WordPress REST API SQL Injection Assessment

Plugin risk assessment and database protection

Overview

Assessed a deliberately vulnerable WordPress deployment and confirmed that an unauthenticated REST API parameter could influence database queries. The case study focuses on validation, risk, and remediation rather than exploitation details.

Approach

- Identified the WordPress application and relevant plugin surface.
- Used controlled comparison tests to validate unsafe query construction.
- Mapped the potential path from data exposure to account compromise.

Key findings

- An API parameter was not safely constrained before reaching a database query.
- The flaw could expose application data and authentication material.

Defensive recommendations

- Update or remove vulnerable components.
- Use parameterized queries, allowlisted API fields, strong passwords, and request monitoring.

Publication note: This is a sanitized portfolio summary. All testing was performed in intentionally vulnerable, isolated training environments. Target identifiers, credentials, payloads, screenshots, and step-by-step exploitation instructions have been omitted.