COMMUNITY CONTENT

Submit #783502: Song-Li cross_browser ca690f0fe6954fd9bcda36d071b68ed8682a786a SQL Injection

Title	Song-Li cross_browser ca690f0fe6954fd9bcda36d071b68ed8682a786a SQL Injection
Description	The legacy MySQL-backed Flask application in cross_browser contains an SQL injection vulnerability in the /details endpoint implemented in flask/uniquemachine_app.py. The handler reads ID from a JSON request body and directly concatenates it into a SQL SELECT statement without parameterization or escaping. An attacker who can reach this endpoint can submit crafted input to alter the SQL query and retrieve unintended database records, and in some MySQL deployment configurations may be able to perform broader data exfiltration or blind SQL injection techniques.
Source	https://github.com/wing3e/public_exp/issues/24
User	BigW (UID 96422)
Submission	03/20/2026 04:13 AM (17 days ago)
Moderation	04/04/2026 04:50 PM (15 days later)
Status	Accepted
VulDB entry	[Song-Li cross_browser up to ca690f0fe6954fd9bcda36d071b68ed8682a786a details Endpoint uniquemachine_app.py ID sql injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling