIVE control (see Positive Assurance), not a gap: it is exactly what should slow an opportunistic attacker. Automated coverage of these two hosts therefore reflects what the protection permits without disruption, supplemented by manual verification of the reported findings. If a deeper authenticated crawl of these hosts is desired, it can be arranged in a scheduled window by temporarily relaxing the edge rate-limit for the Bachao.AI test source — no permanent change and no client-side network configuration required.

5 Methodology

The engagement follows **OWASP ASVS Levels 1–2**, the **PTES** phases and **NIST SP 800-115** technical testing guidance, aligned to **CERT-In** reporting expectations.

1 · Reconnaissance & asset discovery

Passive discovery (Certificate Transparency, DNS) and active enumeration of the in-scope hosts, sub-domains, API base URLs and technology stack; TLS/transport and email-security posture.

2 · Automated assessment (curated, AI-native)

Our platform runs a curated suite covering the OWASP Top 10 and OWASP API Security Top 10 in isolated micro-VMs; every candidate finding is re-validated by a second pass to strip false positives before a human sees it.

3 · Authenticated grey-box (capture-replay)

Real sessions at each privilege level are captured and replayed with access-control tampering (BOLA/IDOR, function-level authorization, mass-assignment) — the class of flaw black-box structurally cannot find.

4 · Senior-led manual exploitation

Hands-on verification of business logic, tenant isolation and result-integrity abuse; every reported finding is manually reproduced with request/response evidence.

5 · Risk rating & reporting

Each finding is scored with CVSS v3.1, mapped to OWASP/CWE and the client's compliance frameworks, and written with a concrete, developer-ready remediation.

Tooling by phase

PHASE	REPRESENTATIVE TOOLING / CHECKS
Reconnaissance	Certificate Transparency (crt.sh), DNS / DNS-over-HTTPS, port & service enumeration, TLS inspection
Transport & TLS	openssl s_client, cipher/protocol & certificate-chain analysis
Email security	SPF / DKIM / DMARC record analysis via authoritative DoH lookups
Web & API	OWASP Top 10 / API Top 10 curated suite, HTTP method & header inspection, CORS probing
Authenticated	Session capture-replay harness with BOLA/IDOR/BFLA and mass-assignment tampering
Verification	Manual reproduction with curl / HTTP proxy; CVSS v3.1 scoring

6 Risk Rating Methodology

Severity is derived from the **CVSS v3.1** base score, adjusted by the assessor for business context (data sensitivity, exposure, exploitability).

SEVERITY	CVSS BAND	MEANING & EXPECTED ACTION
CRITICAL	9.0 – 10.0	Immediate exploitation risk; direct compromise of data or systems. Fix immediately.
HIGH	7.0 – 8.9	Serious impact; realistic exploitation path. Fix urgently.
MEDIUM	4.0 – 6.9	Moderate impact or conditional exploitation. Fix in the normal cycle.
LOW	0.1 – 3.9	Limited impact; defense-in-depth / hardening.
INFO	0.0	No direct security impact; informational / good-practice note.

7 Test Coverage

The assessment executed **512 individual checks** across the categories below; “observations” are candidate signals raised for analyst review (the confirmed subset, after verification, appears in §Detailed Findings).

CATEGORY	WHAT IT CHECKS	CHECKS	OBS.
API Security (OWASP API Top 10)	Auth on API routes, mass-assignment, excessive data exposure, rate limiting.	118	3
Attack-Surface & Recon	Subdomain discovery, DNS/TLS posture, technology fingerprinting, exposed services.	68	4
Authentication & Session	Login flows, API-key/token handling, session cookies, access enforcement.	92	2
Injection & Input Handling	SQLi, NoSQLi, command/template injection, XSS, deserialization, SSRF.	96	0

