

Web Application Penetration Testing. Course preview. Curriculum 1.85.0; syllabus 1.24.0. PDF presentation 1.0.2.

Structured HTML:

<https://hackermartin.com/courses/web-application-penetration-testing/syllabus>. This PDF has no screen-reader document tags or interactive links. Full accessibility and learner testing are still pending.

Web Application Penetration Testing

Course preview. Browse the syllabus and try the separate practice course. Purchase and learner enrollment are not open.

Terms used on this page: Hypertext Transfer Protocol (HTTP) is the request-and-response language between a browser and a web service. Artificial intelligence (AI) means automated generated help; retrieval-augmented generation (RAG) is AI help using selected source material. These aids are excluded during independent assessment.

Syllabus 1.24.0; curriculum 1.85.0. 43 lessons and 34 guided practices.

Begin with BEST BCID: Baseline, Change, Compare, Interpret, Document. Learn request and evidence reasoning, investigate controlled boundaries, report findings and preserve useful functions when retesting corrections.

Entry guidance: basic computer use, reading HTTP requests and responses, and permission to work only within the supplied fictional scope. BEST BCID teaches the comparison method before domain-specific investigation. Study recommendations do not waive lab authorization.

Work through instruction, worked examples, explained formative checks, guided, semi-guided and blind formative work, integrated reporting, then the independent assessment rehearsal. Blind formative work is not an independent exam. AI/RAG/hints and formative practice are excluded during an independent attempt. Lesson completion checks and saved observation records are ungraded.

Beginner start and useful feedback

Read the first BCID lesson, then open its reading-card practice in the separate practice course. Select Ada and own-card for a useful baseline, then other-card to change ownership. Read the response status, the named card owner and the marker (a distinctive value in the card) together. Compare corrected denial with corrected own-card success; denying everything is not a useful correction.

Worked formative interpretation: if the same supplied actor receives the other owner's marker after only the object changes, the observation contradicts own-only policy. It supports a finding about permission checks in this controlled exercise; it does not establish real login or browser behavior.

Explore is temporary. Record collects again and saves a saved observation record (a receipt) that cannot be overwritten; cite its actual identifier, request, response and context. Start again retains prior evidence and creates a fresh run. If evidence is incomplete, say what is unknown and which authorized comparison would resolve it. Formative feedback explains the policy and missing comparison; filling every field does not establish the quality of your report.

In the linked HTML syllabus, open a module heading to read its outcomes, lessons and practice inventory. The starting module opens first; module links open their target. Without scripts all details start open. This PDF lists all module details below.

Ordered topics and status-labeled labs

All 34 guided practices appear under their instructional module. Offline workbooks often overlap these exercises rather than adding new independent labs. Exercises use controlled targets or supplied records. Their limitations explain which observations they support; do not infer behavior on real accounts or other systems.

BEST BCID method

HTTP session lifecycle

Authorization boundaries

Browser security boundaries

DOM input and text boundaries

Recovery authority

Content discovery evidence

Authentication authority

HTTP authentication evidence

Input interpretation

Trusted reconstruction

Continuing channel authority

GraphQL resolver boundaries

REST request and response boundaries

LLM tool and data boundaries

Resolved file containment

File upload storage and retrieval

Server-side destination boundaries

XML parser entity boundaries

JWT trust and application claims

OAuth and OpenID Connect transaction boundaries

TLS and HTTPS assessment basics

Integrated engagement and evidence reporting

Course overview: </courses/web-application-penetration-testing>

Course description and intended audience

Learn to investigate web application security using BEST BCID: Baseline, Change, Compare, Interpret, Document. Study how sessions, authentication, authorization, browser behavior, input handling, APIs and transport trust affect what an application permits. Compare expected policy with observed behavior in original controlled activities, document evidence and uncertainty, and check that a correction preserves legitimate use. Practice combines isolated exercises, simulations and reasoning from supplied records. These formats teach different parts of an investigation; they are not interchangeable evidence of practical competence.

Aspiring web application penetration testers who can already navigate a browser and read a basic HTTP request.

Application developers and application security practitioners learning to test trust boundaries and explain reproducible findings.

Security analysts and defenders who want to interpret web testing evidence and verify the limits of a reported finding.

Prerequisites

Use a browser, files and a terminal at a beginner level; individual practical guides explain their setup and commands.

Recognize a URL, HTTP method, request, response and status code; review introductory HTTP material first if these are unfamiliar.

Understand that testing requires authorization and a defined scope; use only the supplied isolated training targets.

No prior OAuth, GraphQL or certificate-analysis expertise is assumed; the associated lessons introduce their terms before practice.

Equipment and training format

Browser, terminal and local files. Individual isolated practical guides specify Python, browser or OpenSSL requirements; no paid cloud account is required by this outline.

Self-paced lessons and ungraded practice in a separate preview course.

Career context and expected effort

This course introduces web testing and application security. It does not award an employment or government qualification.

No pilot-grounded course duration is available yet.

Price and availability

Standard displayed price: \$349 USD. Purchase disabled.

Individual access will last 183 days when the course is released. Browsing this preview does not begin that access period.

