

TECHNICAL PRODUCT BRIEF

API penetration testing

Test the controls protecting API data and functions.

Why customers use this service

Test API endpoints across unauthenticated, authenticated, cross-role and integration contexts to expose access-control, token, input and workflow weaknesses.

What we assess

Endpoint inventory	Documented, hidden and versioned endpoints exposed by the service.
Object authorisation	Whether identities can reach another user or tenant's records.
Function and property access	Restricted operations and sensitive fields across roles.
Tokens and keys	Issuance, scope, expiry, replay and revocation controls.
Input processing	Injection, unsafe parsing, mass assignment and schema handling.
Business workflows	Sequence bypass, replay and misuse of legitimate operations.
Rate and resource controls	Abuse resistance for quotas, concurrency and expensive operations.
Integrations and logging	Webhook trust, downstream boundaries and traceable security events.

Engagement outcome

A prioritised API report with reproducible requests, affected objects or roles, remediation guidance and retest results.

[How the engagement works](#)

How we test or review

Damocles inventories interfaces and exercises representative API clients across roles and tenants, retaining request-and-response pairs for authorisation, state and resource-control decisions. Design evidence informs but does not substitute for runtime checks; unsafe volume and destructive operations are excluded.

Testing and review perspectives

Unauthenticated API client

Discovers approved interfaces and sends requests without credentials to observe public and authentication-failure behaviour.

Included when: Used for exposed inventory, authentication boundaries and public operations.

Access: Base URLs, published specifications, approved versions and testing windows.

Limitations: Cannot establish behaviour behind authenticated client or tenant boundaries.

Standard authenticated API client

Calls representative operations with an ordinary client or user token and records server-side decisions.

Included when: Used for token lifecycle, object access, workflows and resource controls.

Access: Dedicated credentials, token acquisition steps, scopes and representative objects.

Limitations: Results apply to the supplied client, role, scopes and data.

Cross-role or cross-tenant API identities

Replays equivalent API operations across controlled roles or tenants while exchanging object and property values.

Included when: Used for object, property, function and tenant authorisation.

Access: At least two identities in different roles or tenants plus representative records.

Limitations: Does not establish separation for identities, tenants or object types not represented.

Privileged API client

Invokes approved administrative operations with a dedicated privileged token and compares lower-privilege outcomes.

Included when: Used where privileged API functions are expressly included.

Access: Privileged and standard test credentials, expected permissions and disposable records.

Limitations: No production administration or destructive operation is authorised.

Integration client

Exercises approved webhook, callback and upstream-integration paths using controlled secrets and messages.

Included when: Used when integrations form part of the scoped API trust boundary.

Access: Signing secrets, callback endpoints, retry expectations and representative messages.

Limitations: Does not authorise testing of the external provider itself.

Architecture-assisted reviewer

Compares observed routes, schemas and controls with API specifications, gateway policy and data-flow evidence.

Included when: Used for inventory reconciliation and design-assisted analysis.

Access: Specifications, version inventory, gateway exports, schemas and trust-boundary diagrams.

Limitations: Design evidence cannot prove enforcement on routes that were not exercised.

Customer access or evidence typically required

Base URLs, published specifications, approved versions and testing windows.; Dedicated credentials, token acquisition steps, scopes and representative objects.; At least two identities in different roles or tenants plus representative records.; Privileged and standard test credentials, expected permissions and disposable records.; Signing secrets, callback endpoints, retry expectations and representative messages.; Specifications, version inventory, gateway exports, schemas and trust-boundary diagrams.

What you receive

A prioritised API report with reproducible requests, affected objects or roles, remediation guidance and retest results.

Detailed technical coverage

Interface and version inventory

What is assessed	Damocles enumerates documented and observed API routes, methods and versions and reconciles them with the supported interface inventory.
Perspective / access	Architecture-assisted reviewer. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for interface and version inventory.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to interface and version inventory.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Interface and version inventory when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled interface and version inventory; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Authentication

What is assessed	Damocles tests client and user authentication, token acquisition, unauthenticated requests, failure responses and error behaviour across approved authentication mechanisms.
Perspective / access	Standard authenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for authentication.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to authentication.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Authentication when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled authentication; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Token and key lifecycle

What is assessed	Damocles follows token and key issuance, scopes, audience, storage, expiry, rotation, revocation and replay using representative authenticated clients.
Perspective / access	Standard authenticated API client; Architecture-assisted reviewer. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for token and key lifecycle.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to token and key lifecycle.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Token and key lifecycle when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled token and key lifecycle; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Object-level authorisation

What is assessed	Damocles changes representative object identifiers between controlled identities and tenants and compares the server-side access decision.
Perspective / access	Standard authenticated API client; Cross-role or cross-tenant API identities. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for object-level authorisation.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to object-level authorisation.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Object-level authorisation when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled object-level authorisation; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Property-level authorisation