CATEGORY	WHAT IT CHECKS	CHECKS	OBS.
Security Misconfiguration	Headers, CORS, verbose errors, cache policy, soft-404 / catch-all responses.	84	5
Transport / DNS / Email Hygiene	TLS config, HSTS, SPF/DKIM/DMARC, DNSSEC, DNS TTL / rebinding checks.	54	2
Total		**512**	**16**

8 Findings Summary

ID	SEVERITY	FINDING	HOST	CVSS
F-01	MEDIUM	CORS reflects arbitrary Origin with Allow-Credentials on non-data responses	api.at*****.com	4.3
F-02	LOW	External scripts lack Subresource Integrity (SRI)	app.at*****.com	3.1
F-03	LOW	Technology / version information disclosed in headers	app.at*****.com / dashboard.at*****.com	3.7
F-04	LOW	Public Cache-Control may allow caching of sensitive responses	app.at*****.com / dashboard.at*****.com	3.1
F-05	LOW	DNSSEC not implemented	at*****.com	3.7
F-06	INFO	Soft-404 / catch-all 200 responses	api.at*****.com	—
F-07	INFO	Low DNS TTL (theoretical DNS-rebinding exposure)	api.at*****.com	—

9 Detailed Findings

F-01 MEDIUM ● OPEN

CORS reflects arbitrary Origin with Allow-Credentials on non-data responses

api.at*****.com · / and error responses

CVSS 4.3 · AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N · A05:2021 — Security Misconfiguration · CWE-942

Background. A CORS policy that reflects any Origin back in Access-Control-Allow-Origin together with Access-Control-Allow-Credentials: true lets a hostile web page read credentialed cross-origin responses. It is only exploitable where an endpoint actually returns readable data with those headers.

Description. The root and error (404) responses reflect an arbitrary supplied Origin (e.g. https://evil.com) together with Access-Control-Allow-Credentials: true.

Impact. Impact is CAPPED: the authenticated data endpoints (/api/v3/*) return HTTP 500 with NO Access-Control-Allow-Origin header to a disallowed origin, so a cross-origin browser cannot read the platform's authenticated data today. The reflection is a spec-violating misconfiguration that should be corrected before any endpoint returns data with these headers.

Evidence.

```
$ curl -sI -H 'Origin: https://evil.com' https://api.at*****.com/
  HTTP/2 200
  access-control-allow-origin: https://evil.com
  access-control-allow-credentials: true
$ curl -sI -H 'Origin: https://evil.com' -b '<session>' https://api.at*****.com/api/v3/
notification/search
  HTTP/2 500   (no access-control-allow-origin header => cross-origin read blocked)
```

Remediation. Replace Origin reflection with an explicit allowlist of trusted origins (app/dashboard.at*****.com). Never combine a reflected/wildcard Origin with Allow-Credentials: true. Apply the same policy uniformly across root, error and data responses.

Compliance. ISO 27001 A.8.26 (application security) · SOC 2 CC6.6 · DPDP S.8(4) reasonable safeguards

References. MITRE CWE-942 · OWASP A05:2021

F-02 LOW OPEN

External scripts lack Subresource Integrity (SRI)

app.at*****.com

CVSS 3.1 · AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N · A08:2021 — Software & Data Integrity Failures · CWE-353

Background. Without an integrity hash on third-party <script> tags, a compromise of the CDN or third-party host would let attacker-controlled JavaScript run in the application.

Description. Third-party scripts are loaded without a Subresource Integrity (integrity=…) attribute.

Impact. Supply-chain risk: a compromised third-party script would execute unchecked in the app.

Evidence.

```
External <script> tags on app.at*****.com carry no integrity/crossorigin attributes.
```

> **Remediation.** Add SRI hashes (integrity + crossorigin) to third-party scripts, or self-host and pin them.

Compliance. ISO 27001 A.8.26 · SOC 2 CC7.1 · DPDP —

References. MITRE CWE-353

F-03 LOW OPEN

Technology / version information disclosed in headers

app.at*****.com / dashboard.at*****.com

CVSS 3.7 · AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N · A05:2021 — Security Misconfiguration · CWE-200

Background. Server/framework and X-Powered-By banners help an attacker map the stack to known CVEs.

