

SAMPLE

Web Application Penetration Test

Sample Report — illustrative structure and content only

Client	Meridian Retail Pvt Ltd (fictional)	Engagement	Grey-box web app VAPT
Scope	Customer portal, checkout, admin, public API	Standard	OWASP Testing Guide
Test window	5 business days	Report status	SAMPLE — not a real assessment

Executive summary

This engagement assessed the client's customer-facing web application and supporting API using a grey-box methodology aligned to the OWASP Testing Guide, combining AI-accelerated coverage with manual, expert-led exploitation. Several issues — most notably an injection flaw and a broken access-control condition — require prompt remediation. All findings below are illustrative and use fictional data.

Findings by severity

Critical	High	Medium	Low	Info
1	2	3	4	2

Selected findings (illustrative)

ID	Finding	Severity	CVSS
F-01	SQL injection in product search parameter	Critical	9.1
F-02	Broken access control on admin order-export endpoint	High	8.2
F-03	Session token does not rotate after privilege change	High	7.4
F-04	Verbose error messages disclose stack traces	Medium	5.3
F-05	Missing security headers (CSP, HSTS)	Medium	5.1
F-06	Rate limiting absent on authentication endpoint	Medium	5.8
F-07	Cookie missing Secure/HttpOnly attributes	Low	3.7

In the full report, each finding includes affected component, redacted evidence, business impact, a reproducible test case, and prioritised remediation mapped to your framework (OWASP, PCI DSS, ISO 27001).