Web Application Security Assessment

Penetration Testing Scope & Methodology

Black-Box · Privilege Escalation Focus · OWASP-Mapped · Manual + Automated

Client Engagement Document · April 2026 · CONFIDENTIAL — RESTRICTED

7	OWASP Top 10	Manual +Auto	PoC
Test Domains	Mapping Framework	Testing Approach	Per Finding

RESTRICTED DOCUMENT — This document is intended solely for authorised personnel. It contains sensitive security findings, attack vectors, and proof-of-concept details. Distribution outside the named engagement team is strictly prohibited.

The assessment assumes privileged/admin functionality exists behind the same authentication surface. Testing specifically targets horizontal and vertical privilege escalation paths without requiring source code, internal architecture details, or pre-issued privileged credentials. All testing combines manual verification with targeted automated tooling.

1 ENGAGEMENT SCOPE & OBJECTIVES

SATYA TECHNOLOGIES
We Believe in Solutions

■Target: Web application and associated API surface (authenticated and unauthenticated endpoints)

■Methodology: Black-box testing — no source code, no architecture diagrams, no privileged credentials provided

■Assumption: Admin/privileged functionality is accessible via the same authentication surface as standard users

■Primary objective: Identify horizontal privilege escalation (peer-account access) and vertical escalation (privilege elevation)

■Secondary objectives: Identify all OWASP Top 10 categories, business-logic abuse, and session management weaknesses

■Deliverable per finding: OWASP mapping, proof of concept, impact rating, affected endpoints, reproduction steps, remediation

OWASP: [OWASP Top 10] [OWASP WSTG] [OWASP ASVS]

Burp Suite Pro	OWASP ZAP	Manual Testing	Postman / curl

2 AUTHENTICATION TESTING

■Test for username enumeration via differential responses, timing attacks, and error message leakage

■Assess password policy enforcement: complexity, length, breach-list checking (HaveIBeenPwned integration)

■Evaluate brute-force and credential-stuffing resilience: rate limiting, account lockout, and CAPTCHA bypass

■Test multi-factor authentication implementation: bypass techniques, fallback flows, and OTP reuse windows

■Examine token-based authentication (JWT): algorithm confusion (RS256/HS256), none-algorithm, key exposure, and claim tampering

■Test OAuth 2.0 / OIDC flows: redirect_uri manipulation, state parameter fixation, and implicit grant abuse

OWASP: [A07:2021 Auth Failures] [WSTG-ATHN]

Burp Suite	jwt_tool	hydra	ffuf

3 AUTHORISATION & PRIVILEGE ESCALATION

■Test for Insecure Direct Object References (IDOR): enumerate and substitute user/resource IDs across all endpoints

■Attempt horizontal privilege escalation: access another user's data/actions using own valid session token

■Attempt vertical privilege escalation: access admin/privileged endpoints using low-privilege account credentials

■Test forced browsing to admin panels, management APIs, and internal endpoints without elevated authentication

■Evaluate server-side authorisation enforcement: verify controls are not solely client-side (hidden fields, UI flags)

■Test parameter pollution and mass assignment: inject unexpected fields (role, isAdmin, accountLevel) in requests

■Assess path traversal and function-level access control on all API versioned endpoints (/v1/, /v2/, /admin/)

OWASP: [A01:2021 Broken Access Control] [WSTG-AUTHZ]

Burp Suite Autorize	FFUF	Manual IDOR	Postman

4 SESSION MANAGEMENT TESTING

- Analyse session token entropy, predictability, and length using statistical analysis of token samples
- Test session fixation: ability to force a known session ID pre-authentication and retain it post-login
- Verify session invalidation: logout terminates server-side session; tokens cannot be replayed post-logout
- Test concurrent session controls: multiple simultaneous logins, session displacement, and notification
- Assess cookie security attributes: Secure, HttpOnly, SameSite flags, and domain/path scoping
- Test CSRF protection across all state-changing operations: token validation, origin/referrer header checks
- Evaluate session timeout enforcement: idle timeout, absolute timeout, and re-authentication requirements

OWASP: [A07:2021 Auth Failures] [WSTG-SESS]

Burp Suite	CSRF PoC Generator	Cookie Editor	Manual Analysis

5 ACCOUNT LIFECYCLE & IDENTITY MANAGEMENT

- Test account registration: duplicate accounts, email verification bypass, and disposable domain acceptance
- Assess password reset flows: token entropy, expiry enforcement, host-header injection for link hijacking
- Test account enumeration via reset/registration flows: differential responses exposing registered emails
- Evaluate account takeover via response manipulation: skip email verification, alter role in registration payload
- Assess account deletion and deactivation: data persistence, session validity post-deletion, GDPR compliance
- Test for account linking/OAuth merge vulnerabilities: pre-account takeover via social login binding