Description. Responses disclose server/framework identifiers and an X-Powered-By technology banner.

Impact. Information leakage that assists targeting; requires a matching CVE to exploit (AC:H).

Evidence.

```
Server and X-Powered-By headers present on the application/dashboard responses.
```

> **Remediation.** Suppress or genericise Server / X-Powered-By and framework version headers at the edge.

Compliance. ISO 27001 A.8.9 (configuration mgmt) · SOC 2 CC6.1 · DPDP —

References. MITRE CWE-200

F-04 LOW OPEN

Public Cache-Control may allow caching of sensitive responses

app.at*****.com / dashboard.at*****.com

CVSS 3.1 · AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N · A05:2021 — Security Misconfiguration · CWE-525

Background. Permissive Cache-Control on authenticated responses risks sensitive data being retained in shared/ browser caches.

Description. Some responses carry a public/permissive Cache-Control directive.

Impact. Potential caching of sensitive content in intermediary or browser caches.

Evidence.

```
Cache-Control observed permitting caching on responses that should be private/no-store.
```

Remediation. Set Cache-Control: no-store (or private, no-cache) on authenticated/sensitive responses.

Compliance. ISO 27001 A.8.9 · SOC 2 CC6.1 · DPDP S.8(4)

References. MITRE CWE-525

F-05 LOW OPEN

DNSSEC not implemented

at*****.com

CVSS 3.7 · AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N · A05:2021 — Security Misconfiguration · CWE-350

Background. Without DNSSEC, resolvers cannot cryptographically validate DNS answers for the domain.

Description. The zone is not signed with DNSSEC.

Impact. Marginally increased exposure to DNS spoofing/cache-poisoning. Defense-in-depth.

Evidence.

```
No DS/RRSIG records observed for at*****.com.
```

Remediation. Enable DNSSEC signing and publish the DS record at the registrar.

Compliance. ISO 27001 A.5.14 · SOC 2 CC6.7 · DPDP —

References. RFC 4033

F-06 INFO ● OPEN

Soft-404 / catch-all 200 responses

api.at*****.com

A05:2021 — Security Misconfiguration · CWE-1188

Background. A host that returns HTTP 200 for non-existent paths (soft-404) inflates automated scanners and can mask enumeration.

Description. Some nonsense paths return a 200 application shell rather than a true 404.

Impact. Informational — complicates scanning and can hide brute-force enumeration.

Evidence.

```
Nonsense paths under api.at*****.com return a 200 application shell on some routes.
```

> **Remediation.** Return a true 404/410 for unknown routes.

Compliance. ISO 27001 A.8.9 · SOC 2 CC6.1 · DPDP —

References. MITRE CWE-1188

F-07 INFO ● OPEN

Low DNS TTL (theoretical DNS-rebinding exposure)

api.at*****.com

A05:2021 — Security Misconfiguration · CWE-350

Background. Very low DNS TTLs can, in theory, aid DNS-rebinding against local services; low impact for a public API with no local-network trust.

Description. The A record TTL is very low (~24s).

Impact. Informational — theoretical rebinding aid; no direct impact on the public API.

Evidence.

```
DNS A-record TTL observed at ~24 seconds.
```

> **Remediation.** Use a moderate TTL unless a low value is operationally required.

Compliance. ISO 27001 A.5.14 · SOC 2 CC6.7 · DPDP —

References. MITRE CWE-350

10 Positive Assurance (Controls Verified)

The following controls were tested and found to be working correctly — evidence that the platform is soundly engineered, not merely an absence of findings:

- Authentication is enforced — unauthenticated API calls are rejected (error 4011); the API key auth path returns 4016 for un-provisioned services rather than leaking data.
- Cross-origin theft of authenticated data is BLOCKED — the /api/v3 data endpoints return HTTP 500 with no Access-Control-Allow-Origin header to a disallowed origin, so a hostile web page cannot read the platform's authenticated responses.

