

main

...

[webray.com.cn](https://webray.com.cn) / [cve](#) / [Student Information System](#) / [SIS\\_Stored\\_Cross\\_Site\\_Scripting\(XSS\).md](#)



Xor-Gerke Create SIS\_Stored\_Cross\_Site\_Scripting(XSS).md

History

1 contributor

33 lines (21 sloc) | 1.66 KB

...

# Student Information System - 'Student Roll' Stored Cross-Site Scripting(XSS)

Exploit Title: Student Information System - 'Student Roll' Stored Cross-Site Scripting(XSS)

Exploit Author: [webraybtl@webray.com.cn](mailto:webraybtl@webray.com.cn) inc

Vendor Homepage: <https://www.sourcecodester.com/php/15147/simple-student-information-system-phpoop-free-source-code.html>

Software Link: <https://www.sourcecodester.com/download-code?nid=15147&title=Simple+Student+Information+System+in+PHP%2FOOP+Free+Source+Code>

Version: Zoo Management System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application. Student Information System does not filter the content correctly at the "Student Roll" module, resulting in the generation of stored XSS.

### Payload used:

```
<script>alert(111)</script>
```

### Proof of Concept

1. Login the CMS. Default Admin Access Username: admin Password: admin123
2. Open Page <http://172.24.5.102/sis/admin/?page=students> and click View button
3. Put XSS payload ( `<script>alert(111)</script>` ) in the Student Roll box and click on Save Student Details to publish the page

The screenshot shows the 'Update Student Details' page for student ID 231415061007. The page has a dark sidebar with navigation links: Dashboard, Students, New Student, Student List, Maintenance, Department List, Course List, User List, and Settings. The main content area is titled 'Update Student Details - 231415061007'. It contains a form with the following fields:

- Student Roll:** A text input field containing the XSS payload `<script>alert(111)</script>`, which is highlighted with a red box.
- First Name:** Mark
- Middle Name:** D
- Last Name:** Cooper
- Gender:** Male
- Date of Birth:** 2007/06/23
- Contact #:** 09123456789
- Present Address:** This my sample present address.
- Permanent Address:** This my sample permanent address.

At the bottom right of the form, there are two buttons: 'Save Student Details' and 'Cancel'.

4. Viewing the successfully published page,We can see the alert.