Purchase and learner enrollment are not open. Browse this syllabus without signing in. Partner discounts and bundles have separate terms.

1. BEST BCID method

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Apply Baseline, Change, Compare, Interpret, Document before technical Web practice.

Separate observations, interpretation and completion from assessed competence.

Topics

BEST BCID for Web investigations: Apply Baseline, Change, Compare, Interpret, Document before technical Web practice; Separate observations, interpretation and completion from assessed competence.

Practice inventory

Study BEST BCID method through these original lessons and evidence objectives.

Recommended preparation: Course prerequisites below

BEST BCID: compare fictional reading cards

Controlled practice; saved observation records cannot be overwritten and are not graded.

Executable isolated in-process HTTP reading-card comparisons

Prerequisites: web-best-bcid-method

Modes: guided, semi-guided, blind, retest

Limits: Fixture identity is supplied, not authenticated; no browser, network or production assurance

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

2. HTTP session lifecycle

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish browser cookie removal from server-side session invalidation.

Separate cached display from fresh authenticated server evidence.

Build a controlled session-lifecycle comparison and bounded retest.

Topics

HTTP sessions: logout, fresh requests and cached displays: Distinguish browser cookie removal from server-side session invalidation; Separate cached display from fresh authenticated server evidence; Build a controlled session-lifecycle comparison and bounded retest.

Practice inventory

Study HTTP session lifecycle through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

HTTP sessions: logout, fresh requests and cached displays

Controlled practice; saved observation records cannot be overwritten.

Fixed in-process synthetic session observations

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Two fictional accounts and three fixed observation modes. Fresh replay, cached display and no-credential comparisons with corrected retest are synthetic formative evidence; no native HTTP/browser execution, real credentials, concurrency or other-device validation.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Earlier exercises – not available in the practice course

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

HTTP sessions: logout, fresh requests and cached displays

Not available in the practice course.

Supplied-record simulation

Limits: Compare fresh logout replay with cached display and a no-credential control; no browser, cookies or HTTP execution.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

3. Authorization boundaries

4 lessons; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Separate authentication, object ownership, role and tenant policy.

Choose approved identities and controls before modifying a request.

Demonstrate a bounded horizontal access-control failure.

Distinguish a guessable identifier from missing object authorization.

Separate object-level access from permission to perform a function.

Verify state-changing impact with positive and negative controls.

Produce reproducible B-CID evidence with bounded impact.

Retest the denied operation while preserving approved behavior.

Topics

Build an authorization test matrix: Separate authentication, object ownership, role and tenant policy; Choose approved identities and controls before modifying a request.

Test object references with controlled comparisons: Demonstrate a bounded horizontal access-control failure; Distinguish a guessable identifier from missing object authorization.

Test privileged functions and tenant boundaries: Separate object-level access from permission to perform a function; Verify state-changing impact with positive and negative controls.

Write an access-control finding and a defensible retest: Produce reproducible B-CID evidence with bounded impact; Retest the denied operation while preserving approved behavior.

Practice inventory

Study Authorization boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Access control: owners, roles and tenants

Controlled practice; saved observation records cannot be overwritten and are not graded.

Executable isolated in-process HTTP invoice authorization comparisons

Prerequisites: web-best-bcid-method, web-access-policy, web-idor-comparison, web-role-and-function, web-access-report-retest

Modes: guided, semi-guided, blind, retest

Limits: No production identity, browser, concurrency or exhaustive route assurance

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Earlier exercises – not available in the practice course

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Access control: owners, roles and tenants

Not available in the practice course.

Executable isolated WSGI fixture

Limits: Compare owner, role, tenant and refund state; fixture identities are supplied; no browser, TLS or production authentication.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

4. Browser security boundaries

4 lessons; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Separate origin, site and cookie delivery before interpreting a cross-site request.

Describe what a server trace can establish and what requires browser evidence.

Establish a bounded authenticated state-changing request without confusing response readability.

Retest session-bound tokens, origin checks and legitimate use.

Distinguish server authorization from browser permission to expose a response.

Evaluate exact origins and credentialed-response controls without overstating impact.

Distinguish embeddability from a demonstrated unintended user action.

Test framing headers while preserving allowed navigation.

Topics

Origins, sites and credential delivery: Separate origin, site and cookie delivery before interpreting a cross-site request; Describe what a server trace can establish and what requires browser evidence.

CSRF: verify the state change and the request defense: Establish a bounded authenticated state-changing request without confusing response readability; Retest session-bound tokens, origin checks and legitimate use.

CORS: response sharing is a separate boundary: Distinguish server authorization from browser permission to expose a response; Evaluate exact origins and credentialed-response controls without overstating impact.

Clickjacking: framing permission and user interaction: Distinguish embeddability from a demonstrated unintended user action; Test framing headers while preserving allowed navigation.

Practice inventory

Study Browser security boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Browser boundaries: requests, reads and frames

Controlled practice; saved observation records cannot be overwritten and are not graded.