- Session-namespace API routes are gated on the Origin header (only app/dashboard.at*****.com pass), adding a second barrier beyond authentication.
- Edge protection on the app and dashboard actively rate-limits and blocks aggressive automated traffic — it throttled even Bachao.AI's authorised, deliberately-gentle scanning. This is a genuine defensive control that raises the cost of opportunistic scanning, brute-force and bot attacks against the customer-facing hosts (it is not a substitute for application-layer security, and does not stop a patient targeted attacker, but it is a real and effective first line of defence).

11 Excluded / Verified False Positives

In the interest of an honest, vendor-grade report, the following automated signals were investigated and **excluded** after manual verification:

- **SQL Injection 'Possible' on api.at*****.com (5 signals).** Verified false positive — an injection payload and a benign baseline return identical HTTP 500 (no differential behaviour); the flags are a heuristic on the API's uniform error responses, not an injection.
- **Prototype pollution via query parameters.** Not reproduced — no reflected pollution effect was observed; flagged during a rate-limited scan and unconfirmed.
- **Origin server directly accessible (WAF bypass).** Unconfirmed — flagged during the rate-limited app/dashboard scan; not reproduced.
- **Hardcoded secrets in JavaScript bundles.** Not reproduced in the current app bundle. A prior recon noted a Google Maps key; it could not be re-located, so it is not asserted here — flagged for the recommended deeper pass.
- **CORS finding on qa.api.at*****.com.** Excluded — qa.api.at*****.com is OUT OF SCOPE (scope is api/app/dashboard.at*****.com).

12 Compliance Mapping

The methodology and every finding are tested, rated and reported against the frameworks the client's enterprise customers and auditors ask about — one engagement, evidence reusable across all.

FRAMEWORK	HOW THIS ENGAGEMENT ALIGNS
CERT-In (India)	Report produced in CERT-In format with full evidence and proof-of-testing; findings carry CVSS v3.1, affected asset, reproduction and remediation.
DPDP Act 2023 — Schedule I	For a platform processing PAN/Aadhaar/GST/bank/biometric data, findings are referenced to the S. 8(4) reasonable-security-safeguards obligation.
RBI IT Framework	Findings mapped to the RBI IT/cyber-security framework controls the platform's banking/NBFC customers require of their vendors.
SEBI CSCRF	Referenced to SEBI Cyber-Security & Cyber-Resilience Framework controls for regulated-market customers.
ISO/IEC 27001:2022 Annex A	Referenced to A.8.9 configuration, A.8.26 application security and A.5.14 information transfer.
OWASP · CVSS · PTES · NIST	OWASP Top 10 & API Security Top 10, ASVS L1–L2, PTES, NIST SP 800-115; every finding scored with CVSS v3.1.

13 Standards Coverage & Control Cross-Reference

OWASP Top 10:2021 — coverage & result

OWASP TOP 10:2021	COVERAGE	RESULT
A01:2021 Broken Access Control	Tested (authenticated BOLA/IDOR/BFLA)	No issue
A02:2021 Cryptographic Failures	Tested (TLS, cert, transport)	No issue (strong TLS)
A03:2021 Injection	Tested (SQLi/XSS/command/template)	No issue
A04:2021 Insecure Design	Reviewed (business logic, workflow)	No issue
A05:2021 Security Misconfiguration	Tested (headers, CORS, DMARC, exposure)	Findings — see §Findings
A06:2021 Vulnerable Components	Tested (version fingerprinting, known-CVE)	Informational (version disclosure)
A07:2021 Auth & Identification Failures	Tested (auth, session, MFA, origin)	Low (defense-in-depth)
A08:2021 Software & Data Integrity	Reviewed	No issue
A09:2021 Logging & Monitoring	Out of test scope (internal)	N/A
A10:2021 SSRF	Tested (candidate endpoints)	No issue (production)

Per-finding control cross-reference

Each finding mapped to the specific ISO/IEC 27001:2022 Annex A control, SOC 2 Common Criteria and DPDP Act 2023 obligation an auditor will ask about.

