PENETRATION TEST REPORT

Document Reference:	PEN-001	**Test Period:**	5-9 August 2025
Testing Firm:	CyberShield Consulting Pty Ltd	**Test Date:**	August 2025
Report Date:	18 August 2025	**Classification:**	Confidential

EXECUTIVE SUMMARY

A comprehensive external penetration test was conducted on HorseInsure Pty Ltd's IT infrastructure from 5-9 August 2025. The scope included external network perimeter and web application testing. A total of 8 vulnerabilities were identified: 1 Critical, 2 High, 3 Medium, and 2 Low severity findings. Critical findings require immediate remediation.

TESTING SCOPE & METHODOLOGY

In-Scope Systems:
- EquiClaim web portal (external access)
- EquiQuote web portal (external access)
- External network perimeter
- Public-facing web servers

Testing Methodology:
Black-box testing approach was used. Reconnaissance, scanning, enumeration, exploitation, and post-exploitation techniques were applied. No credentials were provided to testers.

FINDINGS SUMMARY

Severity	Count	Status
Critical	1	Remediation In Progress
High	2	Open
Medium	3	Open
Low	2	Open

DETAILED FINDINGS

ID	Title	Severity	Status	Remediation
PEN-001-001	SQL Injection in EquiQuote Legacy Module	Critical	Remediation In Progress	Code review and input validation fix scheduled
PEN-001-002	Weak TLS Configuration on EquiClaim Portal	High	Open	Update web server TLS settings
PEN-001-003	Missing HTTP Security Headers	High	Open	Implement CSP, X-Frame-Options headers
PEN-001-004	Unvalidated Redirects in Portal Login	Medium	Open	Implement redirect whitelist
PEN-001-005	Weak Password Policy	Medium	Open	Enforce minimum 12-char passwords
PEN-001-006	Outdated SSL Certificate on Dev Server	Medium	Open	Renew SSL certificate
PEN-001-007	Information Disclosure in Error Messages	Low	Open	Sanitize error messages

PEN-001-008	Missing HSTS Header	Low	Open	Enable Strict-Transport-Security header

MANAGEMENT RESPONSE

David Chen, CISO, provided the following response:

Critical Finding (PEN-001-001): Acknowledged. Development team is actively working on remediation. Code review scheduled for completion by end of September 2025. Testing will occur in UAT before production deployment.

High Findings (PEN-001-002, 003): Web server configuration update is planned. Timeline depends on change management approval. Currently in change request pipeline.

Medium & Low Findings: Will be addressed in regular maintenance windows. Prioritized in backlog. No immediate risk to operations expected.

NEXT STEPS & RECOMMENDATIONS

1. **Immediate:** Critical SQL injection vulnerability (PEN-001-001) must be patched immediately. Target: 30 days
2. **High Priority:** Address TLS and HTTP header findings within 60 days
3. **Follow-up Assessment:** Recommend re-test of critical/high findings post-remediation
4. **Preventive:** Implement secure SDLC practices and code scanning in CI/CD pipeline
5. **Training:** Conduct security awareness training for development teams

REPORT SIGN-OFF

Testing Firm:	CyberShield Consulting Pty Ltd	**Report Date:**	18 August 2025
Authorized By:	James Morrison (Lead Pentester)	**HorseInsure Recipient:**	David Chen (CISO)