

**Researcher Name:** Guru Raghav Saravanan

**Product:** File Manager App SourceCodester

**Vulnerability:** Cross Site Scripting

### POC:

A Cross-Site Scripting (XSS) vulnerability exists in the **add-file** functionality of the application. This issue arises because the input fields for **File Title** and **Uploaded By** do not properly sanitize user inputs, allowing attackers to inject malicious scripts.

### Attack Screenshots:

### Dashboard:

| File Manager App           |                       |                                       |             |                     |        |
|----------------------------|-----------------------|---------------------------------------|-------------|---------------------|--------|
| <div>+ Add File</div>      |                       |                                       |             |                     |        |
| Show <div>10</div> entries |                       | Search: <input type="text"/>          |             |                     |        |
| File ID                    | File Title            | File                                  | Uploaded By | Date                | Action |
| 1                          | JavaScript            | What Is JavaScript.docx               | Lorem Ipsum | 2023-10-17 04:52:31 | Action |
| 2                          | HTML                  | HTML stands for.docx                  | Jane Doe    | 2023-10-17 04:53:21 | Action |
| 3                          | CSS                   | What Is CSS and How Does It Work.docx | John Doe    | 2023-10-17 04:53:39 | Action |
| 4                          | Projects              | List of Projects.txt                  | Lorem Ipsum | 2023-10-17 05:27:39 | Action |
| 5                          | Programming Languages | ProgrammingLanguage.docx              | Jane Doe    | 2023-10-17 05:29:17 | Action |

### Injecting Payload in File Title and Uploaded By fields:

Add file

File Title

"><script>alert('File Title')</script>

File

Choose file

sample.txt.txt

Uploaded By (Optional)

"><script>alert('Uploaded By')</script>

Close

Add File

### Payload Execution:



