



JOE BLACK
SECURITY
BLACK IS THE NEW RED

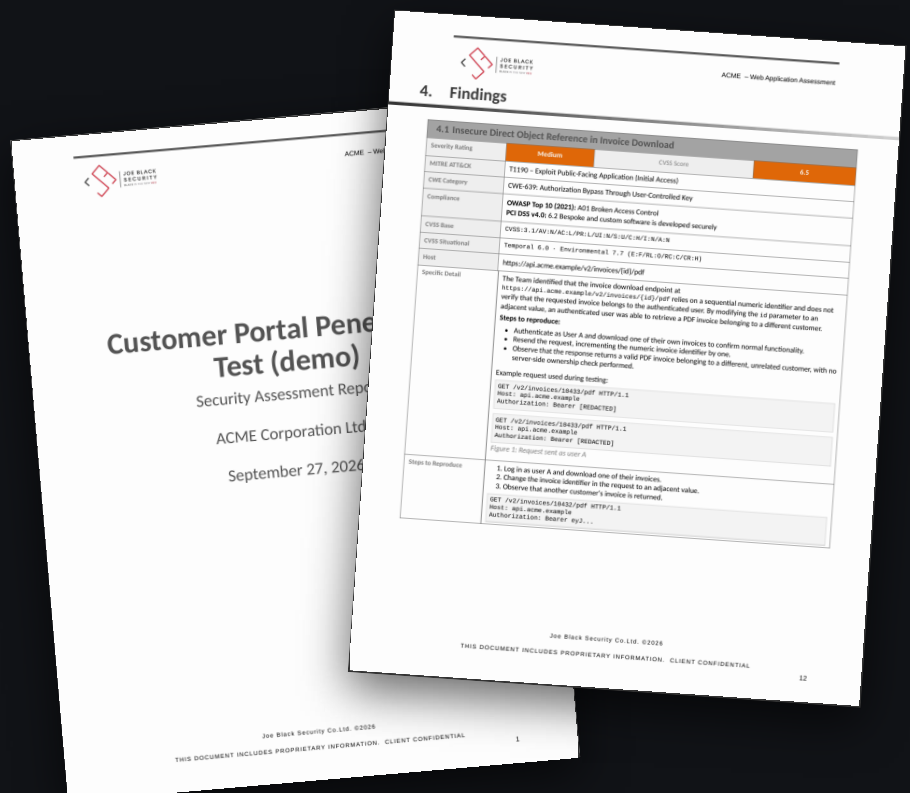


PRODUCT BROCHURE

ClearView Report Ledger

From scope sign-off to verified retest.
Penetration test reports you can stand
behind, reviewed by people, and findings that
get fixed.

Joe Black Security Co.Ltd.
joe.black · i.am@joe.black



THE PLATFORM

One workspace for the whole engagement

ClearView Report Ledger manages clients, engagements, findings and evidence, and produces branded, digitally signed PDF reports. Your clients get a secure portal to read, comment, approve and track remediation. Every report goes through a human review before it reaches a client.

Built-in

peer review
workflow

7

compliance
frameworks

4

scanner
importers

CVSS 3.1

plus risk
heatmap

PADES

signed
PDFs

HOW AN ENGAGEMENT FLOWS

1

Scope & RoE

Client reviews
and signs; you
countersign.

2

Test & capture

Evidence and
scan results flow
in.

3

Write & review

Testers write; a
second person
approves.

4

Issue

Signed PDF
published to the
portal.

5

Fix & retest

Client tracks, you
verify.

THE DELIVERABLE

Reports clients actually read

Executive summary with strengths and weaknesses, a findings summary by severity, and a page per finding with detail, impact, recommendation and the evidence placed exactly where the text refers to it.

