

TECHNICAL PRODUCT BRIEF

Web application penetration testing

Test the controls that protect application users, data and workflows.

Why customers use this service

Test the application from public, authenticated, cross-role and integration perspectives to identify weaknesses that could expose accounts, data, privileged functions or business workflows.

What we assess

Authentication and recovery	Login, MFA, reset and recovery weaknesses.
Authorisation and tenant isolation	Role, object, function and cross-tenant access controls.
Sessions and tokens	Cookie, session and token lifecycle, replay and revocation.
Input and output handling	Injection, unsafe parsing and browser output risks.
Business logic	Workflow bypass, replay, limits and misuse of legitimate functionality.
Browser security	Client-side trust, storage, messaging and CORS.
Files and integrations	Upload, download, APIs, webhooks and integration boundaries.
Logging and auditability	Whether relevant security events can be traced when operational evidence is available.

Engagement outcome

A prioritised technical report with reproducible evidence, affected roles or functions, remediation guidance and retest results.

How the engagement works

How we test or review

Damocles combines unauthenticated, role-based and architecture-assisted testing, retaining HTTP evidence for each observed behaviour. Document or configuration review is identified separately from runtime validation, and testing stops before availability, destructive data or uncontrolled account impact.

Testing and review perspectives

Unauthenticated application user

Exercises public routes, registration, login, recovery and pre-authentication browser behaviour without an account.

Included when: Used for entry points and controls reachable before authentication.

Access: Approved URLs, test window and any public workflow prerequisites.

Limitations: Cannot establish behaviour available only after login.

Standard authenticated user

Uses a dedicated ordinary account to test sessions, workflows, data handling and server-side enforcement.

Included when: Used for features available to a representative customer or workforce role.

Access: A test account, representative data and expected permissions.

Limitations: Findings apply to the supplied role and configured feature set.

Cross-role or cross-tenant identity

Repeats equivalent object and function requests between controlled roles or tenants to test isolation.

Included when: Used where role or tenant boundaries are explicitly in scope.

Access: At least two identities, representative objects and the expected access matrix.

Limitations: Establishes only the represented boundaries, not every role or tenant.

Privileged application user

Exercises administrative functions and privilege transitions with a controlled privileged account.

Included when: Used only when administrative application behaviour is included.

Access: A dedicated privileged identity, ordinary comparison identity and approved admin workflows.

Limitations: Does not authorise changes outside test data or prove all privileged roles.

Integration or API client

Calls approved APIs, webhooks and callbacks using scoped client credentials and controlled payloads.

Included when: Used for machine-to-machine paths that are part of the web service.

Access: Test client credentials, endpoint inventory, scopes, signing secrets and representative objects.

Limitations: Does not cover undocumented third-party systems or credentials not supplied.

Architecture-assisted reviewer

Correlates runtime requests with diagrams, deployment settings, trust boundaries, logging and cryptographic design evidence.

Included when: Used when architecture or configuration-assisted conclusions are agreed.

Access: Current diagrams, data flows, configuration excerpts and relevant operational evidence.

Limitations: Documents describe intended design and are not treated as proof of runtime enforcement.

Customer access or evidence typically required

Approved URLs, test window and any public workflow prerequisites.; A test account, representative data and expected permissions.; At least two identities, representative objects and the expected access matrix.; A dedicated privileged identity, ordinary comparison identity and approved admin workflows.; Test client credentials, endpoint inventory, scopes, signing secrets and representative objects.; Current diagrams, data flows, configuration excerpts and relevant operational evidence.

What you receive

A prioritised technical report with reproducible evidence, affected roles or functions, remediation guidance and retest results.

Detailed technical coverage

Discovery and entry points

What is assessed	Damocles enumerates approved application hosts, routes, parameters, virtual hosts and public entry points, reconciles them with the supplied inventory and records unexpected or missing exposure.
Perspective / access	Unauthenticated application user. Approved hostnames, base URLs, deployment inventory, public documentation and test window.
Evidence	Discovered host, route, parameter and response evidence is mapped to the expected application entry-point inventory.
References	Web Security Testing Guide 4.2 — WSTG-v42-INFO-02, WSTG-v42-INFO
Applicability	Applies to public and supplied application entry points included in the authorised scope.
Limitations	Discovery is bounded to approved hosts and does not establish hidden functionality that is unreachable from the tested position.

