SIMULATED WEB APPLICATION SECURITY REPORT

FOR TRAINING / DEMO PURPOSES ONLY
NOT A REAL ASSESSMENT

Report ID: SIM-2025-1769
Generated: 2025-10-02
Environment: Staging (simulated)

Prepared by: Security Testing Simulation Engine

Executive Summary

Scope: Simulated sample web application (login, profiles, comments, API).
Objective: Identify common web vulnerabilities (SQLi, XSS, Auth, IDOR, CSRF).

Key Metrics:

Total Endpoints Tested:	96
Automated Alerts (ZAP/Burp):	33
Confirmed Vulnerabilities:	10
High Severity:	1
Medium Severity:	5
Low Severity:	1
Average Time to Remediate (days):	25
Tests Run (manual):	116
Tests Run (automated):	430

Top Prioritized Issues:

- SQL Injection (Parameterized missing) (Severity: High, CVSS-like: 9.0)

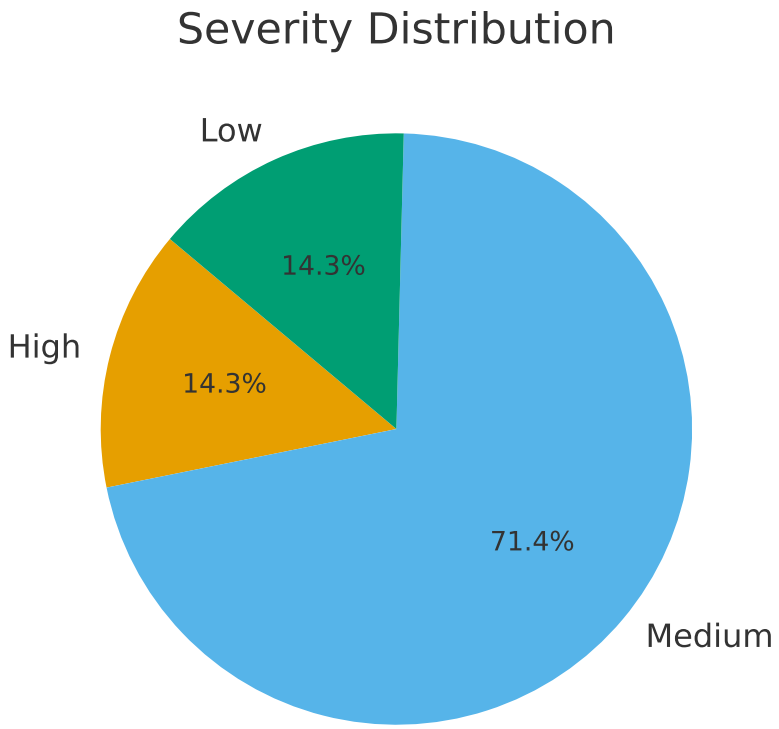
- Stored Cross-Site Scripting (XSS) (Severity: High, CVSS-like: 8.8)