- Likelihood × impact heatmap and optional charts: findings by category, most affected hosts, ATT&CK coverage, retest progress
- Your brand: logo, colours, methodology, footer; white-label for partners
- Retest reports with remediation status per finding
- Import your existing Word reports as drafts

Assessment Overview	Critical	High	Medium	Low	Info	Total
Web Application Assessment	0	0	3	1	1	5

3.1 Summary of Findings

Strengths

- The application manages sessions very well
- Web application firewall adequately prevents most scanning
- Service exposure is limited
- SSL is correctly configured for all in-scope hosts

Weaknesses

Insecure Configuration

Description: Insecure configuration can lead to sensitive information being disclosed or services being exposed to attack.

Solution: Modify the current configuration files to ensure they adhere to good practice principles, and conduct regular configuration reviews to ensure that current variables are up-to-date with the latest industry good security practice guidelines.

Protection Mechanism Failure

Description: No controls were implemented to prevent the application being embedded in third-party websites.

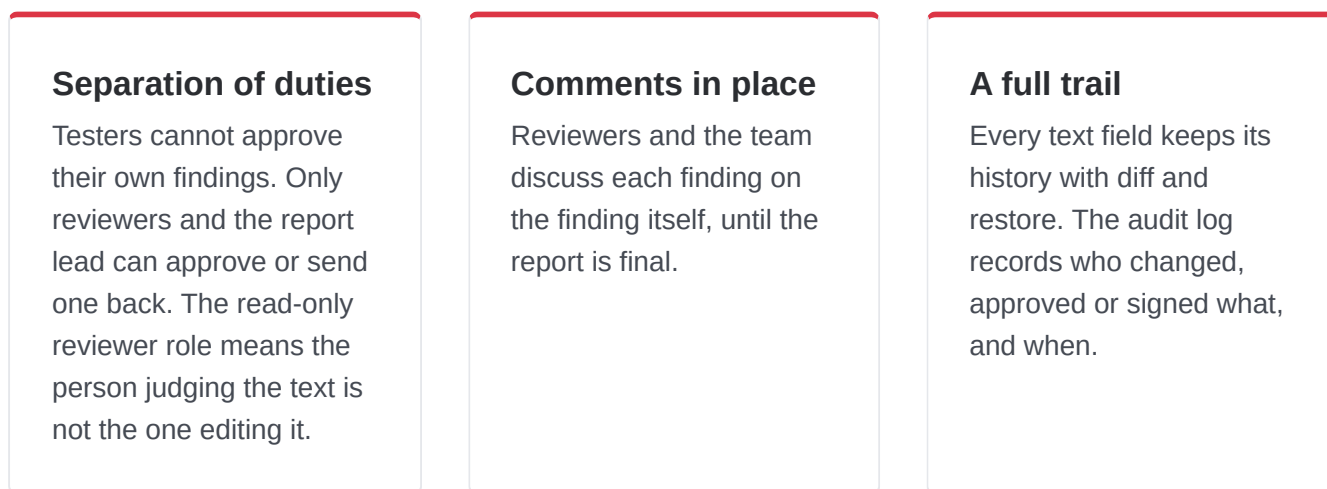
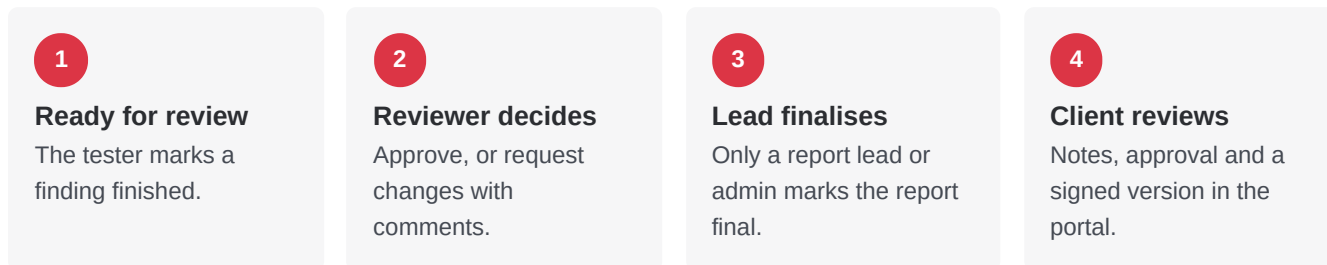
Solution: Modify the application to prevent it being included in external frames, by following the recommendations included in this report.