Architecture and trust boundaries

What is assessed	Damocles reviews diagrams and discovered entry points, identifies browser, application, API, identity, storage and third-party boundaries, then tests representative runtime crossings to confirm where trust is enforced.
Perspective / access	Architecture-assisted reviewer. Current architecture and data-flow diagrams, component and integration inventory, approved URLs, representative accounts and technical owners.
Evidence	Annotated boundary observations linked to the diagram, entry point and representative request or response used to validate the crossing.
References	Web Security Testing Guide 4.2
Applicability	Included when architecture evidence is supplied or multiple components and trust domains are in scope.
Limitations	Diagrams may not match every deployment; runtime testing covers representative crossings and does not authorise testing the third party itself.

Configuration

What is assessed	Damocles reviews deployment mode, security headers, CORS, error exposure, debug behaviour, administrative interfaces, default content and transport settings, then validates externally observable behaviour.
Perspective / access	Architecture-assisted reviewer. Approved application URLs, deployment and security configuration, expected headers and CORS policy, and representative public and authenticated routes.
Evidence	Configuration excerpts and HTTP request-and-response pairs showing the observed header, CORS, error, debug, default-content or administrative behaviour.
References	Web Security Testing Guide 4.2 — WSTG-v42-CONF
Applicability	Included when the relevant setting is observable or configuration evidence is supplied.
Limitations	A snapshot cannot prove consistent settings across excluded nodes or future releases; no production configuration is changed during review.

Identity lifecycle

What is assessed	Damocles tests registration, invitation, activation, role assignment, suspension, deactivation, deletion and reactivation paths, including orphaned identities and administrative lifecycle actions where included.
Perspective / access	Unauthenticated application user. Assessment requires approved URLs, controlled accounts, representative data and relevant architecture or configuration evidence, selected specifically for identity lifecycle.
Evidence	Evidence records the HTTP request, response, browser state, rendered output or cited configuration evidence relevant to identity lifecycle.
References	Web Security Testing Guide 4.2 — WSTG-v42-IDNT
Applicability	Applies to Identity lifecycle when the feature and representative identity are present in the authorised application.
Limitations	The conclusion is limited to the sampled identity lifecycle; results cover supplied roles, data and workflows; destructive data and availability impact are excluded.

Authentication, MFA and recovery

What is assessed	Damocles tests login controls, account enumeration, MFA enrolment and enforcement, recovery paths, reset tokens, alternate authentication routes, session establishment and approved lockout or throttling thresholds.
Perspective / access	Unauthenticated application user; Standard authenticated user. Unauthenticated login and recovery endpoints, standard test accounts, MFA factors, recovery channels and privileged authentication only where administration is in scope.
Evidence	HTTP exchanges and state observations record enumeration differences, MFA decisions, recovery-token handling, established sessions and bounded throttling results.
References	Web Security Testing Guide 4.2 — WSTG-v42-ATHN
Applicability	Applies to each customer-approved authentication, MFA and recovery path exposed by the application.
Limitations	Credential attempts remain within approved thresholds; Damocles does not lock real users, intercept third-party recovery messages or exhaust availability.

Role, function, object and tenant authorisation

What is assessed	Damocles attempts permitted and denied functions and varies representative object identifiers across standard, privileged and cross-role or cross-tenant identities to verify server-side role, function, object and tenant enforcement.
Perspective / access	Standard authenticated user; Cross-role or cross-tenant identity; Privileged application user. At least two representative identities in different roles or tenants, privileged access where included, representative objects and the expected access matrix.
Evidence	HTTP request-and-response pairs identify each identity, object or function, expected decision and observed authorisation result.
References	Web Security Testing Guide 4.2 — WSTG-v42-ATHZ
Applicability	Applies to server-side functions, records and tenant boundaries reachable by the supplied identities.
Limitations	Results cover only the supplied roles, tenants and objects; destructive changes and access to real customer data are prohibited.

Sessions, cookies and tokens

What is assessed	Damocles examines cookies, browser sessions and tokens across issuance, client storage, renewal, expiry, logout, revocation, fixation, replay and privilege changes.
Perspective / access	Standard authenticated user; Privileged application user. Standard authenticated accounts, privileged accounts where relevant, test browsers, issued tokens and documented session settings.
Evidence	Cookie attributes, token claims and HTTP exchanges show lifecycle transitions, replay outcomes, revocation and privilege-change behaviour.
References	Web Security Testing Guide 4.2 — WSTG-v42-SESS
Applicability	Applies to session or token mechanisms used by the supplied application identities.
Limitations	Testing does not assert lifecycle behaviour for excluded clients or identities and stops before disruption of shared identity services.