Executable isolated in-process HTTP browser-boundary comparisons

Prerequisites: web-best-bcid-method, web-origin-site-credentials, web-csrf-state-change, web-cors-response-reading, web-framing-and-retest

Modes: guided, semi-guided, blind, retest

Limits: No production identity, browser, concurrency or exhaustive route assurance

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Fixed browser exercises

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

CORS reads and framing comparisons

Separate local exercise; observations are not saved to your course notebook.

Fixed original browser fixture / optional native harness

Limits: Executable loopback fixture responses; native browser harness separate. Same-site origins only; no cross-site cookie, CSRF, production session or TLS proof.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Earlier exercises – not available in the practice course

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Browser boundaries: requests, reads and frames

Not available in the practice course.

Executable isolated WSGI fixture

Limits: Compare server state, response and headers. Browser readability, framing and cookie delivery are unmeasured by this provider.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

5. DOM input and text boundaries

3 lessons; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Trace query/fragment input through decoding to a DOM operation.

Distinguish source controllability, markup interpretation and script execution.

Use a benign execution marker without accessing accounts or external targets.

Avoid equating HTML insertion, script tags and actual event execution.

Retest a text sink with both the original marker and ordinary names.

Document decoding/context limits and map unfamiliar evidence to an independent task.

Topics

Trace browser input from source to sink: Trace query/fragment input through decoding to a DOM operation; Distinguish source controllability, markup interpretation and script execution.

Separate HTML interpretation from executable effects: Use a benign execution marker without accessing accounts or external targets; Avoid equating HTML insertion, script tags and actual event execution.

Fix the sink and preserve intended display: Retest a text sink with both the original marker and ordinary names; Document decoding/context limits and map unfamiliar evidence to an independent task.

Practice inventory

Study DOM input and text boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

DOM sources, markup and benign execution: supplied-model comparisons

Controlled practice; saved observation records cannot be overwritten.

Fixed supplied-model DOM observations

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Three fixed supplied cases with query/fragment comparisons and useful display, markup and benign marker controls. Synthetic formative observations; no native browser execution or learner-collected browser evidence. This activity has not yet been tested with learners or assistive technology.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Fixed browser exercises

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

DOM source and sink comparisons

Separate local exercise; observations are not saved to your course notebook.

Fixed original browser fixture / optional native harness

Limits: Twelve fixed query/fragment and initial/corrected sink cases. Local benign marker only; no arbitrary payload, account impact, Trusted Types or multi-browser proof. These observations do not establish behavior on another host.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Auxiliary evidence exercises

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

DOM prediction and observation worksheet

Local workbook exercise; observations are not saved to your course notebook.

Empty worksheet

Limits: Six empty rows per selected source; preparation executes no browser and collects no evidence. Browser observations must be recorded separately; no automatic grade or managed receipt.

Preparation: Read the DOM source/sink lessons; recognize URL query/fragment and plain text. Record observations separately in the supplied browser fixture.

6. Recovery authority

2 lessons; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Isolate account binding, expiry and single-use recovery boundaries.

Support a bounded finding with state evidence and fresh controls.

Distinguish reset request, recipient delivery, victim action and usable account authority.

Compare a requester Host with configured reset authority using fixed local controls.

Document a correction with legitimate recovery and account-specific session retests.

Topics

Test recovery authority and lifecycle: Isolate account binding, expiry and single-use recovery boundaries; Support a bounded finding with state evidence and fresh controls; Distinguish reset request, recipient delivery, victim action and usable account authority; Compare a requester Host with configured reset authority using fixed local controls; Document a correction with legitimate recovery and account-specific session retests.

Trace reset-link authority from request to fresh login: Distinguish reset request, recipient delivery, victim action and usable account authority; Compare a requester Host with configured reset authority using fixed local controls; Document a correction with legitimate recovery and account-specific session retests.

Practice inventory

Study Recovery authority through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Reset-link authority: isolated HTTP and modeled recipient comparisons

Controlled practice; saved observation records cannot be overwritten.

Executable isolated HTTP reset authority fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Member-a only in an original disposable in-process HTTP fixture. Recipient action is modeled; no real email, MFA or browser delivery. Compare original and corrected reset authority, session/login observations and legitimate recovery control. Formative receipts do not attest every session, independently demonstrated skill or full course completion.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Reset authority

Local workbook exercise; observations are not submitted to your course notebook.

Executable fixture with simulated components

Limits: Flask requests execute; victim link opening/capture modeled, no mail or browser action.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Earlier exercises – not available in the practice course

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Recovery authority: controlled lifecycle comparisons

Not available in the practice course.

State-machine simulation

Limits: Compare account binding, clock, replay and credential counters; symbolic references are not real tokens, email or password changes.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

7. Content discovery evidence

2 lessons; 2 managed practices; controlled preview

Lesson outcomes and practice

Outcomes

Compare public, absent and authorized controls before claiming protected disclosure.

Separate delivered bytes from HEAD metadata and redirect destinations.

Retest a correction with fresh lineage and retained legitimate access.

Distinguish HTTP authority routing from DNS and TLS evidence.

Use absent-name controls before interpreting a discovered representation.

Retest authorization while preserving public and staff access.