JOE BLACK SECURITY Co. Ltd. ©2020
THIS DOCUMENT INCLUDES PROPRIETARY INFORMATION. CLIENT CONFIDENTIAL

Findings summary page (demo data)

Human review, every time

Review is part of the workflow, whether a finding was written by hand, imported from a scanner or drafted with a suggestion. Nothing is issued on a tool's say-so.



FINDING REVIEW STATES	
Draft	The tester is still writing or editing.
Ready for review	The tester hands it over; it is waiting for a reviewer.
Changes requested	The reviewer sent it back with comments for the tester to address.
Approved	A reviewer or the report lead has signed it off.

Optional AI assistant. A supporting tool, never the author. Testers can ask for a suggested wording, CWE or summary; a person accepts, edits or discards it, and it goes through the same review as everything else. It can be disabled per client, run on local or cloud models, and every request is logged.

SEE IT IN ACTION: THE TEAM SIDE

Review, feedback and delivery in one place

Real screens from the platform, shown with demo data.

The screenshot shows the 'Session Cookie Without 'Secure' Attribute' finding in the ClearView Report Ledger. The interface includes a sidebar with navigation options like Dashboard, Reports, Finding library, Brands, and Settings. The main content area displays the finding details, including a title, a description, and a scoring section (CVSS 3.1). The scoring section includes fields for Attack vector, Attack complexity, Privileges required, User interaction, Scope, Confidentiality, Integrity, Availability, and Severity. The finding is classified as 'MEDIUM' with a CVSS score of 4.3. The right sidebar shows the 'Remediation status' as 'Open', a 'Review' section with 'Mark ready for review' and 'Approve' buttons, and a 'Checklist item' section with a 'Resolve' button. The bottom section shows 'Evidence' and 'Classification'.

BUILT-IN PEER REVIEW

A second pair of eyes on every finding

- Mark ready for review, approve, or request changes with a comment
- Testers cannot approve their own findings
- Comments stay on the finding until the report is final

The screenshot shows the 'All client notes are answered' finding in the ClearView Report Ledger. The interface includes a sidebar with navigation options like Dashboard, Reports, Finding library, Brands, and Settings. The main content area displays the finding details, including a title, a description, and a scoring section (CVSS 3.1). The finding is classified as 'MEDIUM' with a CVSS score of 4.3. The right sidebar shows the 'Remediation status' as 'Open', a 'Review' section with 'Mark ready for review' and 'Approve' buttons, and a 'Checklist item' section with a 'Resolve' button. The bottom section shows 'Evidence' and 'Classification'.

CLIENT FEEDBACK

Client change requests, answered and tracked

- The client highlights text on the issued PDF and adds a note
- Your team accepts, marks changes made, or rejects with a reason
- Issue the next version once every note is answered

The screenshot shows the 'Preview & versions' section for the 'Customer Portal Penetration Test (demo)' finding in the ClearView Report Ledger. The interface includes a sidebar with navigation options like Dashboard, Reports, Finding library, Brands, and Settings. The main content area displays the finding details, including a title, a description, and a scoring section (CVSS 3.1). The finding is classified as 'MEDIUM' with a CVSS score of 4.3. The right sidebar shows the 'Remediation status' as 'Open', a 'Review' section with 'Mark ready for review' and 'Approve' buttons, and a 'Checklist item' section with a 'Resolve' button. The bottom section shows 'Evidence' and 'Classification'.

