MNA
TECH ACADEMY
LEARN • PRACTICE • SUCCEED

DETAILED STUDY NOTES · 2026 EDITION

Web Application Testing Master Study Notes

Architecture, HTTP, authentication, authorization, injection, browser security, APIs, files, server-side risks, evidence, and remediation.

18	10	40+
Detailed pages	Core domains	Review prompts

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Study web security through data flows, trust boundaries, and server-side controls. Use intentionally vulnerable training applications and approved targets only.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **HTTP & Application Architecture**
Understand clients, proxies, servers, APIs, storage, queues, and trust boundaries.

02 **Mapping the Attack Surface**
Build an endpoint and data-flow inventory before testing.

03 **Authentication Security**
Review identity proof, login, MFA, recovery, enumeration, and session creation.

04 **Session Management**
Understand cookies, tokens, rotation, expiry, revocation, and concurrent sessions.

05 **Authorization & IDOR**
Validate permissions on every object and function server-side.

06 **Injection Fundamentals**
Recognize unsafe data entering SQL, OS commands, templates, and interpreters.

07 **Cross-Site Scripting**
Differentiate reflected, stored, and DOM-based unsafe rendering.

08 **CSRF, CORS & Browser Trust**
Separate cross-site request, origin policy, and credential behavior.

09 **Files, Paths, SSRF & XXE**
Control parsers and server-side access to local or remote resources.

10 **API & JWT Security**
Review object, function, property, resource, token, and workflow controls.

11 **Concept Review Questions**
Use explanation-first questions to expose gaps before attempting a lab.

12 **Defensive Lab Exercises**
Practise with synthetic data and isolated environments.

13 **Investigation Worksheet**
Structure technical reasoning so conclusions remain auditable.

14 **Exam & Interview Revision**
Convert notes into concise explanations and practical examples.

15 **Further Study & References**
Prefer official documentation and repeatable practice over unverified shortcuts.

HTTP & Application Architecture

Understand clients, proxies, servers, APIs, storage, queues, and trust boundaries.

Purpose: Understand clients, proxies, servers, APIs, storage, queues, and trust boundaries.

Working checklist

01 · Requests
Method, path, headers, cookies, body, origin, and content type.

02 · Responses
Status, headers, caching, cookies, body, redirects, and error behavior.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Mapping the Attack Surface

Build an endpoint and data-flow inventory before testing.

Purpose: Build an endpoint and data-flow inventory before testing.

Working checklist

01 · Inventory
Pages, APIs, parameters, files, roles, integrations, and state-changing actions.

02 · Coverage
Track tested roles, objects, methods, formats, and error cases.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Authentication Security

Review identity proof, login, MFA, recovery, enumeration, and session creation.

Purpose: Review identity proof, login, MFA, recovery, enumeration, and session creation.

Working checklist

01 · Workflows
Test normal, invalid, locked, expired, and recovery states.

02 · Controls
Rate limits, MFA, secure reset, generic errors, and audit events.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Session Management

Understand cookies, tokens, rotation, expiry, revocation, and concurrent sessions.

Purpose: Understand cookies, tokens, rotation, expiry, revocation, and concurrent sessions.

Working checklist

01 · Cookie flags
Secure, HttpOnly, SameSite, domain, path, and lifetime.

02 · Lifecycle
Rotate on privilege change; invalidate on logout and risk events.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Authorization & IDOR

Validate permissions on every object and function server-side.

Purpose: Validate permissions on every object and function server-side.

Working checklist

01 · Matrix
Roles × actions × object ownership × state.

02 · Evidence
Use synthetic records and demonstrate minimum unauthorized impact.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Injection Fundamentals

Recognize unsafe data entering SQL, OS commands, templates, and interpreters.

Purpose: Recognize unsafe data entering SQL, OS commands, templates, and interpreters.

Working checklist

01 · Root cause
Dynamic construction without safe parameterization or encoding.

02 · Fix
Safe APIs, allow-lists, least privilege, and structured validation.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Cross-Site Scripting

Differentiate reflected, stored, and DOM-based unsafe rendering.

Purpose: Differentiate reflected, stored, and DOM-based unsafe rendering.

Working checklist

01 · Context
HTML, attribute, URL, JavaScript, CSS, and DOM sinks need different controls.

02 · Defense
Framework escaping, sanitization, CSP support, and safe DOM APIs.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

CSRF, CORS & Browser Trust

Separate cross-site request, origin policy, and credential behavior.

Purpose: Separate cross-site request, origin policy, and credential behavior.

Working checklist

01 · CSRF
Protect state changes with tokens, SameSite, origin checks, and re-authentication.

02 · CORS
Allow only required origins, methods, headers, and credential combinations.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Files, Paths, SSRF & XXE

Control parsers and server-side access to local or remote resources.

Purpose: Control parsers and server-side access to local or remote resources.

Working checklist

01 · Files
Validate content, store outside executable paths, rename, scan, and serve safely.

02 · Egress
Allow-list destinations, block metadata/private ranges, constrain parsers and protocols.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

API & JWT Security

Review object, function, property, resource, token, and workflow controls.

Purpose: Review object, function, property, resource, token, and workflow controls.

Working checklist

01 · API
Schema validation, authorization, pagination, rate limits, and inventory.

02 · JWT
Validate algorithm, issuer, audience, time, key selection, rotation, and revocation strategy.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Concept Review Questions

Use explanation-first questions to expose gaps before attempting a lab.

Purpose: Use explanation-first questions to expose gaps before attempting a lab.

Working checklist

01 · Explain
Describe the concept in your own words without tool names.

02 · Differentiate
Compare it with the closest related concept and common confusion.

03 · Predict
State expected behavior before observing traffic or logs.

04 · Defend
Name preventive, detective, and recovery controls.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Defensive Lab Exercises

Practise with synthetic data and isolated environments.

Purpose: Practise with synthetic data and isolated environments.

Working checklist

01 · Baseline
Capture normal behavior before introducing a controlled change.

02 · Generate
Create one safe, observable event in the lab.

03 · Detect
Locate evidence across endpoint, application, identity, and network layers.

04 · Improve
Tune a control and show the before/after result.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Investigation Worksheet

Structure technical reasoning so conclusions remain auditable.

Purpose: Structure technical reasoning so conclusions remain auditable.

Working checklist

01 · Question
Write the precise question being answered.

02 · Evidence
Record source, timestamp, timezone, integrity, and limitations.

03 · Hypotheses
List multiple plausible explanations before deciding.

04 · Conclusion
Separate facts, inferences, unknowns, and next actions.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Exam & Interview Revision

Convert notes into concise explanations and practical examples.

Purpose: Convert notes into concise explanations and practical examples.

Working checklist

01 · One-minute answer
Define the concept, risk, example, and control.

02 · Diagram
Draw the data flow or trust boundary from memory.

03 · Scenario
Explain how you would investigate a realistic event.

04 · Mistakes
List common false assumptions and how to verify them.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Further Study & References

Prefer official documentation and repeatable practice over unverified shortcuts.

Purpose: Prefer official documentation and repeatable practice over unverified shortcuts.

Working checklist

01 · Primary sources
Read vendor, standards, protocol, and project documentation.

02 · Version awareness
Record edition, product version, and publication date.

03 · Lab notes
Link each claim to evidence or a trusted reference.

04 · Learning loop
Plan the next topic from observed gaps, not social-media trends.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.