Topics

Decide what a discovery response proves: Compare public, absent and authorized controls before claiming protected disclosure; Separate delivered bytes from HEAD metadata and redirect destinations; Retest a correction with fresh lineage and retained legitimate access; Distinguish HTTP authority routing from DNS and TLS evidence; Use absent-name controls before interpreting a discovered representation; Retest authorization while preserving public and staff access.

Discover site boundaries and retest roster authorization: Distinguish HTTP authority routing from DNS and TLS evidence; Use absent-name controls before interpreting a discovered representation; Retest authorization while preserving public and staff access.

Practice inventory

Study Content discovery evidence through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Virtual-host routing: evidence and authority

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: In-process HTTP host routing; fictional authority and fixed requests, no DNS or listener.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

HTTP discovery: observed bodies and authorization controls

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: In-process HTTP discovery comparisons; observed bodies and authorization controls, no external target.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Discovery workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Fixed in-process routes; not a general scanner or external enumeration.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Virtual hosts

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: WSGI hostname routing; no DNS, SNI, TLS, proxy or real identity validation.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Auxiliary evidence exercises

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Discovery request and response capture

Local workbook exercise; observations are not saved to your course notebook.

Executable isolated fixture with simulated actors

Limits: Seven fixed in-process WSGI exchanges; supplied role headers are not authenticated identities. No wire, TLS, proxy or browser evidence.

Preparation: Read the discovery workbook first; recognize GET/HEAD, response bodies, supplied actors and the expected route policy. Scope inventory additionally requires the enumeration workbook.

Finite route enumeration

Local workbook exercise; observations are not saved to your course notebook.

Executable isolated fixture with simulated actors

Limits: Seven supplied routes, GET/HEAD and absent controls; no arbitrary wordlist, scanner, network or completeness claim.

Preparation: Read the discovery workbook first; recognize GET/HEAD, response bodies, supplied actors and the expected route policy. Scope inventory additionally requires the enumeration workbook.

One-variable discovery comparisons

Local workbook exercise; observations are not saved to your course notebook.

Executable isolated fixture with simulated actors

Limits: Thirteen fixed in-process request comparisons; no arbitrary URL/payload, normalization-bypass or authentication proof.

Preparation: Read the discovery workbook first; recognize GET/HEAD, response bodies, supplied actors and the expected route policy. Scope inventory additionally requires the enumeration workbook.

Scoped discovery evidence inventory

Local workbook exercise; observations are not saved to your course notebook.

Executable isolated fixture with simulated actors

Limits: Forty-two in-process observations from six bounded runs; blank interpretation fields require learner reasoning. Redirect destinations and real application completeness remain untested.

Preparation: Read the discovery workbook first; recognize GET/HEAD, response bodies, supplied actors and the expected route policy. Scope inventory additionally requires the enumeration workbook.

Earlier exercises – not available in the practice course

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Content discovery: evidence before impact

Not available in the practice course.

Supplied-record simulation

Limits: Compare fixed fictional bytes, soft-404 controls, HEAD and unfollowed redirects; no HTTP execution or scanner.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

HTTP discovery: observed bodies and authorization controls

Not available in the practice course.

Executable isolated WSGI fixture

Limits: Compare seven actual in-process exchanges with supplied actor headers; no authenticated identities, network or redirect following.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

Virtual-host routing: evidence and authority

Not available in the practice course.

Executable isolated WSGI fixture

Limits: Compare four fixed hosts and roster policy; supplied role headers, no DNS, SNI, TLS or real authentication.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

8. Authentication authority

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish identity recognition from verified private-resource authority.

Retest renewal revocation while preserving legitimate access and account identity.

Separate sequential symbolic-authority evidence from the disposable HTTP fixture and state the boundary each supports.

Topics

Compare pending, verified and renewed authority: Distinguish identity recognition from verified private-resource authority; Retest renewal revocation while preserving legitimate access and account identity; Separate sequential symbolic-authority evidence from the disposable HTTP fixture and state the boundary each supports.

Practice inventory

Study Authentication authority through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Pending, verified and renewed authority: symbolic comparisons

Controlled practice; saved observation records cannot be overwritten.

Sequential symbolic authentication authority model

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed fictional identities and supplied factor result; sequential private-read and renewal comparisons only. No actual password, MFA, cookie, HTTP, browser, timing, concurrency or takeover validation. Single-reference fixture logout does not establish BEST account-wide logout behavior. Formative receipts are ungraded; independent assessment excludes this practice and AI/RAG.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

9. HTTP authentication evidence

3 lessons; 3 managed practices; controlled preview

Lesson outcomes and practice

Outcomes

Compare pending and verified HTTP private access with controls.

Verify renewal and account revocation without inferring real MFA or takeover.

Distinguish recipient-channel authorization from challenge/session verification.

Compare cross-recipient denial, legitimate delivery, one-use consumption and exact expiry.

Document modeled private-read evidence without claiming independent factor possession.

Separate channel change from verified private authority.

Compare queued and already-delivered challenge retirement with useful access.

Document rebinding and recovery separately with honest assurance limits.

Topics

Collect HTTP authentication boundary evidence: Compare pending and verified HTTP private access with controls; Verify renewal and account revocation without inferring real MFA or takeover.