VERSIONS

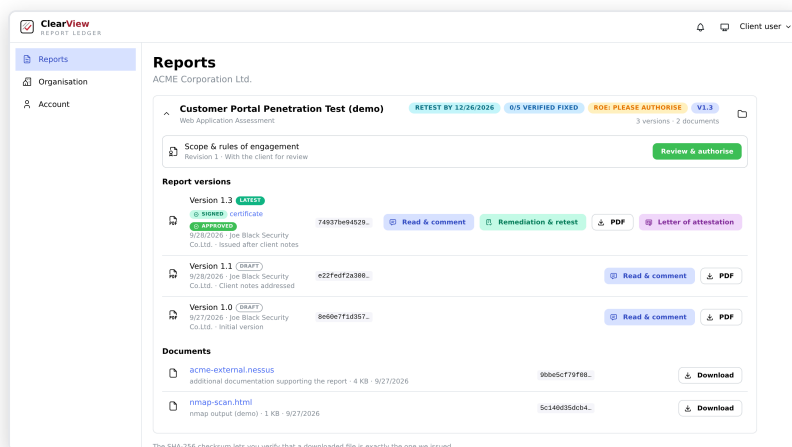
Every version kept, signed and verifiable

- Each issued PDF is kept with a checksum and digital signature
- Switch a version between Draft and Final without changing its content
- Publish to the client portal with one switch

SEE IT IN ACTION: THE CLIENT SIDE

What your clients see

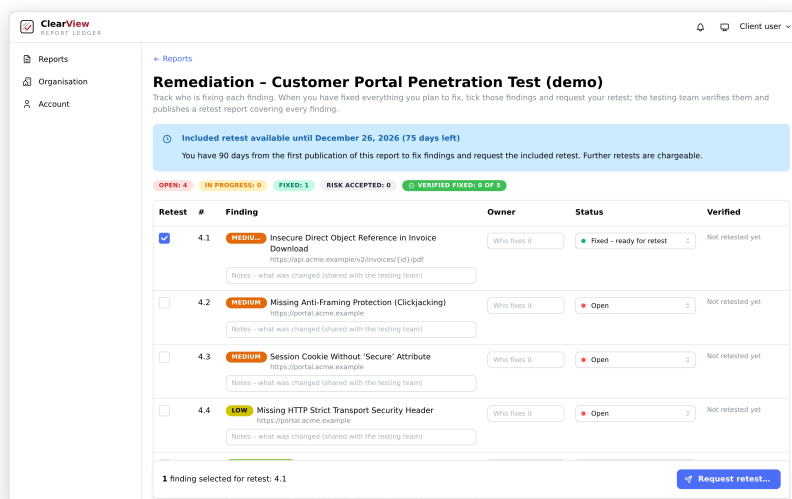
Real screens from the platform, shown with demo data.



CLIENT PORTAL

One home for everything the client needs

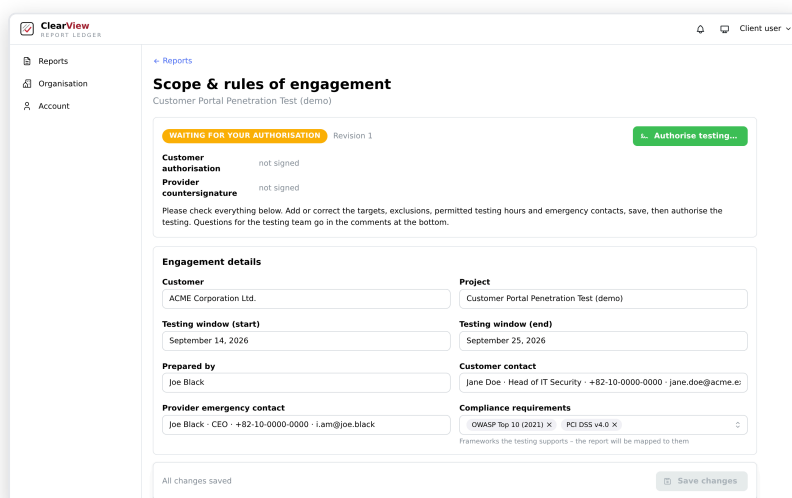
- Every version, newest first, plus the documents you share
- Signed versions with a downloadable certificate
- Status badges: retest deadline, verified fixes, scope sign-off



REMEDIATION AND RETESTS

Fixes tracked, retests on agreed terms

- Owner, status and notes for every finding
- A visible retest window and included retests
- Verified results flow back into the tracker



SCOPE AND RULES OF ENGAGEMENT

Agreed and signed before testing starts

- Targets, hours, deconfliction and emergency contacts
- The client edits their part and authorises; you countersign
- The signed PDF is the authorisation record

Built for the way testers work

Capture proof as you test, import what your scanners found, and keep every finding in the same shape.