OWASP: [A07:2021 Auth Failures] [WSTG-IDNT]

Burp Suite	Manual Testing	MailHog	ffuf

6 COMMON WEB & API VULNERABILITY TESTING

- SQL Injection: error-based, blind boolean, time-based, and ORM-layer injection across all input vectors
- Cross-Site Scripting (XSS): reflected, stored, and DOM-based XSS in parameters, headers, and JSON fields
- Server-Side Request Forgery (SSRF): internal network probing via URL parameters, webhooks, and file imports
- XML/JSON injection: XXE, SSTI (Jinja2, Twig, Freemarker), and deserialization vulnerabilities
- Broken Object-Level Authorization (BOLA/IDOR) across REST and GraphQL API endpoints
- API-specific: mass assignment, excessive data exposure, lack of resource/rate limiting, and versioning abuse
- File upload: MIME type bypass, polyglot files, path traversal in filename, and web shell upload attempts
- HTTP security header assessment: CSP, HSTS, X-Frame-Options, and Referrer-Policy configuration review

OWASP: [A03:2021 Injection] [A05:2021 Misconfig] [WSTG-INPV] [WSTG-APIT]

sqlmap	Burp Suite	nuclei	ghauri	ffuf

7 BUSINESS LOGIC ABUSE TESTING

- Identify and abuse application workflow assumptions: skip steps, replay completed actions, reverse flows
- Test numeric/price manipulation: negative values, zero-cost transactions, integer overflow in quantity fields
- Assess feature flag and entitlement abuse: access premium/restricted features via parameter manipulation
- Test for race conditions: concurrent requests to exploit TOCTOU (time-of-check/time-of-use) windows
- Evaluate multi-tenancy isolation: cross-tenant data access, shared resource bleed, and tenant ID substitution
- Test export and bulk-action endpoints for data aggregation risks and authorisation bypass at scale

OWASP: [A04:2021 Insecure Design] [WSTG-BUSL]

Burp Turbo Intruder	Race Condition Tools	Manual Testing

Sample Finding Classification Structure

Finding	Severity	OWASP Ref	Affected Area
Vertical Privilege Escalation via IDOR	Critical	A01:2021	Admin API /api/v1/admin/*
JWT Algorithm Confusion (RS256 → HS256)	Critical	A07:2021	Authentication Surface
Horizontal Escalation — User Data IDOR	High	A01:2021	/api/users/{id}/profile
CSRF on Account Email Change	High	A07:2021	/account/settings
Stored XSS in User Profile Bio Field	High	A03:2021	/profile/edit
Password Reset Token — No Expiry Enforced	Medium	A07:2021	/auth/reset-password
Verbose Error Messages — Stack Trace Exposure	Medium	A05:2021	All API Endpoints
Missing SameSite Cookie Attribute	Low	A07:2021	Session Cookie

Per-Finding Report Structure

Field	Content
Finding Title	Descriptive name identifying the vulnerability class and location
Severity	Critical / High / Medium / Low / Informational (CVSS v3.1 scored)
OWASP Mapping	OWASP Top 10 2021 category + WSTG test case reference
Affected Endpoint(s)	Full URL path(s) including method (GET/POST/PUT), parameters, headers
Description	Technical explanation of the vulnerability and root cause
Proof of Concept	Step-by-step reproduction, HTTP request/response, screenshots or video
Reproduction Steps	Numbered steps for the client team to independently verify the finding
Impact	Business and technical impact — data exposure, account takeover, etc.
Remediation	Specific, actionable fix guidance with code examples where applicable
References	OWASP, CVE, CWE, vendor advisory, or framework-specific guidance links

Testing Toolset

Category	Tools Used	Purpose
Proxy / Interception	`Burp Suite Professional`	Request interception, modification, active scanning
API Testing	`Postman, curl, httpie`	Manual API exploration and authorisation testing
Fuzzing	`ffuf, feroxbuster`	Directory/endpoint discovery, parameter fuzzing
Vulnerability Scan	`nuclei, OWASP ZAP`	Automated vulnerability signature matching
Injection	`sqlmap, ghauri`	SQL injection detection and exploitation

JWT Analysis	`jwt_tool, jwt.io`	Token structure, algorithm confusion, claim testing
Recon	`Subfinder, httpx`	Asset discovery, endpoint enumeration, URL mining

> All findings are manually verified before inclusion in the final report. Automated scan output is used only as a triage aid and is never included without independent confirmation. The final deliverable maps every finding to the OWASP Top 10 2021 and OWASP WSTG, and includes executive summary, technical detail, and remediation roadmap sections.