Separate challenge verification from recipient delivery: Distinguish recipient-channel authorization from challenge/session verification; Compare cross-recipient denial, legitimate delivery, one-use consumption and exact expiry; Document modeled private-read evidence without claiming independent factor possession.

Retire old recipient authority during rebinding and recovery: Separate channel change from verified private authority; Compare queued and already-delivered challenge retirement with useful access; Document rebinding and recovery separately with honest assurance limits.

Practice inventory

Study HTTP authentication evidence through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

HTTP password, challenge, renewal and logout comparisons

Controlled practice; saved observation records cannot be overwritten.

Executable isolated HTTP authentication fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Original disposable in-process HTTP fixture for both fictional members: pending, renewal, account logout and credential lockout. Fixed sanitized observations and corrected retests; no real MFA delivery, browser or live account testing. Formative receipts do not establish independently demonstrated skill, full course completion or certification.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Recipient delivery and challenge verification comparisons

Controlled practice; saved observation records cannot be overwritten.

Executable isolated recipient capability model with WSGI verification

Prerequisites: BEST BCID, HTTP authentication boundary and recipient binding instruction

Modes: guided, semi-guided, blind formative, retest

Limits: In-process recipient capability simulation and WSGI verification only; no independent device, mailbox, browser, factor recovery, competence or release validation.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Recipient rebinding and recovery lifecycle comparisons

Controlled practice; saved observation records cannot be overwritten and are not graded.

Executable isolated in-process WSGI recipient lifecycle comparisons

Prerequisites: web-best-bcid-method, web-authentication-http-boundary, web-authentication-recipient-binding, web-authentication-recipient-lifecycle

Modes: guided, semi-guided, blind, retest

Limits: No real device, mailbox, identity proofing or independent recovery assurance; no browser execution

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Authentication workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: In-process Flask; factor delivery uses owner-controlled substitutes.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Earlier exercises – not available in the practice course

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

HTTP authentication comparisons

Not available in the practice course.

Executable isolated WSGI fixture

Limits: Compare password/challenge verification, renewal and logout; harness privately supplies challenges, no independent delivery channel or native browser.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

HTTP authentication learner practice

Not available in the practice course.

Executable isolated WSGI fixture

Limits: Historical controlled provider also underlies managed practice. Injected clock measures challenge/session boundaries; harness supplies challenges. No new distinct lab or browser timing proof.

Preparation: read BEST BCID and this module's lessons, then state the expected policy before choosing supplied comparisons. Use only the fictional inputs described in the exercise instructions.

Symbolic review activity

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Symbolic authentication authority comparisons

Earlier review activity; not available in the practice course.

Bounded state-machine simulation

Limits: Supplied factor-acceptance boolean and symbolic authority only; no measured password, OTP, cookies, concurrency or real account impact. Each submission creates fresh state; no enrollment, progress, independent evidence, score or mastery persists. Alternate path, not a new distinct lab.

Preparation: read BEST BCID, session authority and authentication lessons. This earlier review activity has no learner launch route.

Versioned workbook additions

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Recipient binding comparisons

Standalone formative collection only; not a managed learner practice

In-process recipient capability model with isolated WSGI verification

Limits: In-process recipient capability simulation and WSGI verification only; no independent device, mailbox, browser, factor recovery, competence or release validation.

Preparation: BEST BCID and HTTP authentication boundary instruction

10. Input interpretation

2 lessons; 2 managed practices; controlled preview

Lesson outcomes and practice

Outcomes

Trace raw query, intake, policy and consumer values.

Distinguish form-space from literal plus.

Retest denial and legitimate access with B-CID evidence.

Distinguish JSON scalar data from selector structure.

Apply trusted ownership scope alongside type validation.

Retest denial and legitimate function using B-CID evidence.

Topics

Trace identifiers through decoding and authorization: Trace raw query, intake, policy and consumer values; Distinguish form-space from literal plus; Retest denial and legitimate access with B-CID evidence.

Keep selection data separate from query structure: Distinguish JSON scalar data from selector structure; Apply trusted ownership scope alongside type validation; Retest denial and legitimate function using B-CID evidence.

Practice inventory

Study Input interpretation through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Encoding boundary: evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed WSGI decoding comparisons; role headers are scaffolding, no real login.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

NoSQL selector: evidence and correction

Controlled practice in the separate practice course.

Simulation

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Finite Python selector model; no native database.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Encoding workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: ASCII query decoding only; no universal encoding or bypass validation.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Nosql workbook

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: Fixed modeled queries; no database engine.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

11. Trusted reconstruction

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Trace integrity, inert validation, reconstruction and authorization separately.

Distinguish modeled side effects from native execution evidence.

Retest corrected denial and useful role access using B-CID.

Topics

Keep reconstructed state inside a trusted data contract: Trace integrity, inert validation, reconstruction and authorization separately; Distinguish modeled side effects from native execution evidence; Retest corrected denial and useful role access using B-CID.

Practice inventory

Study Trusted reconstruction through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Reconstruction boundary: evidence and correction

Controlled practice in the separate practice course.

