CYBRA SECURITY

PUBLIC SAMPLE REPORT • 100% SYNTHETIC LAB DATA

External & Web Application Penetration Test Report

Prepared for: Southern Cross FinTech Pty Ltd (Fictional Sample)

This is a shortened sample report built entirely with fictional lab data—no real client details are ever shared. It gives you a quick look at how Cybra Security presents risk clearly for both leadership and technical teams.

A full Cybra Security penetration test report goes significantly further, including detailed scope coverage, attack narratives, complete technical findings, retesting results, and full appendices. Want to see a full-length sample report or talk through a test for your own environment? Get in touch with our Australian team anytime.



METHODOLOGY
OWASP & PTES
ISO 31000 5-tier risk ratings

DELIVERED BY
CREST & OSCP
Senior Australian testers

CLASSIFICATION
PUBLIC SAMPLE
Zero real client data

Cybra Security Pty Ltd — Offensive Security Practice
Melbourne • Sydney • Brisbane • Perth • Adelaide • Darwin • Tasmania

cybra.com.au
1300 788 781

1. Executive Summary (Board-Ready Overview)

In November 2026, **Cybra Security** conducted a manual External Network and Web Application Penetration Test for **Southern Cross FinTech Pty Ltd** (fictional demonstration), covering its public customer portal (`portal.southerncross-demo.example`) and external cloud perimeter. The engagement assessed whether an unauthenticated internet attacker—or a standard logged-in customer—could compromise customer personal information or disrupt operations.

1	1	1	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

Overall Security Posture: High Risk (Immediate Action Required on Two Exposures).

While the public marketing site sat securely behind a Web Application Firewall (WAF), manual testing uncovered an **unauthenticated MongoDB database port** reachable via a direct cloud IP (Critical) and an **API authorisation defect (IDOR)** returning unmasked customer names despite frontend UI masking (High). Both flaws were missed by monthly automated vulnerability scans and could trigger an **OAIC Notifiable Data Breaches (NDB)** event under Privacy Act APP 11 if exploited.

Key Findings Summary

Ref	Risk	Finding Title	Primary Business Impact
2.3.1	CRITICAL	**Unauthenticated Exposed MongoDB Database**	Full unauthenticated extraction of customer PII & records from internet.
2.3.2	HIGH	**Broken Object Level Authorisation (IDOR) & Unmasked API**	Sequential harvesting of customer names & account status; targeted phishing.
2.3.3	MEDIUM	**Failure to Invalidate Session Tokens on Logout**	Persistent account takeover via stolen cookies or shared workstations.
2.3.4	INFO	**Missing Defence-in-Depth HTTP Security Headers**	Reduced browser-side protection against clickjacking & MIME sniffing.

Strategic Remediation Roadmap (30-Day Executive Plan)

Immediate (Within 48 Hours)

Restrict MongoDB TCP/27017 strictly to private VPC subnets, enable SCRAM-SHA-256 authentication, and review database access logs for historical unauthorised connections.

Short-Term (Within 14–30 Days)

Enforce server-side object ownership checks & DTO field filtering on customer APIs, revoke sessions server-side on logout, and schedule a focused Cybra verification retest.

Unauthenticated Exposed MongoDB Database Service

Reference: 2.3.1 **Risk:** Critical **Consequence:** Severe **Likelihood:** Almost Certain

Affected: 198.51.100.42:27017

Technical Details

External perimeter enumeration identified an internet-reachable MongoDB database listener on TCP port `27017` bypassing the organisation's Cloudflare WAF via a direct cloud origin IP address. The instance accepted connections without authentication (`security.authorization` disabled), exposing three databases including a `customers_prod` collection containing synthetic customer names, email addresses, residential addresses, and account balances.

Cybra verified read access safely without extracting bulk datasets or modifying records, confirming immediate remote exploitability using standard MongoDB client tooling:

```
$ mongosh "mongodb://198.51.100.42:27017" --quiet --eval "db.adminCommand('listDatabases')"
{ databases: [ { name: 'customers_prod', sizeOnDisk: 184320000 }, { name: 'admin', sizeOnDisk: 40960 } ],
ok: 1 }

$ mongosh "mongodb://198.51.100.42:27017/customers_prod" --quiet --eval "db.accounts.findOne({}, {email:1,
tier:1})"
{ _id: ObjectId('67401a...'), email: 'demo.customer@southerncross-demo.example', tier: 'Platinum' }
```

Business & Regulatory Impact

Automated internet-wide scanners continuously discover and ransom unauthenticated MongoDB instances within minutes of cloud security-group drift. Exploitation would allow full customer data exfiltration or destructive data wiping, triggering mandatory assessment under the **OAIC Notifiable Data Breaches (NDB) scheme**, severe reputational damage, and material financial recovery costs (ASD reports mid-market cybercrime costs averaging $141,300 per incident).

