VIRTUAL CAIM

SERVICE DATASHEET AND METHODOLOGY BRIEF

VAPT and Offensive Security

How Virtual Caim plans, tests, reports and re-tests. Written for security heads, risk teams and procurement reviewers who want to see the working method, not just a list of services.

SAMPLE REPORT - fictional engagement, sanitized

SAMPLE

Service	Vulnerability assessment and penetration testing (VAPT), red teaming, application and infrastructure security testing
Credentials	CERT-In empanelled auditing organisation. ISO 27001 certified.
Typical duration	1 to 3 weeks for most scopes, plus re-test
Report format	Agreed with you before testing starts (CERT-In guidance)
Contact	audit<at>virtualcaim.com | Corporate office: Ahmedabad

The sample finding in section 7 is fictional and sanitized. It shows the reporting depth, not any real client data.

Overview

A penetration test is only as useful as the report you can act on. We put as much care into the evidence, the business impact and the fix as into the testing itself.

Manual-led
TESTING STYLE
Scanners for breadth, people for depth

Safe
EXPLOITATION
Proof of impact without damage

CVSS + EPSS
SCORING
Severity and likelihood, with CWE and CVE mapping

Re-test
CLOSURE
Verified fixes and a closure statement

1. What we test

Area	Typical coverage	Common standards used
Web applications	Authentication, session, access control, input handling, business logic, file handling, client-side security	OWASP WSTG, OWASP ASVS, OWASP Top 10
Mobile applications (Android, iOS)	Local storage, transport, binary protections, platform misuse, back-end API behaviour	OWASP MASVS and MASTG
APIs (REST, SOAP, GraphQL)	Object-level and function-level authorisation, authentication, resource limits, mass assignment, schema abuse	OWASP API Security Top 10 (2023)
Internal and external networks	Host and service discovery, misconfiguration, weak protocols, segmentation, Active Directory paths	PTES, NIST SP 800-115
Cloud (AWS, Azure, GCP)	Identity and access, storage exposure, network paths, secrets, logging and guardrails	CIS Benchmarks, cloud provider security guidance
Wireless, IoT and OT	Encryption and authentication, device interfaces, protocol handling, safe passive assessment for OT	Vendor and sector guidance, IEC 62443 concepts
Red team and social engineering	Objective-based adversary simulation, phishing exercises, physical and process tests (rules agreed in writing)	MITRE ATT&CK for planning and reporting
Secure code review (optional)	Targeted review of authentication, authorisation, crypto and data-handling code paths	OWASP Code Review Guide, ASVS

Test depth options

Mode	What you share	Best for
Black box	Only the target name or address	Seeing what an outsider can find
Grey box	Test accounts for each role, documentation, API specifications	Most application assessments: efficient, high coverage
White box	Architecture, configuration, optionally source code	High-assurance systems and pre-release reviews

2. Methodology

Four phases, aligned with the Penetration Testing Execution Standard (PTES) and NIST SP 800-115, with the OWASP Web Security Testing Guide giving the checklist for web and API work.

1
RECONNAISSANCE
Map the attack surface, roles, trust boundaries and technology stack.

2
DISCOVERY
Manual testing by category, supported by tools for breadth.

3
EXPLOITATION AND POST-EXPLOITATION
Prove realistic impact safely. Chain findings. No destructive actions.

4
REPORTING
Rate, write, walk through, agree closure dates, plan re-test.

Phase	Activities	What you receive
Reconnaissance	Asset and route inventory, role matrix, API specification review, technology fingerprinting, threat modelling notes	Agreed test plan and asset list
Discovery	OWASP WSTG categories: information gathering, configuration, identity, authentication, authorisation, session, input validation, error handling, cryptography, business logic, client side, API	Immediate notice of Critical and High findings as found
Exploitation and post-exploitation	Confirm findings with safe proof. Assess reach: what data, which roles, what chain. Pivot analysis within agreed limits	Validated findings with evidence
Reporting and walkthrough	CVSS v3.1, EPSS, CWE and CVE mapping, business impact, practical fixes, roadmap	Final report, evidence annex, walkthrough call

Principles we hold to

- **Validated, not just detected.** Scanner output is never reported without manual confirmation.
- **Safe by design.** No denial-of-service, no destructive payloads, test data wherever possible, agreed stop conditions.
- **Respect for your data.** Evidence is stored encrypted, shared only with your named Point of Contact and disposed of on the agreed date.
- **Plain reporting.** Every finding says what it is, why it matters to the business, and what to change.