Simulation

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Inert reconstruction model and boolean hook marker; no gadget or code execution.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Deserialization comparison

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: Paired inert reconstruction model; combined correction does not isolate individual control causality.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Deserialization workbook

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: No native object loader or executable serialized objects.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

12. Continuing channel authority

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Separate origin admission from trusted identity and object permission.

Compare existing-channel revocation and reconnect evidence.

Retest useful role access and document model limits using B-CID.

Topics

Check authority throughout a channel lifetime: Separate origin admission from trusted identity and object permission; Compare existing-channel revocation and reconnect evidence; Retest useful role access and document model limits using B-CID.

Practice inventory

Study Continuing channel authority through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Continuing channel authority: evidence and correction

Controlled practice in the separate practice course.

Simulation

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Offline channel-state model; no WebSocket transport or browser.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Websocket workbook

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: Fictional channel state machine; no native WebSocket transport.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

13. GraphQL resolver boundaries

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish object permission from field permission using useful controls.

Trace authorization through aliases, nested paths and partial responses.

Compare query admission controls and document bounded B-CID evidence.

Topics

Trace GraphQL object, field and query boundaries: Distinguish object permission from field permission using useful controls; Trace authorization through aliases, nested paths and partial responses; Compare query admission controls and document bounded B-CID evidence.

Practice inventory

Study GraphQL resolver boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

GraphQL resolver boundaries: evidence and correction

Controlled practice in the separate practice course.

Simulation

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed authored resolver plans; no GraphQL text parser or external endpoint.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

GraphQL workbook

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: Fixed resolver model; no native GraphQL engine.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

14. REST request and response boundaries

2 lessons; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Compare object read/write policy with actual HTTP observations.

Distinguish protected-property assignment from response disclosure.

Verify atomic rejection and preserved useful access with B-CID evidence.

Separate client-visible responses from privileged instrumentation.

Explain atomic rejection, earlier failure and useful correction controls.

Produce bounded reproducible REST B-CID claims with explicit uncertainty.

Topics

Test REST object and property boundaries: Compare object read/write policy with actual HTTP observations; Distinguish protected-property assignment from response disclosure; Verify atomic rejection and preserved useful access with B-CID evidence.

Build a defensible REST correction claim ledger: Separate client-visible responses from privileged instrumentation; Explain atomic rejection, earlier failure and useful correction controls; Produce bounded reproducible REST B-CID claims with explicit uncertainty.

Practice inventory

Study REST request and response boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

REST HTTP boundaries: evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed in-process HTTP requests and booking-state comparisons; no network listener.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Rest workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Fixed in-process HTTP/JSON; no production API transport.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

15. LLM tool and data boundaries

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Identify trusted identity separately from retrieved instructions and proposed arguments.

Compare object, field and tool policy with state and useful controls.

Document gateway evidence without claiming actual model attack success.

Topics

Validate proposed tools at the application boundary: Identify trusted identity separately from retrieved instructions and proposed arguments; Compare object, field and tool policy with state and useful controls; Document gateway evidence without claiming actual model attack success.

Practice inventory

Study LLM tool and data boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

LLM tool boundaries: evidence and correction

Controlled practice in the separate practice course.

Simulation

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed gateway and tool-authority model; no actual model, executable tool or paid provider.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Llm workbook

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: Fictional model/tool observations; no model provider or network calls.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

16. Resolved file containment

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Trace one decoding stage and resolved directory ancestry.

Compare parent, sibling-prefix and symlink disclosures with useful controls.

Document bounded B-CID observations and filesystem limitations.

Topics

Trace decoded paths to resolved file containment: Trace one decoding stage and resolved directory ancestry; Compare parent, sibling-prefix and symlink disclosures with useful controls; Document bounded B-CID observations and filesystem limitations.

Practice inventory

Study Resolved file containment through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Resolved file containment: evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Disposable local file containment cases; no caller-selected path, race-resistant opening or Windows validation.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Path workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Disposable filesystem; no concurrent-link race or Windows validation.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

17. File upload storage and retrieval

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish filename and declared type from actual note bytes.

Compare storage destinations and owner versus peer retrieval.

Document fresh B-CID evidence with useful controls and delivery limitations.

Topics

Separate upload validation, storage and retrieval authority: Distinguish filename and declared type from actual note bytes; Compare storage destinations and owner versus peer retrieval; Document fresh B-CID evidence with useful controls and delivery limitations.

Practice inventory

Study File upload storage and retrieval through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Upload storage and retrieval: evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed local upload/storage/retrieval fixture; no live server or arbitrary upload.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Upload http

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: In-process multipart requests; inert contents, no code execution.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Upload workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Disposable fictional storage; inert contents, no server execution.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

18. Server-side destination boundaries

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Identify the server fetch actor and separate reachability from permission.

Compare direct and redirected destination policies using fresh evidence.

Write a bounded B-CID finding with useful controls and uncertainty.

Topics

Follow the server fetch across destination boundaries: Identify the server fetch actor and separate reachability from permission; Compare direct and redirected destination policies using fresh evidence; Write a bounded B-CID finding with useful controls and uncertainty.

Practice inventory

Study Server-side destination boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

Server-side destinations: evidence and correction

Controlled practice in the separate practice course.