Actionable Remediation

- **Remove Public Exposure Immediately:** Remove all `0.0.0.0/0` ingress rules on TCP/27017 in cloud security groups and bind `mongod.conf` strictly to private internal interfaces (`bindIp: 10.x.x.x`).
- **Enforce Authentication & TLS:** Enable `security.authorization: enabled` using SCRAM-SHA-256 with least-privilege application roles and mandatory TLS encryption in transit.
- **Audit Historical Access:** Inspect MongoDB audit logs and VPC Flow Logs for external connections prior to remediation, and rotate any credentials or API secrets stored in exposed collections.

Remediation Effort

Low. Approximately 1–2 hours to restrict cloud security-group ingress rules and enable SCRAM-SHA-256 authentication.

References

- MongoDB Security Checklist https://www.mongodb.com/docs/manual/administration/security-checklist/
- OWASP Top 10 A05: Security Misconfiguration https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Broken Object Level Authorisation (IDOR) & Unmasked API Response

Reference: 2.3.2 **Risk:** High **Consequence:** Major **Likelihood:** Likely

Affected: https://portal.southerncross-demo.example/api/v2/members/{id}

Technical Details

The customer portal renders a masked email address (`a***@example.org.au`) in the browser UI to protect user privacy. However, inspecting the raw HTTP response revealed that the API enforces **no server-side object ownership validation** on the sequential numeric `{id}` parameter and returns unmasked PII fields directly in the JSON payload. Automated vulnerability scanners reported zero issues because every enumerated request returned a valid `HTTP 200 OK`.

VULNERABLE RAW API RESPONSE (BEFORE)

```
GET /api/v2/members/104830 HTTP/2
Cookie: session=USER_A_TOKEN

HTTP/2 200 OK
{
  "memberId": 104830,
  "maskedEmail": "a***@example.org.au",
  "fullName": "Alex Taylor (User B)",
  "mobile": "+61 400 000 123",
  "tier": "Active"
}
```

HARDENED API RESPONSE (AFTER FIX)

```
GET /api/v2/members/104830 HTTP/2
Cookie: session=USER_A_TOKEN

HTTP/2 403 Forbidden
{
  "error": "access_denied",
  "message": "Resource not authorised"
}

// Own profile returns strict DTO only
// Non-sequential UUIDv4 identifiers
```

Business Impact

Any authenticated customer (or attacker holding a single compromised account) can script a trivial loop across sequential IDs to harvest the entire customer directory—enabling convincing Australian spear-phishing, account takeover, and potential APP 11 privacy compliance exposure.

Actionable Remediation

- **Enforce Server-Side Ownership Checks:** Validate on every request that the authenticated session's `user_id` matches the requested resource owner (or holds an explicit admin role), returning `HTTP 403` otherwise.
- **Implement Strict Output DTOs:** Never rely on frontend JavaScript masking—strip sensitive fields at the backend serialiser before transmitting JSON.
- **Replace Sequential IDs & Rate-Limit:** Migrate public object identifiers to random UUIDv4 values and enforce per-session API rate limiting.

Remediation Effort

Moderate. Approximately 1–2 sprint days to implement server-side ownership checks, DTO filtering, and UUIDv4 identifiers.

References

- OWASP API1:2023 Broken Object Level Authorization https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- OWASP API3:2023 Broken Object Property Level Authorization https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/

3. Cybra Risk Rating Methodology (ISO 31000 Aligned)

Every confirmed finding in a Cybra Security report is scored objectively across **Likelihood** and **Consequence** using our 5-tier scale so engineering, risk, and board stakeholders share one consistent prioritisation language:

Risk Rating	Recommended SLA	Definition & Executive Meaning
CRITICAL	**Immediate (24–48 hrs)**	Direct, unauthenticated or trivial compromise of sensitive customer data, Domain Admin, or critical infrastructure. Escalated verbally during testing.
HIGH	**Urgent (7–14 days)**	Substantial exposure enabling unauthorised data access, privilege escalation, or business-logic bypass requiring immediate sprint prioritisation.
MEDIUM	**Planned (30–60 days)**	Exploitable weakness requiring specific conditions or chained controls; degrades resilience and audit readiness.
LOW	**Next Release Cycle**	Minor security weakness with limited direct impact; address as part of routine system hardening.
INFO	**Best Practice**	Defence-in-depth observations, hygiene enhancements, and hardening recommendations with no direct exploit path confirmed.

What Every Cybra Security Penetration Test Includes

100% Manual Senior-Led Execution

Delivered by CREST, OSCP, CISSP, and GWAPT specialists in Australia—testing business logic, chained exploits, and real adversary paths.

Live Technical Debrief & Retesting

Every engagement includes a live walkthrough directly with your lead tester plus optional formal retesting and auditor attestation letters.

READY FOR THIS LEVEL OF CLARITY ON YOUR OWN ENVIRONMENT?

Estimate Your Penetration Test Scope in 60 Seconds

Get an instant Australian consulting effort range, tailored methodology, and pre-test readiness checklist —or book a 15-minute scoping call directly with a senior Cybra tester.

cybra.com.au/pentest-estimator | 1300 788 781 | enquiries@cybra.com.au