DVWA — SQL Injection (low)

Security Micro-Scan

Client: DVWA Lab
Date: 2025-09-26
Author: Braxton Beck (Ben-Frank17)
Severity: High — SQL injection permits database data disclosure and authentication bypass.

Summary

The DVWA SQL Injection module accepts unsanitized input and interpolates it into SQL queries. An attacker can inject boolean or union payloads to retrieve database rows.

PoC

Payload: `1' OR '1'='1`
Steps

1. Login to DVWA (`admin` / `password`) and set Security = **low**.
2. Navigate to **Vulnerabilities** → **SQL Injection**.
3. Enter payload in the User ID field and click **Submit**.
4. Multiple user rows are returned indicating successful injection.

Evidence

- Screenshot: `dvwa_sqli.png`

Impact

An attacker can read sensitive database contents, bypass authentication, and potentially modify data depending on DB privileges.

Remediation

- Use parameterized queries / prepared statements.
- Enforce strict input validation and type checks.
- Limit DB account privileges and enable query logging.

Retest

Verify parameterized queries block the payload and that results no longer expose database rows.