Badminton Center Management System - 'username' Stored Cross-Site Scripting(XSS)

Exploit Title: Badminton Center Management System - 'username' Stored Cross-Site Scripting(XSS)

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html

Software Link:https://www.sourcecodester.com/download-code?nid=15318&title=Badminton+Center+Management+System+in+PHP%2FOOP+Free+Source+Code

Version: Badminton Center Management System

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.Badminton Center Management System does not filter the content correctly at the "userlist" module, resulting in the generation of stored XSS.

Payload used:

```
</td><img src="" onerror="alert(111111111)"><td>123
```

Proof of Concept

1. Login the CMS. Admin Default Access: username:admin Password: admin123
2. Open Page http://192.168.67.5/bcms/admin/?page=user/list and click Edit button
3. Put XSS payload in the content box and click on Edit Account to publish the page

image-20220523162828564

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