Simulation

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed destination-authority comparisons; no live destination, DNS or arbitrary URL.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Ssrf http

Local workbook exercise; observations are not submitted to your course notebook.

Executable fixture with simulated components

Limits: WSGI requests execute against modeled destination graph; no real DNS or remote reachability.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Ssrf workbook

Local workbook exercise; observations are not submitted to your course notebook.

Simulation

Limits: Fixed destination graph; no sockets or real DNS.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

19. XML parser entity boundaries

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish escaped text, internal replacement and external resolution.

Separate policy denial, malformed XML and unavailable resources using paired evidence.

Document fresh B-CID retests, useful controls, compatibility and limits.

Topics

Trace XML entity resolution and preserve useful parsing: Distinguish escaped text, internal replacement and external resolution; Separate policy denial, malformed XML and unavailable resources using paired evidence; Document fresh B-CID retests, useful controls, compatibility and limits.

Practice inventory

Study XML parser entity boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

XML entities: evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Real Expat parsing with memory-only fictional resolver; no real file/network resolution.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Xxe http

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Listener-free HTTP/XML receipts; no arbitrary XML or external resources.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Xxe workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Fixed owned parser fixtures; no arbitrary XML or external resource target.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

20. JWT trust and application claims

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish decoding, MAC validation and application claim rules.

Apply resource ownership after token validation.

Document and retest fixed JWT comparisons with B-CID.

Topics

Verify token origin, claims and notebook permission: Distinguish decoding, MAC validation and application claim rules; Apply resource ownership after token validation; Document and retest fixed JWT comparisons with B-CID.

Practice inventory

Study JWT trust and application claims through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

JWT trust: evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Fixed offline signed-token comparisons; no production identity or caller key.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Jwt workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Fixed fictional tokens/claims; no external identity provider or arbitrary-token tool.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

21. OAuth and OpenID Connect transaction boundaries

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish OAuth exchange, OIDC identity and resource authorization.

Test state, S256, redirect, client, reuse and identity-context boundaries with fixed receipts.

Document controlled comparisons and useful retests using B-CID.

Topics

Trace code exchange, identity and notebook permission: Distinguish OAuth exchange, OIDC identity and resource authorization; Test state, S256, redirect, client, reuse and identity-context boundaries with fixed receipts; Document controlled comparisons and useful retests using B-CID.

Practice inventory

Study OAuth and OpenID Connect transaction boundaries through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

OAuth/OIDC transaction evidence and correction

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Offline fixed WSGI transactions and cryptographic checks; no external identity provider/browser/TLS.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Oauth workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Offline transactions; no live authorization server, browser redirect or external identity account.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

22. TLS and HTTPS assessment basics

7 lessons; 8 managed practices; controlled preview

Lesson outcomes and practice

Outcomes

Distinguish trust, reference identity, negotiation and application policy.

Collect actual isolated TLS observations with useful and forbidden controls.

Document bounded TLS B-CID conclusions and unmeasured HTTPS behavior.

Trace client, edge and backend transport as separate boundaries.

Compare actual middleware behavior with explicitly supplied topology.

Retest scheme-header trust while preserving useful access.

Distinguish server redirects from browser transport policy.

Identify first-visit, cached-policy and resource evidence gaps.

Write bounded BCID findings with useful and forbidden retests.

Compare explicit local CRL verification with unchecked acceptance.

Separate expiry, name mismatch, missing CRL and observed revocation.

Document bounded BCID findings with an unrevoked positive control.

Compare signed CRL date windows at one fixed verification instant.

Distinguish stale, future, revoked and unchecked evidence.

Document a bounded BCID finding with an accepted unrevoked control.

Compare fixed offline signed OCSP responses for the same certificate.

Separate verified good, revoked, unknown and unverified good text.

Document bounded BCID evidence with honest client-policy limits.

Compare issuer and delegated signer authority using fixed offline evidence.

Separate signer purpose, response signature and reported certificate status.

Document same-run BCID comparisons and limits without browser-policy claims.

Topics

Assess TLS trust, names and negotiated protocols: Distinguish trust, reference identity, negotiation and application policy; Collect actual isolated TLS observations with useful and forbidden controls; Document bounded TLS B-CID conclusions and unmeasured HTTPS behavior.

Trace HTTPS termination and forwarded scheme trust: Trace client, edge and backend transport as separate boundaries; Compare actual middleware behavior with explicitly supplied topology; Retest scheme-header trust while preserving useful access.

Separate redirects, HSTS and mixed-content evidence: Distinguish server redirects from browser transport policy; Identify first-visit, cached-policy and resource evidence gaps; Write bounded BCID findings with useful and forbidden retests.

Distinguish revocation from missing issuer evidence: Compare explicit local CRL verification with unchecked acceptance; Separate expiry, name mismatch, missing CRL and observed revocation; Document bounded BCID findings with an unrevoked positive control.

Check whether signed revocation evidence is usable now: Compare signed CRL date windows at one fixed verification instant; Distinguish stale, future, revoked and unchecked evidence; Document a bounded BCID finding with an accepted unrevoked control.