Evidence capture

Proof goes in as you test.

- Browser extension (Firefox, Chrome): snip an area or window, with URL and time strip
- Annotate: black out, box, underline, crop
- CLI and Burp extension; an evidence bucket for items without a finding yet

Scan importers

Nessus, Nmap, Burp and OpenVAS. Parse, review, and choose what to import.

Duplicates are detected and findings map to your library by scanner id.

Structured findings

CVSS 3.1, CWE and ATT&CK references, likelihood × impact, and a reusable library, so every report reads consistently.

Compliance mapping

Enable per report only what the client needs. Appendix C lists every control.

OWASP Top 10

OWASP API

ASVS

PCI DSS 4.0

ISO 27001

NIST 800-53

CIS v8

Finding library

Reusable finding templates keep their text, CWE and compliance mappings; new findings inherit them.

Team workflow

Leads, testers and reviewers per report, client folders, private team notes, and a full activity trail per report.

A client portal, not an email attachment

Each client organisation signs in and sees only its own published reports. They are guided, kept informed, and never left to chase.

Read and comment in place

Reports open in the browser. Highlight text, add a note, and it is tied to that page and quote of that exact version. Testers accept, resolve or reject with a reason; the client is notified.

Remediation tracking

Owner, due date, status and notes per finding: Open, In progress, Fixed - ready for retest, Risk accepted.

Retests, with terms

A retest window (30, 60, 90 days or custom) and the number of included retests are set per report. Requests within terms are included; extras are clearly marked chargeable. Verified results flow back to the tracker.

Approval and attestation

Clients approve the final version once their notes are answered, then generate a letter of attestation for customers or auditors: scope, counts, verified fixes, never the finding details.

Scope & rules of engagement

Targets, exclusions, testing hours, deconfliction and emergency contacts are agreed and e-signed before testing starts. The signed PDF is the authorisation record.

Ask the Report

Optional: where the client's AI policy allows, they can ask questions about the version they are reading.

EVERYTHING THE CLIENT SEES IS CONTROLLED

Versions

Every published version in one folder, newest first, with a Draft / Final switch. Drafts carry a DRAFT watermark.

Shared files

Supporting documents you choose to share, available once a version is published.

Organisation page

Clients upload their logo and keep their contacts current; changes flow into reports still being written.

Notifications

In-app bell, plus optional e-mail. E-mails carry only a title and a link; report content is never e-mailed.

Built for security people, by security people

A reporting platform holds your clients' most sensitive findings. It is designed accordingly.

Security baseline

- Self-hosted: data stays on your infrastructure
- Optional two-factor login, login rate limiting
- Secure, HttpOnly cookies and CSRF protection on every write
- Private files served only through authorised requests
- Render workers have no internet access

Proof and traceability

- Issued versions, letters and signed RoE are digitally signed (PAdES) with your brand's certificate and a trusted timestamp
- Tampering is visible in any PDF reader
- Audit log of changes, downloads, sign-ins, approvals and signatures, with CSV export and configurable retention

Operations

- Docker Compose stack: web, worker, tasks, database, nginx with TLS
- Encrypted backups with verify and restore
- Archive and purge with a purge log
- Dependency lock and audit

White label

- Multiple brands in one installation
- Per-brand logo, methodology, footer and signing certificate
- Letters signed by the brand's signatory

See it on your own engagement

We will walk you through a live report: imported scan, AI-drafted finding, signed PDF and the client portal.

Joe Black Security Co.Ltd. · joe.black · i.am@joe.black

Report pages shown are generated from demo data. Features described reflect the current release.