> **WHERE WE DIFFER FROM A SCAN-AND-REPORT VENDOR**
> Most serious application flaws (broken access control, flawed authentication flows, business logic abuse) are not found by scanners. They are found by testers who understand the way your product is meant to work.

SAMPLE

3. Engagement lifecycle

Stage	Typical timing	What happens	What we need from you
Scoping call	Day 0	Understand systems, user roles, environments, regulatory drivers, timelines	Asset list, environment details, previous reports if any
Proposal and plan	Day 1 to 3	Fixed-scope quote, test plan, tool list, rules of engagement, report format	Written approval, Point of Contact, NDA
Kick-off	Before testing	Confirm windows, source IPs, test accounts, escalation numbers	Test accounts per role, access paths, build version and hash
Testing	1 to 3 weeks	Phases 1 to 3, interim notice of serious findings	Access to a technical contact for questions
Reporting	3 to 5 working days	Draft report, factual review, final report, walkthrough	Factual review within the agreed window
Re-test	After your fixes	Targeted verification, closure report	Fix notification with build details

Indicative effort by scope

Scope	Typical effort	Notes
Single web application, grey box	5 to 10 person-days	Depends on roles, features and depth
Mobile app plus API	8 to 15 person-days	Both platforms add time
External network, up to 30 live hosts	3 to 6 person-days	Plus follow-up on verified exposures
Internal network and Active Directory	8 to 15 person-days	Needs on-site or VPN access
Red team engagement	4 to 8 weeks elapsed	Objective based, defined rules

Figures are indicative planning ranges, not quotes. A fixed-scope quote follows a short consultation.

Test environment guidance

- We state the environment tested (test, UAT, staging or production) in every report and certificate.
- Where a staging stack is tested instead of production, the report says so clearly.
- The build version and hash of the assessed application are recorded so that the exact release can be traced.

SAMPLE

4. Deliverables

Deliverable	Audience	Contents
Executive summary	Board, CEO, CISO	Risk posture in business terms, headline risks, what works well, where to start
Technical report	Engineering, security team	Scope and assumptions, methodology, findings table, detailed findings, risk matrix, roadmap
Evidence annex (confidential)	Named Point of Contact	Redacted requests and responses, screenshots, scan outputs, reproduction notes
Compliance mapping annex	GRC, audit, regulator-facing teams	Findings mapped to CERT-In Directions, ISO 27001:2022 controls, RBI and other expectations
Walkthrough session	All stakeholders	Live explanation of findings, Q and A, agreement of closure dates
Closure report and statement	Management, auditors	Verified status of each finding with tested build hash, signed by Lead Auditor and Head of the auditing organisation

Anatomy of the technical report

Section	What it answers
Document control	Which version, which build, which environment, who has seen it
Executive summary	Are we safe enough to go live? What do we fix first?
Scope and rules of engagement	What was tested, when, how, and what was not
Methodology	How the testing was done and how findings are scored
Findings summary	One table of every finding with CVSS, EPSS, CWE and status
Detailed findings	Description, affected assets, sanitized evidence, business impact, remediation, references
Risk matrix and roadmap	Order of work, owners, effort and dependencies
Re-test policy	How and when closure is verified
Annexes	Compliance mapping, test coverage, evidence register, glossary, sign-off

REPORT INTEGRITY

Reports are signed by the auditors who did the work, reviewed and signed by an independent reviewer who is not part of the test team, and authorised by the head of the auditing organisation. They are delivered from an official mailbox through a password-protected or encrypted channel to your Point of Contact.

5. Severity model, re-test and closure

Each finding carries a CVSS v3.1 base score and vector, an EPSS likelihood of exploitation where available, and a CWE identifier. Where a CVE exists, it is quoted. Business context can change the order of remediation, but never the score.

Severity	CVSS v3.1	Meaning	Proposed closure target
Critical	9.0 to 10.0	Direct compromise or mass data exposure with little effort	7 days
High	7.0 to 8.9	Serious weakness with a realistic path to harm	15 days
Medium	4.0 to 6.9	Needs conditions or chaining	30 days
Low	0.1 to 3.9	Hardening or limited impact	90 days
Informational	0.0	No direct exploitable impact	Next planned release

Closure targets are proposals for planning; your policy and regulator decide the binding timelines.

Re-test and closure

1. You tell us which findings are fixed, with the build version and hash.
2. We re-test each fix and closely related routes, typically within 5 working days of the request.
3. Each finding is marked Closed, Partially closed or Open, with the evidence.
4. A closure report is issued. If only staging was re-tested, the report states that production was not tested.
5. Re-test rounds included in the fee are written into the proposal.

