New issue

Jump to bottom

SQL injection Vulnerability on "heading_field_id" in rukovoditel 3.2.1 #16

Open **anhdq201** opened this issue on Nov 2 · 1 comment

anhdq201 commented on Nov 2 Owner

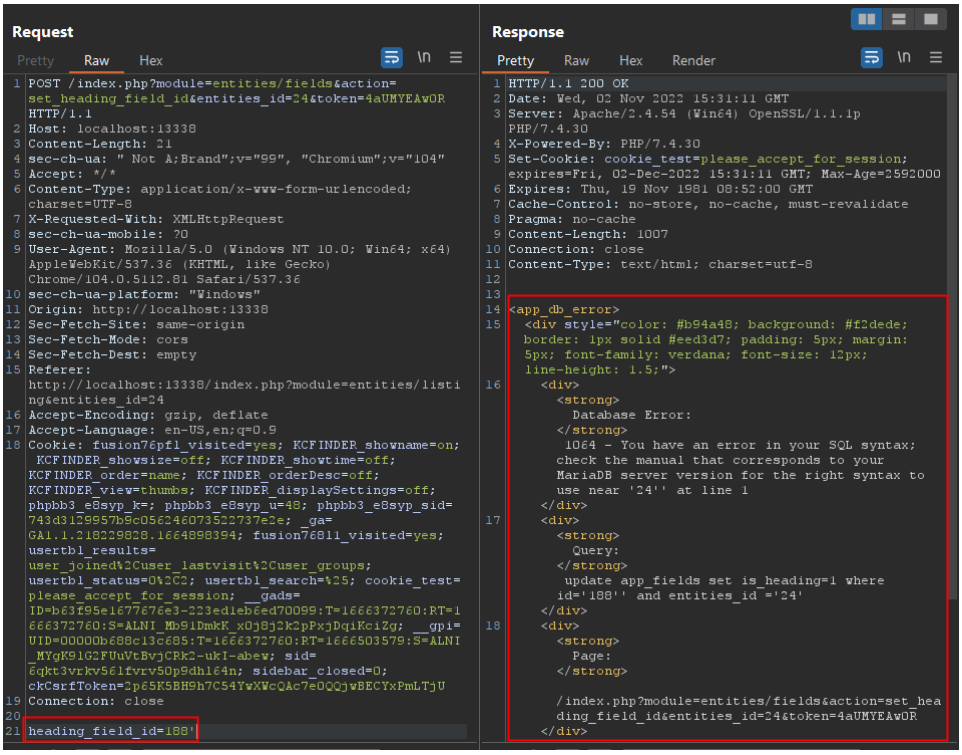
Version: 3.2.1

Description

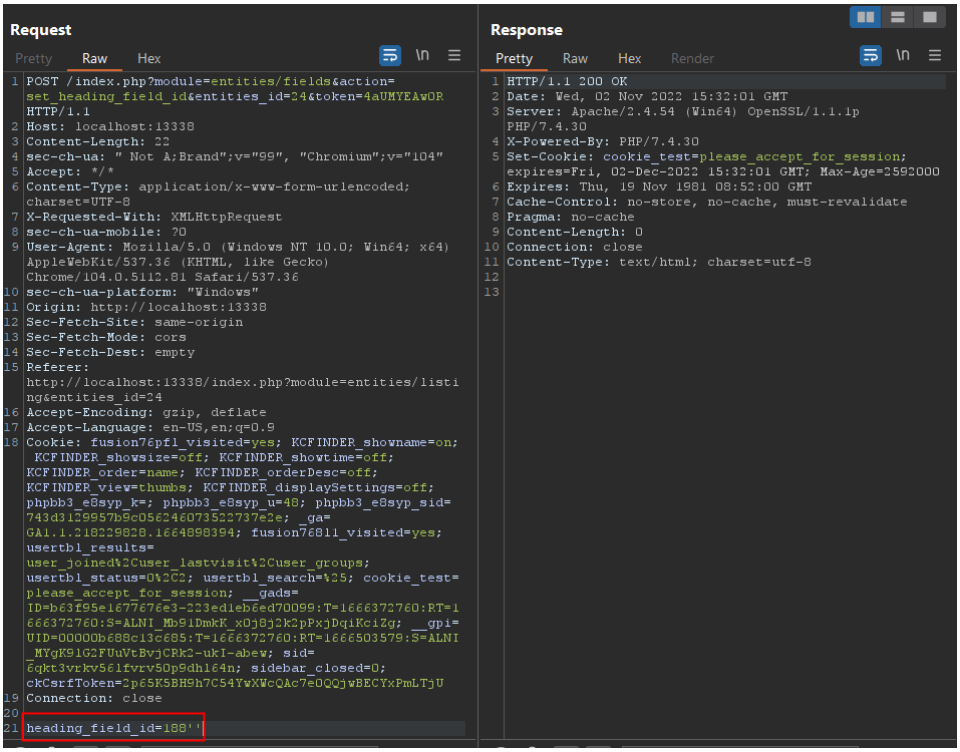
The heading_field_id parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the heading_field_id parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared.

Proof of Concept

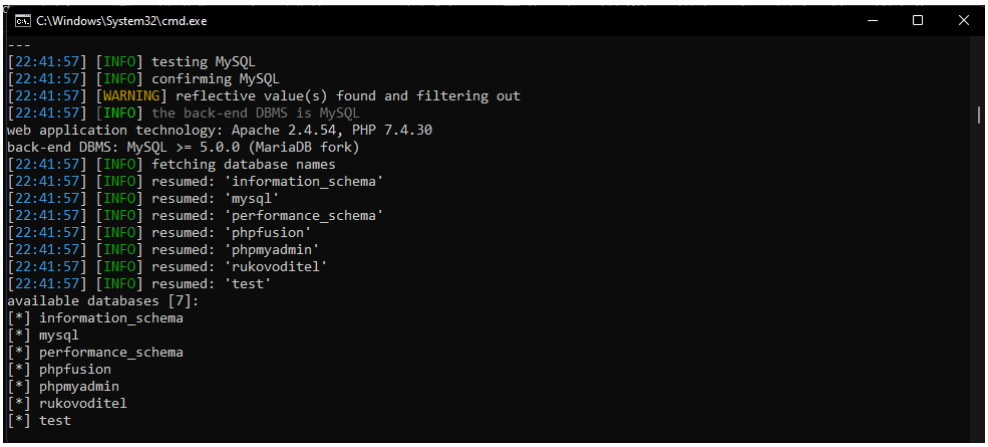
Step 1: Add single quote was submitted in the heading_field_id parameter, and a database error message was returned.



Step 2: Then add two quotes and submit the request, the error message disappears.



Step 3: Use SQLMap to dump full database.



Impact

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.
A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

qnxnb commented 3 days ago

Where do I download to rukovoditel to verify?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants