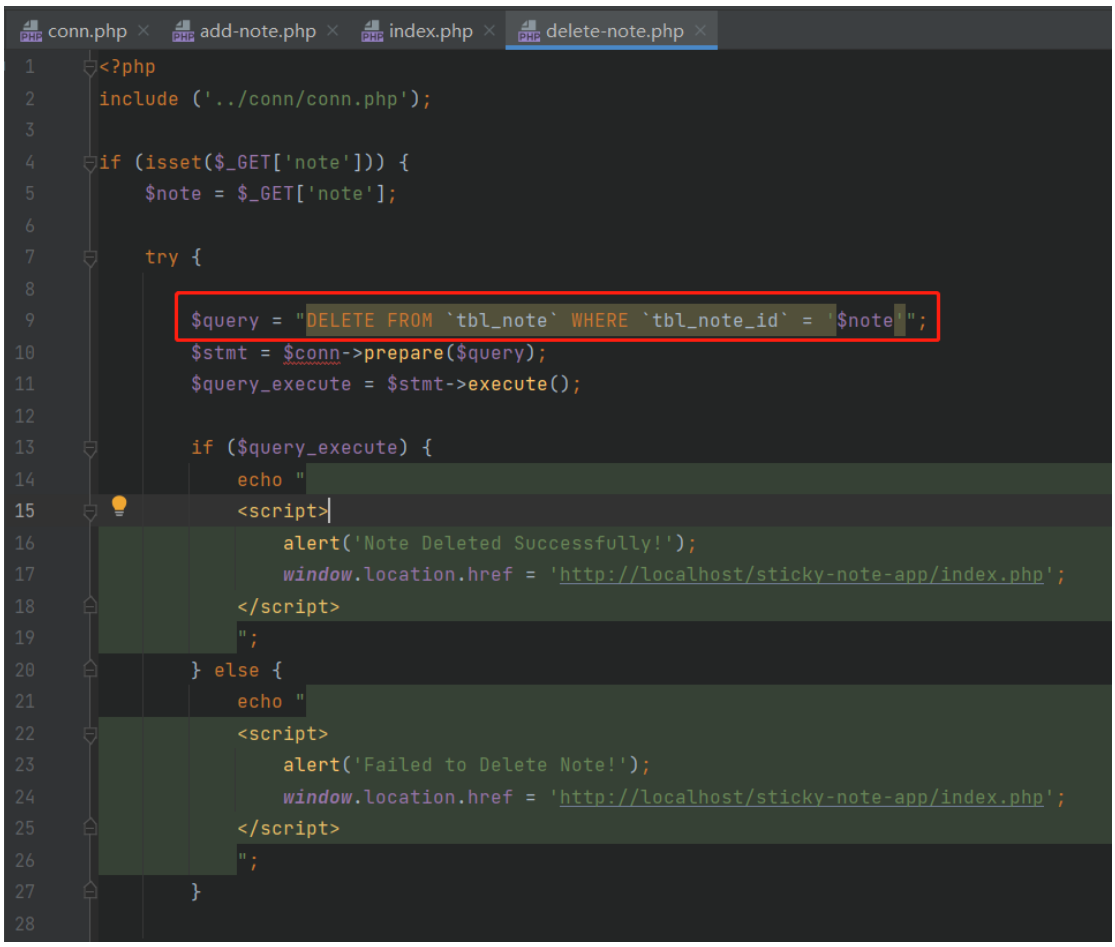
SQL injection vulnerability exists in 'note' parameter of 'endpoint/delete-note.php' file of Sticky Notes App. Important user data or system data may be leaked and system security may be compromised. When visit 'delete-note.php' and page parameter is 'note' can do sql injection. 'note' variables are dynamically concatenated even though the code is precompiled.

delete-note.php:



Poc:

http://127.0.0.1/sticky-notes-app/endpoint/delete-note.php?note=0%27%20and%20updatexml(1,concat(0x7e,(database())),1)--+