Separate OCSP response verification from certificate status: Compare fixed offline signed OCSP responses for the same certificate; Separate verified good, revoked, unknown and unverified good text; Document bounded BCID evidence with honest client-policy limits.

Check who may sign a certificate status response: Compare issuer and delegated signer authority using fixed offline evidence; Separate signer purpose, response signature and reported certificate status; Document same-run BCID comparisons and limits without browser-policy claims.

Practice inventory

Study TLS and HTTPS assessment basics through these original lessons and evidence objectives.

Recommended preparation: BEST BCID and the preceding topics in this outline; this is guidance, not an enrollment restriction.

TLS trust, name and protocol evidence

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Socket-free TLS trust/name/protocol comparisons; temporary fixture keys, no public CA or production transport.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

TLS expiry and renewal evidence

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Socket-free certificate expiry/renewal comparisons; fixed fixture scope.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

HTTPS termination and forwarded scheme evidence

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Real in-process Werkzeug middleware; supplied transport context, no actual edge/TLS/browser.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Supplied browser-policy evidence ledger

Controlled practice in the separate practice course.

Supplied records

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Eight authored browser-policy records; no browser/transport execution, timestamps mark packet copies.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Certificate revocation evidence

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Socket-free certificate/CRL comparisons; no live revocation service.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

CRL freshness evidence

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Socket-free CRL freshness comparisons; fixed fixture scope.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Offline OCSP response evidence

Controlled practice in the separate practice course.

Executable isolated fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Offline fixed signed OCSP response comparisons; no live responder/browser/stapling.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Offline OCSP signer authority evidence

Controlled practice; saved observation records cannot be overwritten.

Executable isolated offline OpenSSL fixture

Prerequisites: BEST BCID and this module's instruction; study guidance, not an admission gate

Modes: guided, semi-guided, blind formative, retest

Limits: Four fixed offline issuer/delegate comparisons. Separates signer authority, signature verification and reported status. No network target, freshness/nonce/stapling, delegate revocation or browser enforcement; BCID receipts are formative and ungraded.

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Alternate standalone workbooks

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Https proxy

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Fixed in-process scheme comparisons; no live proxy or network transport.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Tls crl freshness

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Offline OpenSSL checks; no live distribution or actual client policy.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Tls ocsp

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Offline signed responses; no live responder or actual client policy.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Tls renewal

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Offline certificate comparisons; no deployed renewal automation.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Tls revocation

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Offline CRL checks; no live publication or client enforcement.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Tls workbook

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Offline certificate checks; no socket handshake or production trust store.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Fixed browser exercises

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

HTTPS resource-policy comparisons

Separate local exercise; observations are not saved to your course notebook.

Fixed original browser fixture / optional native harness

Limits: Five intercepted resource cases; simulated transport, no TLS handshake, certificate or HSTS proof. Testing on a real browser and host is not included.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

Versioned workbook additions

Alternate collection paths and historical activities overlap the instruction; they are not additional managed labs.

Who may sign a certificate status response?

Local workbook exercise; observations are not submitted to your course notebook.

Executable isolated fixture

Limits: Four fixed offline OpenSSL issuer/delegate/signature comparisons; no live responder, browser, stapling, freshness or delegate revocation. Requires BCID, certificate identity/trust, CRL and OCSP. Not an enrolled receipt or independent assessment.

Preparation: read BEST BCID and this module's lessons first. Local workbook exercises require their own setup guide; a syllabus listing does not launch them.

23. Integrated engagement and evidence reporting

1 lesson; 1 managed practice; controlled preview

Lesson outcomes and practice

Outcomes

Plan a bounded two-boundary engagement and separate supplied observations from learner conclusions.

Write reproducible findings, permission-check mitigations and useful retests with explicit uncertainty.

Topics

From paired observations to a useful engagement report: Plan a bounded two-boundary engagement and separate supplied observations from learner conclusions; Write reproducible findings, permission-check mitigations and useful retests with explicit uncertainty.

Practice inventory

Integrated engagement: fictional reading and invoice boundaries

Controlled practice; saved observation records cannot be overwritten and are not graded.

Executable isolated in-process HTTP reading and invoice engagement

Prerequisites: web-best-bcid-method, web-access-policy, web-idor-comparison, web-role-and-function, web-access-report-retest

Modes: guided, semi-guided, blind, retest

Limits: Supplied identities and corrections; separate contexts, not atomic; no browser or production assurance

Task: apply BEST BCID to the stated boundary, document comparisons and check useful retests within the supplied scope.

Independent assessment rehearsal: dispatch permission investigation

Ungraded assessment rehearsal. People have not yet checked whether the assessment measures skills consistently.

Distinct executed dispatch authorization, BCID and reporting sample. Not an independent exam of every topic.

Plan your comparisons, execute the fictional workbench, cite saved observation identifiers and submit one original report. No correctness feedback or automatic retake. Named reviewers assess submitted evidence separately, preserve disagreement and give actionable feedback. Assessment consistency and validation have not been established. This rehearsal does not award mastery or certification.

Use the linked HTML syllabus for structured headings and module navigation. The downloadable PDF contains the same course information and has no screen-reader document tags or interactive links. Full accessibility and learner testing are still pending.