Prison Management System - system_info 'name' Stored Cross-Site Scripting(XSS)

Exploit Title: Prison Management System - system_info 'name' Stored Cross-Site Scripting(XSS)

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15368/prison-management-system-phpoop-free-source-code.html

Software Link:https://www.sourcecodester.com/download-code?nid=15368&title=Prison+Management+System+in+PHP%2FOOP+Free+Source+Code

Version: Prison Management System 1.0

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

Description

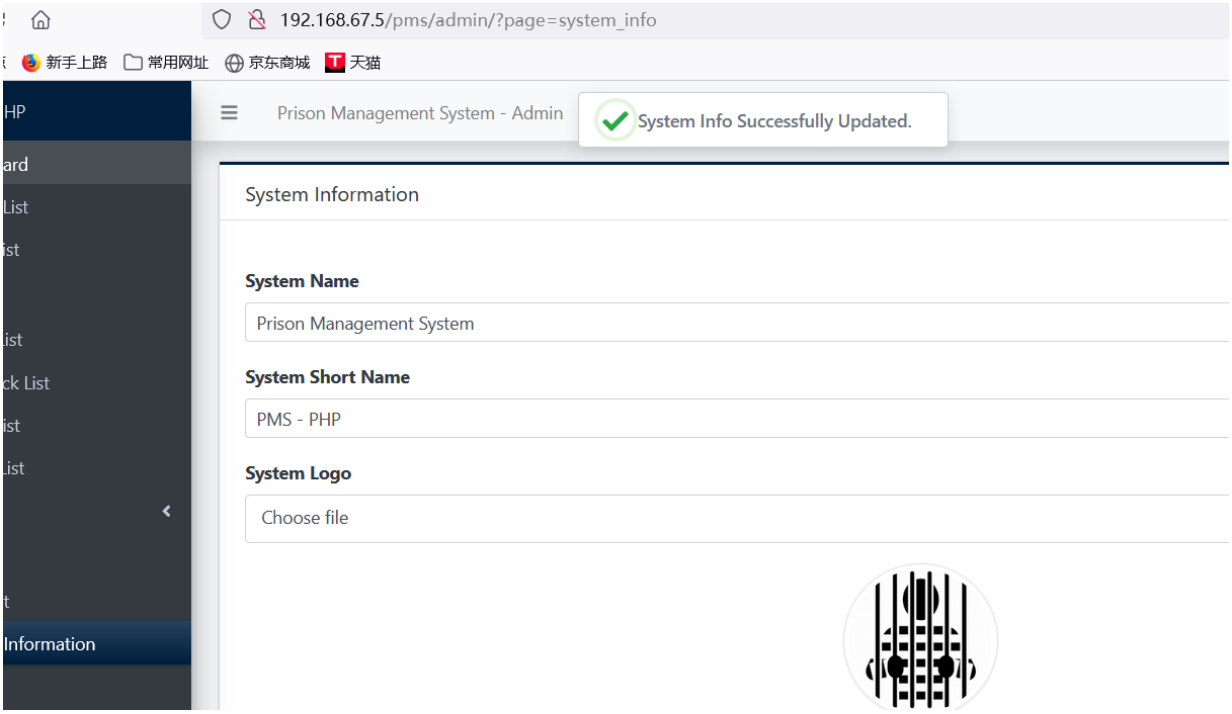
Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application.Prison Management System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

Payload used:

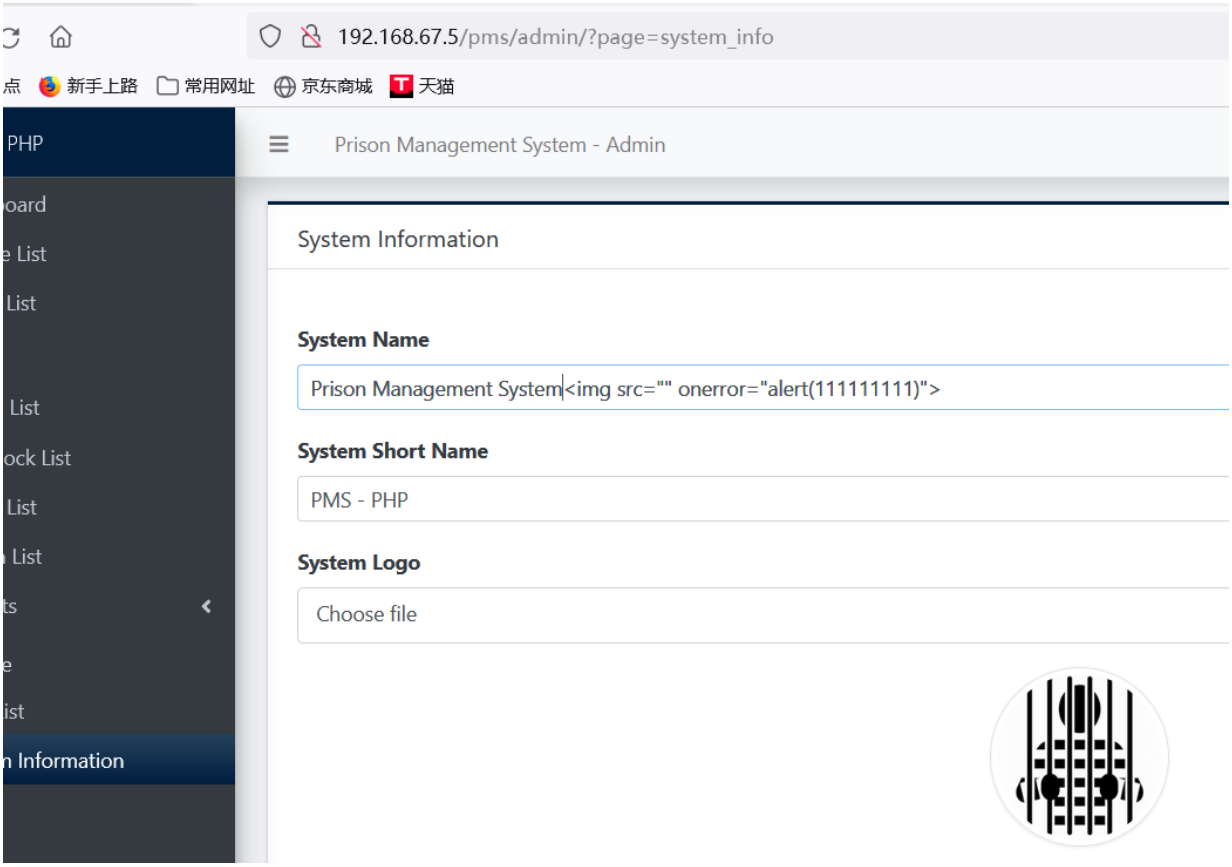
```
<img src="" onerror="alert(111111111)">
```

