## Service Overview

SynAck Solutions delivers comprehensive Web Application Penetration Testing that goes beyond automated scanning to identify complex, logic-driven vulnerabilities in your web applications and APIs. Our certified operators combine automated tooling with deep manual testing to uncover injection flaws, authentication bypasses, access control failures, and business logic vulnerabilities that scanners consistently miss.

Every engagement follows the OWASP Testing Guide v4.2 methodology, mapped to the OWASP Top 10 and MITRE ATT&CK framework, and is conducted by professionals with extensive experience across modern application architectures including SPAs, microservices, serverless, and API-first platforms.

## Business Value

- Identify exploitable vulnerabilities in web applications before attackers find them
- Uncover business logic flaws, IDOR, and access control bypasses that automated scanners miss
- Validate the effectiveness of WAF rules, input validation, and session management
- Meet compliance obligations: ISO 27001, PCI DSS, Essential Eight, APRA CPS 234, SOC 2
- Receive developer-friendly remediation guidance with code-level fix recommendations
- Protect customer data and maintain trust through proactive security assessment
- Support secure SDLC practices with pre-release and post-deployment testing options

## What's Included

- Authentication and session management testing: brute force, credential stuffing, session fixation
- Authorisation testing: horizontal and vertical privilege escalation, IDOR, role-based access
- Injection testing: SQL, NoSQL, LDAP, OS command, SSTI, and expression language injection
- Cross-site scripting (XSS): reflected, stored, and DOM-based variants
- Cross-site request forgery (CSRF) and server-side request forgery (SSRF)
- Business logic testing: workflow bypass, race conditions, price manipulation
- API security assessment: REST, GraphQL, and SOAP endpoint testing
- File upload and download vulnerability testing
- Security header and TLS configuration analysis
- Branded report: executive summary, findings, OWASP mapping, remediation guidance
- Delivery in four formats: Word, PDF, interactive HTML, and Google Doc
- Post-engagement debrief and remediation guidance with your development team

## Scope

The engagement covers web applications and APIs as defined in the Rules of Engagement, including:

- Web application front-end: all user-accessible pages, forms, and workflows
- API endpoints: REST, GraphQL, SOAP, and WebSocket interfaces
- Authentication mechanisms: login, registration, password reset, MFA, SSO/OAuth
- Role-based functionality across all defined user privilege levels
- Third-party integrations and payment processing workflows where authorised
- Administrative panels and content management interfaces

Testing is performed from both unauthenticated and authenticated perspectives. Test accounts for each application role are provided by the client prior to engagement start.

## What's Excluded

- Infrastructure-level penetration testing beyond the application host (available separately)
- Source code review or static analysis (available as a separate engagement)
- Denial-of-service or load/stress testing
- Social engineering or phishing campaigns
- Mobile application testing (available separately)
- Testing of third-party hosted components without explicit written authorisation

## Methodology

Our methodology aligns with the OWASP Testing Guide v4.2 and OWASP Application Security Verification Standard (ASVS). Each finding is scored using CVSS v3.1 with full vector strings, mapped to OWASP Top 10 categories and CWE identifiers. Remediation includes code-level tactical fixes and strategic architectural recommendations.

## Engagement Timeline

A typical web application assessment runs 5-15 business days depending on application complexity, number of roles, and API surface area. Final report delivery within 5 business days of testing completion. Re-test of remediated findings available within 30 days at 30% of initial engagement cost. Expedited timelines available on request.

## Get Started

Contact us to discuss your requirements and receive a tailored proposal. We will work with you to define application scope, user roles, test environments, and schedule testing aligned to your release cycle.

**info@synack.au | https://www.synack.au**

ABN 88 667 784 956