Input validation and injection

What is assessed	Damocles identifies interpreters and data contexts, submits safe representative payloads through reachable inputs, observes server-side handling and stops before destructive queries, commands or downstream effects.
Perspective / access	Unauthenticated application user. Approved routes and parameters, representative accounts and records, technology context where available, and prohibited payload or data boundaries.
Evidence	HTTP requests and responses showing the input, encoding, server behaviour and the minimum non-destructive proof for a confirmed injection condition.
References	Web Security Testing Guide 4.2 — WSTG-v42-INPV
Applicability	Applied to public and authenticated inputs reachable by the supplied perspectives.
Limitations	No destructive query, command execution, bulk extraction or unsafe out-of-band interaction is attempted without separate authority.

Output encoding

What is assessed	Damocles submits safe marker values through an identity able to create the affected data and observes rendering in HTML, attribute, URL, script and other relevant output contexts.
Perspective / access	Standard authenticated user. The submitting and viewing identities, representative writable fields, affected pages and approved marker payloads.
Evidence	The originating request, returned response, DOM or rendered result and exact output context are retained.
References	Web Security Testing Guide 4.2
Applicability	Applies to user-controlled values that the application returns or renders in a browser or downstream document.
Limitations	Active exploitation is limited to harmless proof; Damocles does not execute payloads that access real data or affect other users.

Error handling

What is assessed	Damocles sends malformed requests and triggers bounded exceptional conditions from unauthenticated and representative authenticated viewpoints, comparing response content, status, timing and recovery behaviour.
-------------------------	--

Perspective / access	Unauthenticated application user; Standard authenticated user. Approved endpoints, unauthenticated access, standard test accounts and known safe malformed values or exceptional conditions.
Evidence	Request-and-response pairs capture status, error details, identifiers, stack information and subsequent application availability.
References	Web Security Testing Guide 4.2 — WSTG-v42-ERRH
Applicability	Applies to reachable request handlers and workflows where safe exceptional conditions can be produced.
Limitations	No deliberate availability impact, resource exhaustion or destructive fault injection is performed.

Transport and cryptography

What is assessed	Damocles tests externally observable TLS versions, certificates, protocol negotiation and transport enforcement, and reviews application cryptographic use only when architecture or configuration evidence is supplied.
Perspective / access	Unauthenticated application user; Architecture-assisted reviewer. Approved hostnames and endpoints, an unauthenticated client path, and cryptographic design or configuration evidence when review is included.
Evidence	Certificate and protocol observations, redirect or enforcement responses, and cited configuration excerpts support each conclusion.
References	Web Security Testing Guide 4.2 — WSTG-v42-CRYP
Applicability	Applies to in-scope application transport and to cryptographic implementation expressly included with supporting evidence.
Limitations	External observation cannot establish internal key custody or implementation; intrusive downgrade and denial-of-service testing are excluded.

Business logic, workflow, replay and limits

What is assessed	Damocles follows required sequences and state transitions, safely repeats or replays operations, tests quantity, value and approval limits, and checks whether concurrency or legitimate features can bypass prerequisites across relevant roles or tenants.
Perspective / access	Standard authenticated user. Assessment requires approved URLs, controlled accounts, representative data and relevant architecture or configuration evidence, selected specifically for business logic, workflow, replay and limits.
Evidence	Evidence records the HTTP request, response, browser state, rendered output or cited configuration evidence relevant to business logic, workflow, replay and limits.
References	Web Security Testing Guide 4.2 — WSTG-v42-BUSL
Applicability	Applies to Business logic, workflow, replay and limits when the feature and representative identity are present in the authorised application.
Limitations	The conclusion is limited to the sampled business logic, workflow, replay and limits; results cover supplied roles, data and workflows; destructive data and availability impact are excluded.

Browser-side trust, storage, messaging and CORS

What is assessed	Damocles inspects browser storage and sensitive client-side state, exercises cross-window and cross-origin messaging, validates CORS trust, and tests whether client-enforced restrictions or browser-controlled values can be bypassed.
Perspective / access	Architecture-assisted reviewer. Assessment requires approved URLs, controlled accounts, representative data and relevant architecture or configuration evidence, selected specifically for browser-side trust, storage, messaging and CORS.
Evidence	Evidence records the HTTP request, response, browser state, rendered output or cited configuration evidence relevant to browser-side trust, storage, messaging and CORS.
References	Web Security Testing Guide 4.2 — WSTG-v42-CLNT
Applicability	Applies to Browser-side trust, storage, messaging and CORS when the feature and representative identity are present in the authorised application.
Limitations	The conclusion is limited to the sampled browser-side trust, storage, messaging and CORS; results cover supplied roles, data and workflows; destructive data and availability impact are excluded.

