

WEB APPLICATION PENETRATION TESTING PRE-REQUISITE DOCUMENT

VAPT Engagement Onboarding Checklist

Document Attribute	Details
Document Title	Web Application VAPT — Pre-Requisite Document
Document Version	1.0
Classification	Confidential — For Client & Engagement Team Use Only
Applicable Framework	OWASP Testing Guide v4 / OWASP Top 10, PTES, CERT-In Guidelines, RBI Cyber Security Framework
Prepared For	[Client / Application Owner Name]
Prepared By	[Testing Team / Vendor Name]
Date	[DD-MM-YYYY]

Table of Contents

1. Purpose & Objective 3

2. Scope of Engagement 3

3. Access & Test Environment 4

4. Test User Accounts & Credentials 4

5. Network Access & IP Whitelisting..... 4

6. Application Documentation & Architecture 5

7. Security Control Coordination 5

8. Points of Contact & Escalation Matrix 5

9. Testing Window & Timelines 6

10. Legal Authorization & Rules of Engagement 6

11. Backup & Rollback Readiness 6

12. Reporting & Communication Protocol 6

13. Testing Methodology & Tooling Disclosure 7

14. Roles & Responsibilities 7

15. Pre-Engagement Sign-off 8

1. Purpose & Objective

This document defines the complete set of pre-requisites, access requirements, and coordination points that must be fulfilled by the Client / Application Owner prior to the commencement of Web Application Vulnerability Assessment and Penetration Testing (VAPT). Timely completion of these items ensures the assessment proceeds without delay, minimizes disruption to production systems, and enables the testing team to deliver a comprehensive, high-fidelity report within the agreed timelines.

This checklist has been designed in line with industry-recognized methodologies (OWASP Testing Guide, OWASP Top 10, PTES, SANS 25) and, where applicable, regulatory expectations under CERT-In empanelment guidelines and the RBI Cyber Security Framework for institutions in the BFSI sector.

Note: All fields marked “[To be filled]” must be completed and returned by the Client at least 3–5 working days before the scheduled test start date.

2. Scope of Engagement

2.1 Application Details

Field	Details
Application Name	[To be filled]
Application URL(s) — Production	[To be filled]
Application URL(s) — UAT / Staging (preferred for testing)	[To be filled]
Business Criticality	[Critical / High / Medium / Low]
Hosting Environment	[On-premise / Cloud — specify provider]
Public-facing / Internal	[To be filled]
Number of User Roles	[To be filled]
Testing Type	[Black-box / Grey-box / White-box]
Assessment Type	[Vulnerability Assessment + Penetration Testing]

2.2 Out-of-Scope Components

Clearly list any modules, third-party integrations, or functions to be excluded from active/intrusive testing (e.g., live payment gateway, live SMS/email gateway, production database write operations):

- [Component 1 — reason for exclusion]
- [Component 2 — reason for exclusion]
- [Component 3 — reason for exclusion]

3. Access & Test Environment

A dedicated test/UAT environment that mirrors production (same codebase, configuration, and business logic) is strongly recommended. If testing must be performed on production, this must be explicitly confirmed and documented.

Requirement	Status / Details
Test environment URL(s) confirmed and reachable	[Yes / No]
Test environment data parity with production confirmed	[Yes / No]
Environment stable for the entire testing window	[Yes / No]
Supported browsers / OS for the application	[To be filled]
Mobile-responsive / separate mobile app in scope	[Yes / No]
VPN / VDI access required to reach the environment	[Yes / No — attach access instructions]

4. Test User Accounts & Credentials

Please provide a minimum of two accounts per distinct user role (to test both horizontal and vertical privilege escalation). Credentials should be shared through a secure channel (encrypted email, password vault, or secure link) — never in plain text over chat.

User Role	Username	Password	Privilege Level	MFA Enabled
Super Admin	[To be filled]	[To be filled]	Full access	[Y/N]
Standard Admin	[To be filled]	[To be filled]	Elevated	[Y/N]
Regular User (Account A)	[To be filled]	[To be filled]	Standard	[Y/N]
Regular User (Account B)	[To be filled]	[To be filled]	Standard	[Y/N]
Guest / Unauthenticated	N/A	N/A	None	N/A
[Additional role]	[To be filled]	[To be filled]	[To be filled]	[Y/N]

Important: If MFA/OTP is enabled, please provide a mechanism for the testing team to bypass or receive OTPs during the engagement window (e.g., static OTP, whitelisted test numbers, or temporary MFA disablement for test accounts only).

5. Network Access & IP Whitelisting

To avoid false blocking of test traffic by WAF / IPS / rate-limiting controls, please whitelist the following source IP addresses for the duration of the engagement.

Item	Details
Testing Team Source IP(s)	[To be filled by testing team]
WAF / IPS whitelisting completed	[Yes / No / Not applicable]
Rate-limiting / bot-protection exception for source IPs	[Yes / No]
CDN (e.g., Cloudflare, Akamai) bypass or direct-origin access	[Yes / No — details]
Firewall ports to be opened (if applicable)	[To be filled]
Testing traffic monitoring point-of-contact (SOC/NOC)	[Name & contact]

Recommendation: Where feasible, WAF should remain enabled during the assessment to test real-world exposure, with the SOC/NOC team informed in advance to avoid raising unnecessary incident tickets.

