Sample evidence pack

One fix, from the finding to the merge

This sample shows the shape of the evidence pack an auditor gets for each assessment. It is built from the illustrative fix shown on the AUTOSP page. The service, the finding and the fingerprints are examples, not from a real customer.

To confirm: the final layout and contents of the pack.

The finding

Weakness	CWE-89, SQL injection
Where	app/repositories/invoices.py
Reported by	Your existing scanner

Reproduced

Before anything was changed, AUTOSP wrote a test that fails while the weakness is there: test_invoice_id_cannot_change_the_query. It failed on the code as it was.

Patched in a sealed sandbox

The smallest fix was written inside a throwaway container with no internet, a read-only file system and hard time limits. The container was gone when the job ended.

Sandbox	sbx-7f3a
Change	1 line removed, 1 added

Verified before merge

The fix had to pass all three checks before a pull request was opened:

Passed: The reproduction test now passes

Passed: Your existing test suite still passes

Passed: A fresh static scan comes back clear

A person merges

AUTOSP opened a pull request with this evidence and stopped there. Your reviewers approve and merge under your own branch protection, which the GitHub App can't change or bypass.

The record

Every step was written to an append-only log. Each entry carries the fingerprint of the one before it, so editing any entry breaks every fingerprint after it.

1. **Reported: CWE-89 in app/repositories/invoices.py**
   `d84ab5e4ca8fe5840de48f4f74ed3ceccb311abeb18949aebdb8e41eb1f4ac11`

2. **Reproduced: test_invoice_id_cannot_change_the_query failed**
   `fead3b3a5eced2cd326382e3800b5b8fc1ece4d5ac7d9b64e93eeab444d823f0`

3. **Patched in sandbox sbx-7f3a: 1 line removed, 1 added**
   `9e267cd2a625451e62887a4ecadd1dfd755d72774268f02d5df8ad05244a1765`

4. **Verified: all three gates passed**
   `c16297b38bb8adb8402e32409b9fd46bc03caeafcea9cf734a4a6f17a1b4e59f`

5. **Waiting for a person to merge**
   `written when a person merges`