VALIDITY OF A REPORT

A report describes security at the time of testing. A significant change to code, infrastructure or configuration calls for a new or delta test. Frequency is set by your board-approved policy and your regulator.

6. Regulatory alignment

Our reports are structured so that they can be used as evidence for common expectations. Please confirm applicability and periodicity for your own regulatory category.

Framework	Where a VAPT report helps
CERT-In (IT Act section 70B, Directions of 28 April 2022, and the 2025 audit policy guidelines)	Reports follow CERT-In auditor guidance: agreed format, named scope and environment, CVSS with EPSS, CWE and CVE mapping, closure timelines by severity, signed by declared personnel, secure delivery. Critical and High findings are notified during the audit, not only at the end.
RBI (IT governance, risk, controls and assurance practices)	Evidence of periodic independent technical assurance for regulated entities, with findings suitable for the IT risk register
SEBI (Cybersecurity and Cyber Resilience Framework)	Evidence of vulnerability and penetration testing for regulated entities, subject to the entity category
PCI DSS v4.0, requirement 11.4	Penetration testing at least every 12 months and after significant change, internal and external
ISO/IEC 27001:2022	Evidence for A.8.8 (technical vulnerabilities) and A.8.29 (security testing in development and acceptance)
DPDP Act, 2023	Supports the Data Fiduciary duty to take reasonable security safeguards (section 8(5))

7. Sample finding excerpt

Fictional engagement, sanitized. One finding from the full sample report, shown as it appears to the client.

ID / title	F-02 Broken object-level authorisation on the loan statement API
Severity / score	High 7.1 `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N`
CWE / OWASP	CWE-639 | API1:2023 Broken Object Level Authorization | WSTG-ATHZ-04
Affected asset	Mobile API: /api/v2/loans/{id}/statements (fictional)
Closure target	15 days

Description

The statement endpoint confirms that the caller is logged in but does not confirm that the loan belongs to the caller. A logged-in customer can request statements of other customers by changing the loan identifier, which is sequential.

Evidence (sanitized)

```
Caller  : test customer A (session token [REDACTED])
Request : GET /api/v2/loans/[loan ID of test customer B]/statements/2026-08
Result  : HTTP 200, statement for test customer B returned
Control : same request without session token returned HTTP 401
```

Only accounts created for the engagement were used. Identifiers are fictional.

Business impact

Any registered customer can read other customers' loan statements and personal details. At the scale of a retail lending book this is a reportable personal data breach scenario and a direct regulatory concern.

Remediation

1. Derive the customer from the session and compare to the loan owner on the server before returning data.
2. Use non-guessable identifiers as defence in depth.
3. Centralise authorisation so that new endpoints inherit it by default, and add two-user tests to CI.

Findings summary table (excerpt)

ID	Finding	CVSS	Severity	Status
F-01	Predictable password-reset token	9.1	Critical	Open
F-02	Broken object-level authorisation	7.1	High	Open
F-06	Outdated JavaScript library	6.1	Medium	Open
F-08	Verbose error messages	3.7	Low	Open

8. Working with us

Question	Answer
Will testing disturb our systems?	We test in agreed windows, from declared source addresses, with stop conditions. Destructive or denial-of-service tests are excluded unless you ask for them in writing.
Can you test production?	Yes, with prior agreement. We recommend UAT for intrusive tests and non-intrusive checks on production.
How is the report delivered?	From an official Virtual Caim mailbox to your named Point of Contact, encrypted or password protected, password sent separately.
What if a fix does not work?	The re-test shows it as Partially closed or Open, with the reason. Re-test rounds in the fee are written into the proposal.
Can the report be used for regulators and auditors?	Yes. The format is agreed with you before testing, and the compliance annex maps findings to common requirements.

Question	Answer
Do you share our data with anyone?	Audit reports and metadata are shared with CERT-In only where CERT-In guidance requires it, and we tell you before the assignment starts.

NEXT STEP

Tell us your scope, systems and timelines. We reply with a fixed-scope quote and a test plan. Email **audit<at>virtualcaim.com**. Virtual Caim Private Limited, Corporate Office, Ahmedabad.

Sample datasheet. All sample findings are fictional. Standards named here belong to their respective owners (OWASP, FIRST, NIST, MITRE, PCI SSC, ISO/IEC).

SAMPLE