ciph0x01 Create CVE-2022-42201.md History

1 contributor

24 lines (13 sloc) | 851 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

Insecure file upload functionality leads to remote code execution.

Steps to reproduce

Login as Admin

Navigate to below mentioned endpoint

```
"/admin/?page=system_info"
```

There will be a file upload function for uploading System Logo and Website Cover , 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 stored cross site scripting.