Proof of Concept

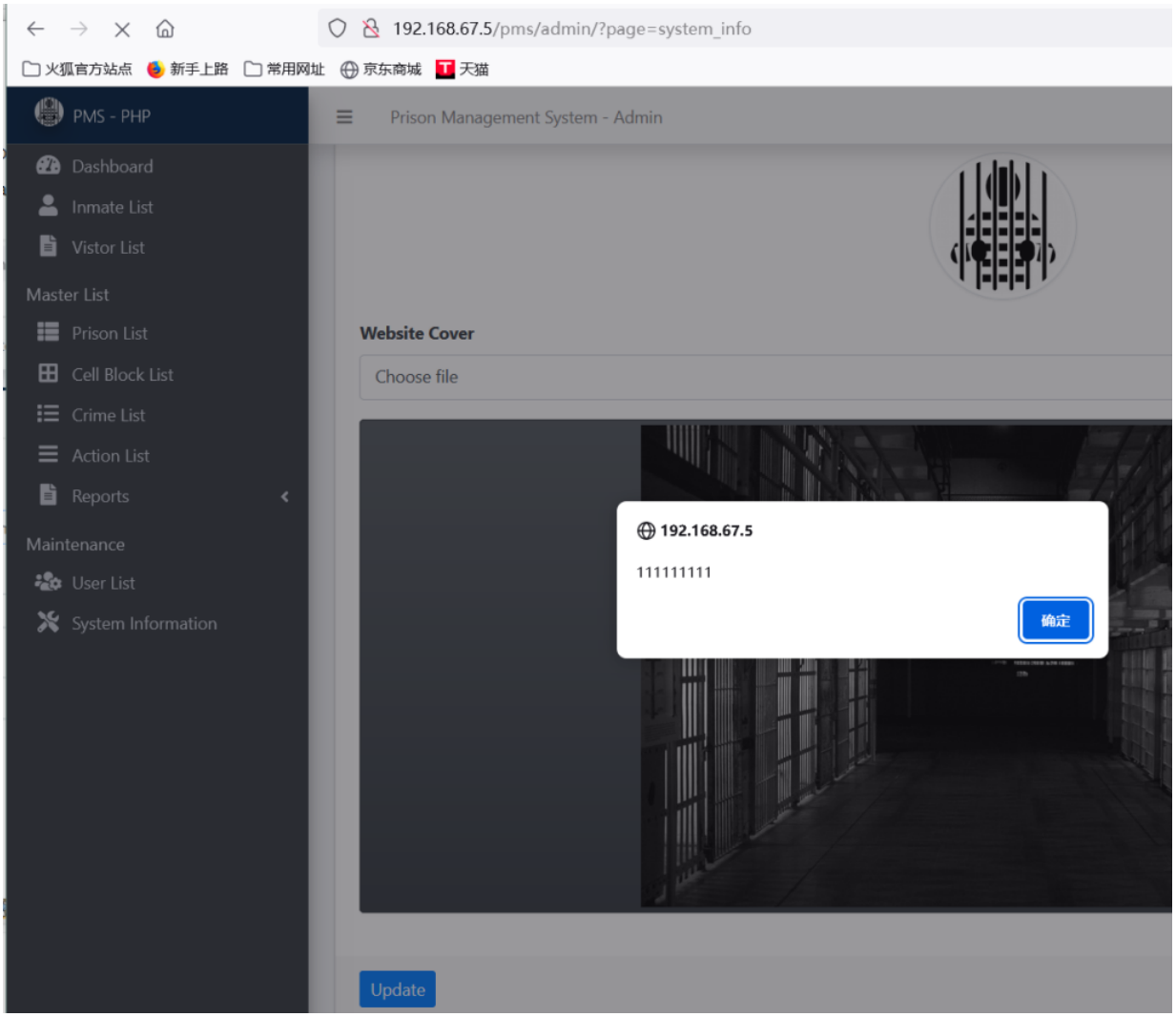
1. Login the CMS. Admin Default Access: username: admin Password: admin123
2. Open Page http://192.168.67.5/pms/admin/?page=system_info



3. Put XSS payload in the content box and click on Update to publish the page ;



4. We can see the alert.;


192.168.67.5/pms/admin/?page=system_info
火狐官方站点
新手上路
常用网址
京东商城
天猫
PMS - PHP
Prison Management System - Admin
Dashboard
Inmate List
Vistor List
Master List
Prison List
Cell Block List
Crime List
Action List
Reports
Maintenance
User List
System Information
Website Cover
Choose file
192.168.67.5
111111111
确定
Update