6. Application Documentation & Architecture

The following artifacts help the testing team achieve deeper coverage and reduce time spent on reconnaissance, allowing more time for actual vulnerability discovery and exploitation:

- High-level architecture / network diagram
- Technology stack details (frontend, backend, database, frameworks, third-party libraries)
- API documentation (Swagger / OpenAPI spec, or Postman collection) — mandatory if APIs are in scope
- Data flow diagram, especially for modules handling PII / financial data
- Previous VAPT report(s) and remediation status (for re-test / regression scope)
- Business logic / user-flow walkthrough document or a short functional demo session
- List of third-party integrations (payment gateway, SMS/email gateway, identity provider, analytics, etc.)

7. Security Control Coordination

Control	Coordination Required
Web Application Firewall (WAF)	Whitelist test IPs or confirm monitored/relaxed mode during test window
Intrusion Prevention / Detection System (IPS/IDS)	Inform SOC team; whitelist source IPs to prevent auto-blocking
DDoS Protection / CDN	Confirm direct-origin access or coordinate bypass rules
Account Lockout Policy	Confirm threshold or provide unlock mechanism for brute-force test cases
CAPTCHA	Provide bypass/disable for designated test accounts, or exclude related test cases
Email / SMS Alerting on Login	Inform relevant teams to avoid false-positive fraud alerts

8. Points of Contact & Escalation Matrix

Role	Name	Contact (Email / Phone)	Availability
Business / Application Owner	[To be filled]	[To be filled]	[To be filled]
Technical POC (Dev / Infra)	[To be filled]	[To be filled]	[To be filled]
SOC / NOC Coordination	[To be filled]	[To be filled]	[To be filled]
Testing Team Lead	[To be filled]	[To be filled]	[To be filled]
Escalation Contact (Critical Findings)	[To be filled]	[To be filled]	24x7 / [specify]

9. Testing Window & Timelines

Item	Details
Proposed Start Date	[To be filled]
Proposed End Date	[To be filled]
Permitted Testing Hours	[e.g., Business hours / Off-peak 22:00–06:00 IST]
Change-freeze / Blackout Periods	[To be filled — e.g., month-end batch processing]
Load / Stress Testing Included	[Yes / No — requires separate authorization]
Re-test Window (post remediation)	[To be filled]

10. Legal Authorization & Rules of Engagement

The following must be signed off before any active testing begins:

- Signed Authorization Letter / Permission-to-Test, explicitly listing in-scope assets
- Non-Disclosure Agreement (NDA), if not already covered under the master services agreement
- Rules of Engagement (RoE) document, including permitted test types (e.g., DoS testing excluded unless explicitly authorized)
- Data handling agreement — confirmation on whether test data / PII discovered during testing can be extracted for evidence, and how it will be securely stored and disposed of post-engagement

Compliance: For regulated BFSI entities, testing authorization should also reference applicable RBI cyber security circulars and, where the assessment is being conducted for statutory/compliance purposes, confirm the empanelment status of the testing organization with CERT-In.

11. Backup & Rollback Readiness

- Full application and database backup taken immediately prior to the start of testing
- Rollback / restoration procedure validated and a named owner identified
- Confirmation that intrusive test cases (e.g., stored XSS, SQLi with data modification, file upload) are permitted, or should be limited to read-only/PoC validation

12. Reporting & Communication Protocol

Item	Details
Status Update Frequency	[Daily / Alternate day — call or email]
Critical/High Finding Escalation SLA	[e.g., within 4 hours of discovery, via email + call]
Draft Report Delivery	[X working days post testing completion]
Report Format	[PDF / Word — Executive Summary + Technical Findings + Evidence]
Report Encryption / Secure Delivery Channel	[To be filled]
Final Report Sign-off Authority	[To be filled]

13. Testing Methodology & Tooling Disclosure

Assessment will be conducted using a combination of manual testing and industry-standard tools, mapped to the OWASP Top 10, OWASP Testing Guide, and SANS Top 25 categories. Indicative toolset (subject to change):

- Burp Suite Professional / OWASP ZAP — interception & active/passive scanning
- Nmap — network and service enumeration (for exposed infrastructure, if in scope)
- Nikto, sqlmap, ffuf/gobuster — targeted vulnerability and content discovery
- Custom scripts for business-logic and authorization test cases

Source IP(s) and tool signatures will be shared in advance (see Section 5) to distinguish authorized test traffic from genuine attack traffic during SOC monitoring.

14. Roles & Responsibilities

Responsibility	Client	Testing Team
Provide test environment & credentials	✓	
Whitelist source IPs / coordinate WAF-IPS	✓	
Provide application documentation	✓	
Conduct testing per agreed scope & RoE		✓
Report critical findings within SLA		✓
Take pre-test backup	✓	
Validate & remediate findings	✓	
Support re-test post remediation		✓

15. Pre-Engagement Sign-off

By signing below, both parties confirm that the above pre-requisites have been reviewed, and the items marked “To be filled” will be furnished prior to the agreed testing start date.

	Client / Application Owner	Testing Team Lead
Name	[To be filled]	[To be filled]
Designation	[To be filled]	[To be filled]
Signature		
Date		