FINDING	OWASP	CWE	ISO 27001:2022	SOC 2	DPDP 2023
F-01	A05:2021 — Security Misconfiguration	CWE-942	A.8.26 (application security)	CC6.6	S.8(4) reasonable safeguards
F-02	A08:2021 — Software & Data Integrity Failures	CWE-353	A.8.26	CC7.1	—
F-03	A05:2021 — Security Misconfiguration	CWE-200	A.8.9 (configuration mgmt)	CC6.1	—
F-04	A05:2021 — Security Misconfiguration	CWE-525	A.8.9	CC6.1	S.8(4)
F-05	A05:2021 — Security Misconfiguration	CWE-350	A.5.14	CC6.7	—
F-06	A05:2021 — Security Misconfiguration	CWE-1188	A.8.9	CC6.1	—
F-07	A05:2021 — Security Misconfiguration	CWE-350	A.5.14	CC6.7	—

14 Remediation Roadmap

SEVERITY	TIMELINE	FINDINGS	ITEMS
MEDIUM	Within 2–4 weeks	F-01	CORS reflects arbitrary Origin with Allow-Credentials on non-data responses
LOW	Next maintenance cycle	F-02, F-03, F-04, F-05	External scripts lack Subresource Integrity (SRI); Technology / version information disclosed in headers; Public Cache-Control may allow caching of sensitive responses; DNSSEC not implemented
INFO	Optional / good practice	F-06, F-07	Soft-404 / catch-all 200 responses; Low DNS TTL (theoretical DNS-rebinding exposure)

Recommended remediation SLAs (CERT-In / RBI-aligned)

SEVERITY	RECOMMENDED REMEDIATION SLA	GUIDANCE
CRITICAL	≤ 7 days	Emergency change; fix before anything else.
HIGH	≤ 14 days	Prioritised fix in the current cycle.
MEDIUM	≤ 30 days	Normal change management.
LOW	≤ 90 days	Next maintenance window.
INFO	Best-effort	Good-practice hardening.

One post-fix re-test is included in this engagement. On confirmation that the Critical, High and Medium findings are remediated and re-tested clean, the signed all-green security certificate is issued for the assessed scope.

15 Next Steps & Contact

1. Review this report with your engineering and compliance teams.
2. Remediate the findings using the developer-ready guidance in §Detailed Findings, prioritised by the Remediation Roadmap SLAs.
3. Notify Bachao.AI when the fixes are deployed; we run the **included post-fix re-test**.
4. On a clean re-test, the signed **all-green security certificate** is issued for the assessed scope — the artefact you share with customers, investors and auditors.

Point of contact. Bachao.AI · Dhisattva AI Pvt Ltd · ceo@bachao.ai · Sample deliverable — certificate reference not live

16 Annex — Evidence Pack (Live Test Captures)

Verbatim commands and responses captured during testing, reproducing the confirmed findings and the key positive-assurance controls. Redacted of any sensitive values.

CORS reflection on non-data responses (F-01)

```
curl -sI -H 'Origin: https://evil.com' https://api.at*****.com/
  access-control-allow-origin: https://evil.com
  access-control-allow-credentials: true
```

Authenticated data endpoint is protected (positive control)

```
curl -sI -H 'Origin: https://evil.com' -b '<session>' https://api.at*****.com/api/v3/notification/search
  HTTP/2 500   (no ACAO header => cross-origin read blocked)
```

SQL Injection flag is a false positive

```
baseline : curl -s -o /dev/null -w '%{http_code}' https://api.at*****.com/api/v2/f****/guest/invite  => 500
injection: curl ... /api/v2/f****/guest/invite%27%20OR%201=1--  => 500   (identical => not SQLi)
```

17 Annex — Test Register (Proof of Testing)

Representative enumeration of the 512 checks executed, by category, with the observed result. “Observation(s)” denotes a candidate signal raised for analyst review; the verified subset appears in §Detailed Findings.

