ciph0x01 Create CVE-2022-42198.md History

1 contributor

26 lines (14 sloc) | 930 Bytes

Affected Component

ERMS v1.0 - https://www.sourcecodester.com/download-code?nid=15160&title=Simple+Exam+Reviewer+Management+System+in+PHP%2FOOP+Free+Source+Code

Description

In Simple Exam Reviewer Management System v1.0 the User List function suffers from insecure file upload.

Steps to reproduce

Login as a low privileged user

Navigate to below mentioned endpoint

```
"/admin/?page=user/list"
```

Choose any user and click on action and select edit

There will be an avatar upload function for the user , where any file can be uploded .

It is possible to upload any malicious files which includes php file for remote code execution,svg for Cross site scripting and so on.

Impact

Insecure file upload leads to Remote code execution and Cross site scripting.