What is assessed	Damocles submits and retrieves fields that the current role should not set or view and records whether property-level policy is enforced.
Perspective / access	Standard authenticated API client; Cross-role or cross-tenant API identities. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for property-level authorisation.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to property-level authorisation.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Property-level authorisation when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled property-level authorisation; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Function-level authorisation

What is assessed	Damocles invokes approved privileged functions with lower-privilege tokens and compares the response with the expected function-level policy.
Perspective / access	Standard authenticated API client; Cross-role or cross-tenant API identities. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for function-level authorisation.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to function-level authorisation.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Function-level authorisation when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled function-level authorisation; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Tenant separation

What is assessed	Damocles exchanges tenant-owned identifiers and context between at least two controlled tenants to test isolation of data and operations.
Perspective / access	Standard authenticated API client; Cross-role or cross-tenant API identities. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for tenant separation.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to tenant separation.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Tenant separation when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled tenant separation; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Excessive data exposure

What is assessed	Damocles compares documented response schemas with fields returned to representative roles and identifies unnecessary sensitive data exposure.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for excessive data exposure.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to excessive data exposure.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Excessive data exposure when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled excessive data exposure; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Mass assignment and unsafe property binding

What is assessed	Damocles adds protected, immutable or server-managed properties to create and update operations and observes binding and validation behaviour.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for mass assignment and unsafe property binding.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to mass assignment and unsafe property binding.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Mass assignment and unsafe property binding when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled mass assignment and unsafe property binding; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Workflow and state manipulation

What is assessed	Damocles reorders, skips or repeats required API state transitions using disposable records and compares the resulting state with workflow rules.
-------------------------	---

Perspective / access	Standard authenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for workflow and state manipulation.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to workflow and state manipulation.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Workflow and state manipulation when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled workflow and state manipulation; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Replay and duplicate operations

What is assessed	Damocles safely replays representative transactions and duplicate messages to assess idempotency, duplicate processing and state consistency.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for replay and duplicate operations.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to replay and duplicate operations.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Replay and duplicate operations when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled replay and duplicate operations; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Rate and resource controls

What is assessed	Damocles sends bounded request rates and safe resource parameters to assess throttling, quotas, pagination, concurrency, costly operations and resource limits.
Perspective / access	Unauthenticated API client. Approved endpoints, dedicated clients, bounded request-rate ceilings, safe pagination and resource parameters, and expected quota behaviour.
Evidence	API request timing, response status and headers, quota state and resource-consumption observations at each approved rate.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies where API rate, quota, pagination, concurrency or expensive-operation controls are implemented and safe to sample.
Limitations	Traffic remains below approved ceilings; results do not establish capacity under denial-of-service or sustained production load.

Deprecated and shadow interfaces

What is assessed	Damocles compares discovered routes and versions with the supported inventory and safely checks deprecated, undocumented or shadow interfaces.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for deprecated and shadow interfaces.

Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to deprecated and shadow interfaces.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Deprecated and shadow interfaces when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled deprecated and shadow interfaces; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Unsafe consumption of third-party APIs

What is assessed	Damocles reviews validation and trust applied to data received from approved upstream integrations without interacting with or testing the provider itself.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for unsafe consumption of third-party APIs.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to unsafe consumption of third-party APIs.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Unsafe consumption of third-party APIs when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled unsafe consumption of third-party APIs; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

Webhooks and callbacks

What is assessed	Damocles tests webhook signatures, authenticity, replay, callback destinations, retry behaviour and tenant or object association using controlled messages.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for webhooks and callbacks.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to webhooks and callbacks.
References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to Webhooks and callbacks when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled webhooks and callbacks; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

GraphQL behaviour

What is assessed	Damocles tests introspection, field and resolver authorisation, query depth and complexity, batching and aliases within safe limits when GraphQL is present.
Perspective / access	Unauthenticated API client. Assessment requires approved endpoints, specifications, controlled clients, representative objects and expected role or tenant behaviour, selected specifically for graphql behaviour.
Evidence	Evidence records the API request, response, token, object state or gateway evidence relevant to graphql behaviour.

References	Web Security Testing Guide 4.2 — WSTG-v42-APIT
Applicability	Applies to GraphQL behaviour when the operation and required representative identities or integration are in scope.
Limitations	The conclusion is limited to the sampled graphql behaviour; results cover supplied clients, objects and bounded rates; destructive or provider-side testing is excluded.

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 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.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised API penetration testing scope.

Evidence: Coverage status, procedure results and findings can inform the customer’s control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised API 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 API 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 API 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.

API request-and-response evidence

Records API request-and-response evidence produced from the authorised API 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.

Object and tenant coverage matrix

Records object and tenant coverage matrix produced from the authorised API 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.

Token and workflow evidence

Records token and workflow evidence produced from the authorised API 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.