COMMUNITY CONTENT

Submit #783139: Akaunting v3.1.21 Cross Site Scripting

Title	Akaunting v3.1.21 Cross Site Scripting
Description	A Stored Cross-Site Scripting (XSS) vulnerability was identified in Akaunting v3.1.21, an open-source accounting application. The vulnerability exists in the notes field of invoice and bill documents. When a user holding at least a Manager-level role (both Manager and Admin roles hold the create-sales-invoices permission; Accountant and Customer roles do not) creates an invoice containing an HTML/JavaScript payload in the Notes field, the payload is stored in the database without sanitization and later rendered unescaped in the browser of any user who views the document. This satisfies the criteria for a Stored (Persistent) XSS attack. https://github.com/akaunting/akaunting
Source	⚠ https://docs.google.com/document/d/1TFwYGdjDblEGCMM0l67PXz0HXZu_iUqWDQZavtM9t1U/edit?usp=sharing
User	gabriel (UID 72007)
Submission	03/19/2026 08:05 PM (17 days ago)
Moderation	04/04/2026 04:29 PM (16 days later)
Status	Accepted
VulDB entry	355308 [Akaunting up to 3.1.21 Invoice/Billing notes cross site scripting]
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