RINGSAFE

VAPT Scoping Worksheet

The 10-page fill-in template we use to scope every Vulnerability Assessment & Penetration Test engagement. Prevents surprises, underscopes, and mid-test rework.

Prepared for: _____

Date: _____ Version: _____

RingSafe Cybersecurity Consulting

ringsafe.in · hello@ringsafe.in · Manish Garg — Associate CISSP, CEH, CCNP Enterprise

HOW TO USE THIS WORKSHEET

Before you engage any VAPT vendor

A bad VAPT scope is the leading cause of low-value pentest reports. This worksheet forces the conversation that should happen *before* a vendor quotes you. Fill every section. If you cannot answer a field, that is the answer — the vendor has to help you decide before test day one.

Send the completed worksheet to your shortlist of VAPT providers. A serious provider will respond with clarifying questions. If they send a quote without questions, they are sizing a generic engagement, not yours.

1. Business context

FIELD	YOUR ANSWER
Organisation legal name	
Primary business / industry	
Regulatory regime (RBI, SEBI, IRDAI, DPDP, PCI-DSS, ISO 27001, SOC 2, HIPAA, other)	
Is this test driven by a specific compliance requirement? Which clause or auditor?	
Is this a first-ever external pentest, or an annual recurring test?	
Previous test report available to current vendor? (Y/N)	
Primary decision-maker for the engagement (name, role, email)	
Technical point of contact during the test (name, role, 24x7 mobile)	

2. Scope of assets

List every asset in scope. Anything not listed is out of scope — including subdomains that may be discovered mid-test.

2.1 Web applications

#	APPLICATION NAME	PRODUCTION URL	TEST ENVIRONMENT URL	TECH STACK

1				
2				
3				
4				

2.2 APIs

#	API NAME	BASE URL	AUTH TYPE	DOC FORMAT (OPENAPI, POSTMAN, NONE)
1				
2				
3				

2.3 Mobile applications

#	APP NAME	PLATFORM	BUILD ARTIFACT (APK/IPA) AVAILABLE?	JAILBROKEN/ROOTED DEVICE TESTING ALLOWED?
1				
2				

2.4 Network / infrastructure

#	ASSET (RANGE, HOSTNAME)	TYPE (EXTERNAL, INTERNAL, DMZ)	CLOUD / ON-PREM	HOSTING PROVIDER
1				
2				
3				

2.5 Cloud tenants (AWS / Azure / GCP)

CLOUD PROVIDER	ACCOUNT / SUBSCRIPTION IDS	REGIONS	READ-ONLY AUDIT ROLE AVAILABLE?

2.6 Active Directory / identity

Number of AD forests / domains in scope	
Entra ID (Azure AD) tenant(s) in scope?	
Approx. number of user accounts	
Privileged accounts (Domain Admins, Enterprise Admins)	
SSO / federation (Okta, Azure, Google) in scope?	

3. Test objectives

Rank each objective 1–5, where 1 = critical, 5 = not relevant.

OBJECTIVE	PRIORITY (1–5)
Identify exploitable vulnerabilities that allow unauthorised data access	
Validate defensive controls (WAF, EDR, SIEM, SOC) against realistic attacker behaviour	
Satisfy a named compliance requirement (specify which)	
Test a specific threat scenario (e.g., insider, compromised third-party, ransomware)	
Benchmark developer security maturity (findings per 1,000 LOC or similar)	
Produce a board-ready risk report for funding / audit / M&A	
Identify business-logic flaws that automated scanners miss	
Assess cloud misconfiguration posture	

4. Testing methodology preferences

DIMENSION	YOUR CHOICE
Test perspective (black-box, grey-box, white-box)	
Credentials provided? If grey-box, how many user roles?	

Source code review in scope? (Y/N & languages)	
Manual testing required, or automated scan sufficient?	
Social engineering / phishing allowed?	
Physical security / on-site testing required?	
Red team / blue team / purple team engagement model?	
OWASP Top 10 coverage sufficient, or full OWASP ASVS Level 2/3?	

> **Tip.** OWASP ASVS Level 2 is the realistic target for most commercial apps. Level 3 is for systems handling regulated data (health, financial, national security). Level 1 is checkbox-only and generally not worth the engagement cost.

5. Test schedule & operational constraints

DIMENSION	YOUR ANSWER
Preferred test start date	
Hard deadline for final report	
Allowed testing hours (business hours / after hours / 24x7)	
Blackout periods (product launches, quarter-end, audits)	
Time zone of the testing team you expect	
Can production be tested, or only staging?	
DDoS and stress testing in scope? (usually excluded)	
Rate limits / API quotas that testers must respect	

6. Rules of engagement

- [ ] Tester IP addresses will be provided before test day and whitelisted in WAF / IDS.

- [ ] Destructive actions (mass delete, service disruption) require prior written approval.
- [ ] Discovered credentials must not be used to pivot outside the agreed scope.
- [ ] Personal data extracted during test will be deleted within 7 days of report delivery.
- [ ] Critical findings will be disclosed within 24 hours of discovery, not at report time.
- [ ] Any exploitation of real user accounts requires written pre-approval.
- [ ] All test traffic will be logged by both tester and client for post-test review.
- [ ] A daily status check-in (15 minutes) is scheduled for the test window.

7. Reporting requirements

Report formats required (PDF / DOCX / CSV / JIRA tickets / HTML)	
Executive summary required? (audience: board, CISO, CTO)	
Technical detail level: exploit reproduction steps required? PoC videos?	
Severity framework: CVSS v3.1, CVSS v4, OWASP Risk Rating, internal?	
Remediation retest included? (typically 1 retest within 90 days)	
Compliance attestation letter needed?	
Presentation / debrief call required? (audience, duration)	

8. Budget & contracting

Indicative budget range (internal; do not share with vendor initially)	
Contracting entity (Indian entity, parent, or subsidiary?)	
MSA already in place with any vendor? (Y/N & which)	
NDA required before scoping calls?	
GSTIN / PAN to be provided	

Preferred payment terms (e.g., 50% advance, 50% on delivery)	
Liability cap or insurance coverage expectation	

9. Vendor evaluation criteria

Score each shortlisted vendor 1–5 after the scoping call.

CRITERION	VENDOR A	VENDOR B	VENDOR C
Certifications of lead tester (OSCP, CREST, CEH, CISSP)			
Relevant industry experience (your sector)			
Sample redacted report quality			
Scoping-call depth (did they ask good questions?)			
Methodology clarity (OWASP, PTES, NIST?)			
Retest policy			
Reference calls with past clients			
Contractual terms (IP, liability, data handling)			
Quoted price / price-to-value			
Total			

10. Sign-off

ROLE	NAME	SIGNATURE / DATE
Engagement sponsor		
CISO / Security lead		
CTO / Engineering lead		
Legal / Compliance		
Vendor project manager		

Want a second opinion on your scope? Send the completed worksheet to hello@ringsafe.in or book a free 30-minute scoping call at ringsafe.in/contact. We will tell you honestly whether the engagement you have scoped will deliver what you actually need — even if the answer is "go with someone else".