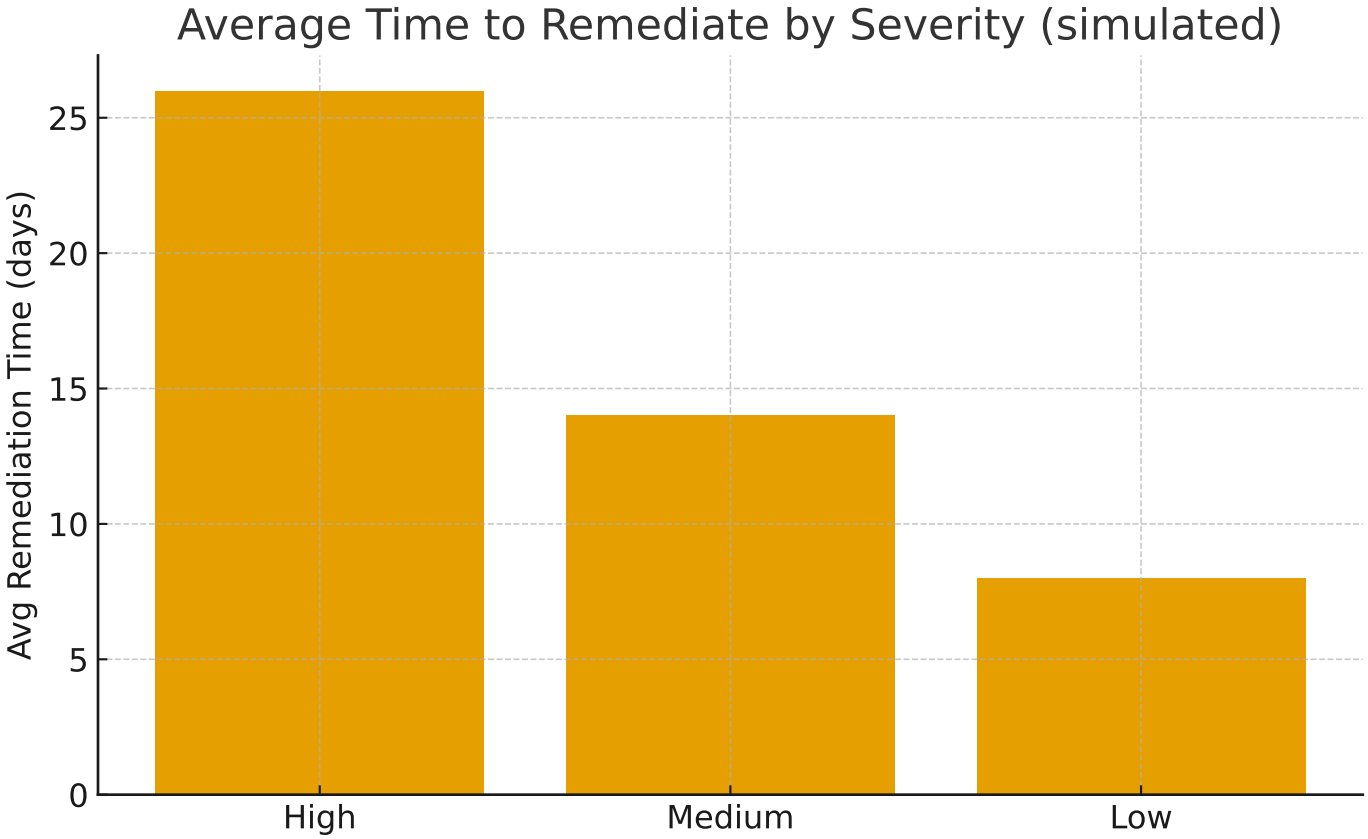
- Broken Password Reset Tokens (Severity: High, CVSS-like: 9.0)

Detailed Findings (Simulated)

ID	Title	Severity	CVSS-like	Instances	Recommended Fix
F-2025-001	SQL Injection (Par	High	9.0	3	Use parameterized queries; least
F-2025-002	Stored Cross-Site	High	8.8	4	Context-aware encoding; sanitize
F-2025-003	Broken Password	High	9.0	1	Cryptographically-random, single
F-2025-004	Insecure Direct Ol	Medium	7.4	5	Server-side authorization checks;
F-2025-005	CSRF on state-cha	Medium	6.4	3	Implement CSRF tokens; SameSit
F-2025-006	Missing Security H	Low	4.0	8	Add CSP, X-Frame-Options, HttpC

Findings Breakdown and Time-to-Remediate (Simulated)





Recommendations & Next Steps (Simulated)

1. Fix critical input validation issues immediately (SQLi, broken auth flows).

2. Deploy output-encoding and input sanitization libraries to prevent XSS.

3. Enforce server-side access control to mitigate IDOR exposures.

4. Implement CSRF protections and secure cookie attributes (HttpOnly, Secure, SameSite).

5. Add security headers (CSP, X-Frame-Options, X-Content-Type-Options).

6. Integrate SAST/DAST in CI pipelines and schedule periodic pentests.

7. Maintain an incident response and patch management process.