Unicorn IT Group

Web Application Penetration Test Report

Security assessment of a customer-facing web application and API

Prepared for: Sample Retail Group

Date: 28 August 2026

Classification: CONFIDENTIAL

1300 904 635 | hello@uitg.com.au | www.uitg.com.au

Document Information

Document title	Sample Penetration Test Report
Version	1.0
Author	Unicorn IT Group Security Team
Classification	Confidential
Contact	hello@uitg.com.au | 1300 904 635

This is a sample report for demonstration purposes. Names, IP addresses and findings have been fictionalised.

Executive Summary

This sample report covers a web application and API penetration test. The assessment identified a critical SQL injection vulnerability that permits authentication bypass, plus a high-risk broken access-control issue exposing customer invoices. These issues should be remediated before the next release. Medium and low findings relate to missing security headers and verbose error messages.

Metric	Value
Test type	Web application and API penetration test
Targets	Customer portal, API endpoints and public website
Duration	5 business days
Critical findings	1
High findings	1
Medium findings	1
Low findings	1

Findings Overview

ID	Finding	Risk	Status
WEB-001	SQL injection in customer portal login	Critical	Open
WEB-002	Broken access control on invoice download	High	Open
WEB-003	Missing Content Security Policy	Medium	Open
WEB-004	Verbose error messages leak stack traces	Low	Open

Detailed Findings

WEB-001 — SQL injection in customer portal login

Risk rating: Critical

Description

The login form on /portal/login is vulnerable to boolean-based SQL injection, allowing authentication bypass and potential extraction of the user database.

Evidence

Payload ' OR '1'='1' -- returned a valid session cookie. sqlmap confirmed time-based injection.

Recommendation

Use parameterised queries, implement input validation and conduct a full code review of authentication flows.

WEB-002 — Broken access control on invoice download

Risk rating: High

Description

Invoice documents can be accessed by incrementing an integer ID in the URL without verifying ownership, exposing customer invoices to other customers.

Evidence

GET /invoices/10234 returned an invoice belonging to a different test account.

Recommendation

Enforce server-side authorisation checks on every document request and use opaque identifiers.

WEB-003 — Missing Content Security Policy

Risk rating: Medium

Description

No Content-Security-Policy header is returned, increasing the impact of any cross-site scripting vulnerability.

Evidence

Response headers inspected; CSP and X-Frame-Options were absent.

Recommendation

Deploy a strict CSP, X-Frame-Options and other security headers.

WEB-004 — Verbose error messages leak stack traces

Risk rating: Low

Description

Application errors return full stack traces and framework version information to end users.

Evidence

Triggering an invalid route produced a detailed ASP.NET exception page.

Recommendation

Configure custom error pages and disable debug output in production.

Scope & Methodology

Scope

- Public-facing customer portal
- REST API endpoints used by mobile and web clients
- Authentication and session management flows
- File upload and document download functionality

Methodology

Testing followed the OWASP Testing Guide and PTES. We used a combination of manual testing, automated scanning and source-assisted review where code was available. No denial-of-service testing was performed.

Standards & Frameworks

- OWASP Testing Guide v4.2
- OWASP Top 10 2021
- PTES
- NIST SP 800-115

Remediation Tracker

ID	Action	Owner	Target
WEB-001	Use parameterised queries, implement input validation and conduct a full code review of authentication flows.	IT Team	30 days
WEB-002	Enforce server-side authorisation checks on every document request and use opaque identifiers.	IT Team	30 days
WEB-003	Deploy a strict CSP, X-Frame-Options and other security headers.	IT Team	30 days
WEB-004	Configure custom error pages and disable debug output in production.	IT Team	30 days

Unicorn IT Group can assist with remediation, re-testing and ongoing security management. Contact us at hello@uitg.com.au or 1300 904 635.