File handling

What is assessed	Damocles tests file type and content validation, filename and path handling, storage access, upload and download authorisation, preview or transformation services, active content, and size or processing limits within safe thresholds.
Perspective / access	Unauthenticated application user. Assessment requires approved URLs, controlled accounts, representative data and relevant architecture or configuration evidence, selected specifically for file handling.
Evidence	Evidence records the HTTP request, response, browser state, rendered output or cited configuration evidence relevant to file handling.
References	Web Security Testing Guide 4.2
Applicability	Applies to File handling when the feature and representative identity are present in the authorised application.
Limitations	The conclusion is limited to the sampled file handling; results cover supplied roles, data and workflows; destructive data and availability impact are excluded.

APIs, webhooks and integrations

What is assessed	Damocles uses the supplied integration or API client to test API authentication, authorisation and scopes, callback destination validation, webhook authenticity and replay, secret or signature handling, retry behaviour and third-party trust boundaries.
Perspective / access	Integration or API client; Standard authenticated user. API or integration credentials, schemas, representative objects for each role or tenant, webhook signing material and a controlled callback endpoint.
Evidence	API request-and-response pairs, webhook payload and signature results, callback observations and affected identity, tenant or object details.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Included only for APIs, webhooks and integrations explicitly named in scope.
Limitations	Testing does not authorise assessment of the third-party provider; callbacks, retries and state changes use controlled records and stop at agreed limits.

Logging, alerting and auditability

What is assessed	Damocles generates representative application events and, when log access is supplied, asks the operational reviewer to confirm the audit record, alert and handling outcome; absence of log access is recorded rather than inferred.
Perspective / access	Standard authenticated user; Architecture-assisted reviewer. A test account and records, agreed event scenarios, read-only application or central log access, expected source inventory and an operational reviewer.
Evidence	The generating request, event timestamp and identifier, received log record, alert or workflow status and any missing-field or delivery gap.
References	Web Security Testing Guide 4.2
Applicability	End-to-end confirmation is included only when log or workflow access is supplied; otherwise the row records that receipt was unable to be validated.
Limitations	A small event sample cannot prove continuous logging or detection; no conclusion is drawn about downstream handling when operational evidence is unavailable.

Methodologies and standards

Web Security Testing Guide 4.2 — Uses the stated WSTG 4.2 category to select relevant web test procedures; category coverage does not mean every test was completed.

Application Security Verification Standard 5.0.0 — Supports requirement-level verification only when exact ASVS 5.0.0 requirements are agreed and recorded in the statement of work and coverage matrix.

OWASP Top 10 2025 — Classifies relevant findings against OWASP Top 10:2025; it is not a testing procedure.

OWASP API Security Top 10 2023 — Classifies API findings against the 2023 risk taxonomy; it is not a complete testing method.

Common Weakness Enumeration 4.20 — Classifies confirmed weakness types using CWE 4.20.

Common Vulnerability Scoring System 4.0 — Calculates technical severity and records a CVSS 4.0 vector separately from customer impact.

Guidelines for Software Development June 2026 — Provides secure-development guidance relevant to the software procedure in scope.

Standards and control mappings

Information Security Manual June 2026 — directly-assessed

References: ISM-1552, ISM-1241, ISM-1424

Assessed: Observed HTTPS enforcement, output encoding and security response-header behaviour where those controls are present.

Evidence: Requests, responses and browser-observed behaviour linked to the affected route.

Applicability: Only the relevant application routes and behaviours in scope.

Limitations: Does not prove continuous enforcement or development-lifecycle governance.

Information Security Manual June 2026 — supporting-evidence

References: ISM-0971, ISM-1850, ISM-1851

Assessed: Application behaviour relevant to agreed ASVS requirements and OWASP web or API risk categories.

Evidence: Coverage and findings that may inform a broader secure-development assessment.

Applicability: API references apply only when APIs are expressly included.

Limitations: A point-in-time test cannot prove that the development lifecycle used ASVS or mitigated every taxonomy category.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Web application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Web application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Web application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

HTTP request-and-response evidence

Records http request-and-response evidence produced from the authorised Web application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Role and tenant coverage matrix

Records role and tenant coverage matrix produced from the authorised Web application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Workflow and authorisation evidence

Records workflow and authorisation evidence produced from the authorised Web application penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.

- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.