5. Security Assessments

Security Assessments or Penetration testing is the practice of simulating attacks on a system or application to uncover security weaknesses:

1. **Black Box**: The tester has no prior knowledge of the system.
2. **White Box**: The tester has detailed knowledge of the system.
3. **Gray Box**: Some knowledge is provided, but not full.

Use Cases

1. **Black Box Testing:** External testers find a login vulnerability. The team patches the issue and retests for confirmation.
2. **White Box Testing:** Full system knowledge reveals code injection risks. Developers implement code fixes and resolve the report.
3. **Gray Box Testing:** Limited access tests expose endpoint vulnerabilities. Engineers secure the endpoints and log retesting results.
4. **Retesting After Fixes:** Vulnerabilities are fixed post-penetration test. Follow-up tests are conducted to ensure no further risks remain.

> Pen testers document discovered vulnerabilities and exploitation paths. In the system, you'd log each test (or each portion of a test) as a Penetration Report, noting the Name and any steps or results in the Description. Security teams typically use it to confirm that known vulnerabilities are patched and no new ones have appeared.

Table View

1. **Total:** (top-left) shows how many penetration reports exist.
2. **Search…** quickly filters by any term in the **Name** or **Description**.
3. **+ Add** (top-right) opens the "Add penetration report" form.

Column	Details
Name ⇅	Title of the test (e.g. "Denial of Service," "Open Redirect"). Clicking the link opens full details.
Description	One-line summary of what was tested or discovered.
File	Uploaded assessment file (e.g. penetration test report or supporting document), downloadable directly from the table.

Column	Details
Project	Link to the related project or environment.
Created at ⇅	Date and time when the report was logged.
Actions	✏ Edit

There’s no built-in delete option for penetration reports—entries are archived by editing or by policy.

> **Penetration Reports – Clickable Name**
> In the Table view for Penetration Reports, the **Name** column entries are clickable. Clicking any Name opens the full-width **View Penetration Report** drawer, showing that report’s Name, Description, Created at timestamp.

Viewing Linked Violation Reports

You can now see which Violation Reports were raised as a result of each penetration test—right in the Penetration Reports table.

Expand the row: In the leftmost column of any report row, click the ▼ arrow.

Review associated violations: A sub-row appears listing each Violation Report linked to that Pen test (with Title, Status, and Date).
Click a Violation Report title to open its detail panel.

No linked violations? You’ll see “No data to display” if no Violation Reports are attached yet.

Adding a Penetration Report

1. Click **+ Add**.
2. In **Add penetration report**:
-Name: Enter a clear title for the engagement.
-Description: Summarize the scope and key findings.
-Project: Select the associated project.
-Attached files: Drag an image or browse to upload one or more PDF documents (e.g. your full pen-test report).
3. Click **Save**. Your new report appears in the table.

Editing a Penetration Report

Click the ✏ icon under **Actions**.
In the **Edit penetration report** panel, update the **Name**, **Description**, or **Project**.
Attached files: Drag an image or browse to upload additional PDFs or replace existing attachments.
Click **Save** to apply changes.

Typical Workflow

Pen Test Execution: Security team or external vendor runs tests (e.g., vulnerability scans, manual exploitation, stress tests).
Report Logging: Each test campaign is logged with a **Name** and **Description** of findings (e.g., “SQL injection found in search endpoint”).
Review & Action: Security engineers review findings, tag them to development/ops teams, and track fixes.

Once remediated, tests may be rerun and the report updated to reflect the final status.

Revision #17
Created 27 February 2025 09:23:34
Updated 27 January 2026 12:06:03