draco1725 / **POC** Public

Code Issues Pull requests Actions Projects Security Insights

main

POC / Exploit / **Stored Xss**

draco1725 Update Stored Xss

History

1 contributor

31 lines (21 sloc) | 1.02 KB

```
# Exploit Title: Human Resource Management System v1.0 - Normal user Apply leave "Reason" Paramete
# Exploit Author: Pratik Shetty
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/15740/human-resource-management-system-proje
# Software Link: https://www.sourcecodester.com/php/15740/human-resource-management-system-project
# Version: v1.0
# Tested on: Windows 10, Apache
# CVE: CVE-2022-3502


Description:
A Persistent XSS issue in Human Resource Management System v1.0 allows to inject Arbitrary JavaScr


Parameter:
Leave Apply = Reason


Payload:
<script>prompt(1)</script>


Steps:
1) Login as a normal user
2) Now in that we can see an tab named "Leave" in that go to "Apply"
3) The Parameter "Reason" in this we put our payload.

Payload: <script>prompt(1)</script>

```

```
4) Now fill the other details and save the file
5) Go to "Application" and we can see that our Payload has been executed.
```