



Web Application Penetration Testing

Uncover deep logic flaws and authentication weaknesses in the applications your business runs on.

43%

of breaches involve web applications.

Verizon Data Breach Investigations Report, 2023

Automated scanners find the easy issues. The vulnerabilities that actually get exploited - broken access controls, JWT manipulation, SSRF, business logic abuse - require a human tester who thinks like an attacker. Sprocket's Web Application Penetration Testing delivers exactly that, continuously and across every application that matters to your business.

🔧 > SCOPE COVERED

Authentication & Session Management

JWT / Token Security

REST & GraphQL APIs

Input Validation

Access Controls (IDOR / BOLA)

SSRF & Injection

Business Logic Flaws

TLS / HTTP Security Headers

Key Capabilities

Authenticated & Unauthenticated Testing

Sprocket tests both the unauthenticated attack surface exposed endpoints, login bypass, TLS weaknesses, and information disclosure as well as all authenticated application functionality across multiple user roles to uncover authorization flaws and privilege escalation paths.

API & Business Logic Testing

Testers analyze REST and GraphQL APIs for injection flaws, insecure direct object references, improper authorization, JWT signature bypass, and logic abuse that automated tools cannot detect. If your application has a workflow, Sprocket will try to break it.

OWASP Top 10 & Beyond

Every engagement maps findings to the OWASP Top 10 (A01–A10) and relevant compliance frameworks. Testing goes beyond the checklist to reflect real attacker TTPs used against modern web applications today, not a generic vulnerability scan rebranded as a pentest.

Why It Matters



Business Risk

Web applications are the front door to your sensitive data. Broken access controls, unvalidated JWTs, exposed API secrets, and SSRF vulnerabilities give attackers direct paths to customer records, internal systems, and critical infrastructure.



Compliance Driver

PCI DSS v4, SOC 2 Type II, HIPAA, and ISO 27001 all require application-layer security testing. Sprocket's findings map directly to these frameworks and include the evidence auditors need.



Operational Value

Every finding is delivered in the Sprocket Portal with a full proof-of-concept exploit, CVSS score, remediation guidance, and unlimited retesting, so you can verify your fixes work before your next audit, not after.

ROI & Outcomes



Framework Coverage

OWASP Top 10

In every engagement



Retesting Post-Remediation

Unlimited

Verify fixes before your audit



Findings Manually Validated

100%

No false positives from scanners



Compliance-Ready Evidence

Included

With every finding

Why Sprocket Security

- Deep manual testing across all user roles, application states, and API endpoints
- API-first approach: REST, GraphQL, and custom authentication schemes fully assessed
- Business logic flaw identification: the class of vulnerability scanners are blind to
- Portal-based findings with proof-of-concept exploits, CVSS scoring, and clear remediation
- Continuous testing means new features and API changes are assessed as they ship

 Sprocket Security	Legacy / Point-in-Time
Continuous testing as your app evolves	Annual or quarterly testing
Every finding manually validated by a human tester	Scanner output rebranded as a report
Live portal with real-time findings	Static PDF delivered weeks later
New features and changes trigger re-testing	Testing stops at engagement end
Proactive & security-driven	Reactive & compliance-driven

The details for each finding are complete with proof and an easy-to-understand explanation. Steps for remediation are given, and Sprocket team is willing to assist if a particular finding is difficult to fix.

— User in Manufacturing, Mid-Market (G2 Verified Review)