API Security (OWASP API Top 10)

Security checks in this category.

TEST	RUNS	RESULT
Authentication enforced on data endpoints (/api/v3/*)	24	Pass (correct)
Cross-origin credentialed read of authenticated data	16	Blocked (positive control)
Mass-assignment / excessive data exposure on API routes	18	No issue
API-key auth path for un-provisioned services	10	Pass (no data leak)

Security Misconfiguration

Security checks in this category.

TEST	RUNS	RESULT
CORS Origin reflection with Allow-Credentials	14	Observation — Medium (capped impact)
Security response headers (HSTS / CSP / X-Frame-Options)	20	Observation
Public / permissive Cache-Control on responses	12	Observation
Soft-404 / catch-all 200 responses	9	Informational

Transport / DNS / Email Hygiene

Security checks in this category.

TEST	RUNS	RESULT
SPF hard-fail on primary domain	4	Pass (correct)
DKIM signing present	4	Pass (correct)

TEST	RUNS	RESULT
DNSSEC signing	3	Observation — recommended
DNS A-record TTL	3	Informational

18 Annex — Tools & Techniques

- Bachao.AI VAPT engine (curated OWASP/API test suite, isolated micro-VM execution)
- Authenticated capture-replay harness (SPA session capture, BOLA/IDOR tampering)
- Manual tooling: curl, OpenSSL, DNS-over-HTTPS resolvers, HTTP proxy

19 Annex — Glossary

TERM	MEANING
BOLA / IDOR	Broken Object Level Authorization — a user reaches another user's object by id.
BFLA	Broken Function Level Authorization — access to functions above one's privilege.
CVSS v3.1	Common Vulnerability Scoring System — the standard 0–10 severity score.
CORS	Cross-Origin Resource Sharing — browser policy controlling cross-site reads.
DMARC	Domain-based Message Authentication — email anti-spoofing policy.
SSRF	Server-Side Request Forgery — coercing the server to make attacker-chosen requests.
Soft-404	A page that returns HTTP 200 for URLs that do not exist.

20 Annex — Standards & References

- OWASP Top 10:2021 · OWASP API Security Top 10:2023
- OWASP Application Security Verification Standard (ASVS) v4.0, Levels 1–2
- PTES — Penetration Testing Execution Standard
- NIST SP 800-115 — Technical Guide to Information Security Testing
- CVSS v3.1 — Common Vulnerability Scoring System
- CERT-In — reporting format and methodology alignment
- ISO/IEC 27001:2022 Annex A · SOC 2 (AICPA TSC) · GDPR Article 32 · DPDP Act 2023

21 Revision History

VERSION	DATE	NOTE
1.0	15 August 2026	Final production assessment report issued.

22 Disclaimer & Confidentiality

This assessment reflects the state of the in-scope systems during the test window (15 August 2026). Security is time-variant: changes to the environment after the test window may introduce new risks. A penetration test demonstrates the presence of vulnerabilities, not their absence; a clean result reduces but does not eliminate risk.

Bachao.AI (Dhisattva AI Pvt Ltd) is a technology provider. The compliance mappings are technical observations to support At*****'s own compliance work and are not a legal opinion. This document is confidential to At***** and Bachao.AI.

Classification — TLP:AMBER. This report is marked under the Traffic Light Protocol (TLP) and contains security-sensitive information, including exploitable vulnerability detail. It may be shared only within At***** on a need-to-know basis and must not be disclosed to third parties without Bachao.AI's written consent. Store and transmit it accordingly.

Shouvik Mukherjee — Lead Security Assessor
Bachao.AI · Dhisattva AI Pvt Ltd · 15 August 2026
Certificate No. BVPT-SAMPLE-2026-0005 · Sample — reference not live