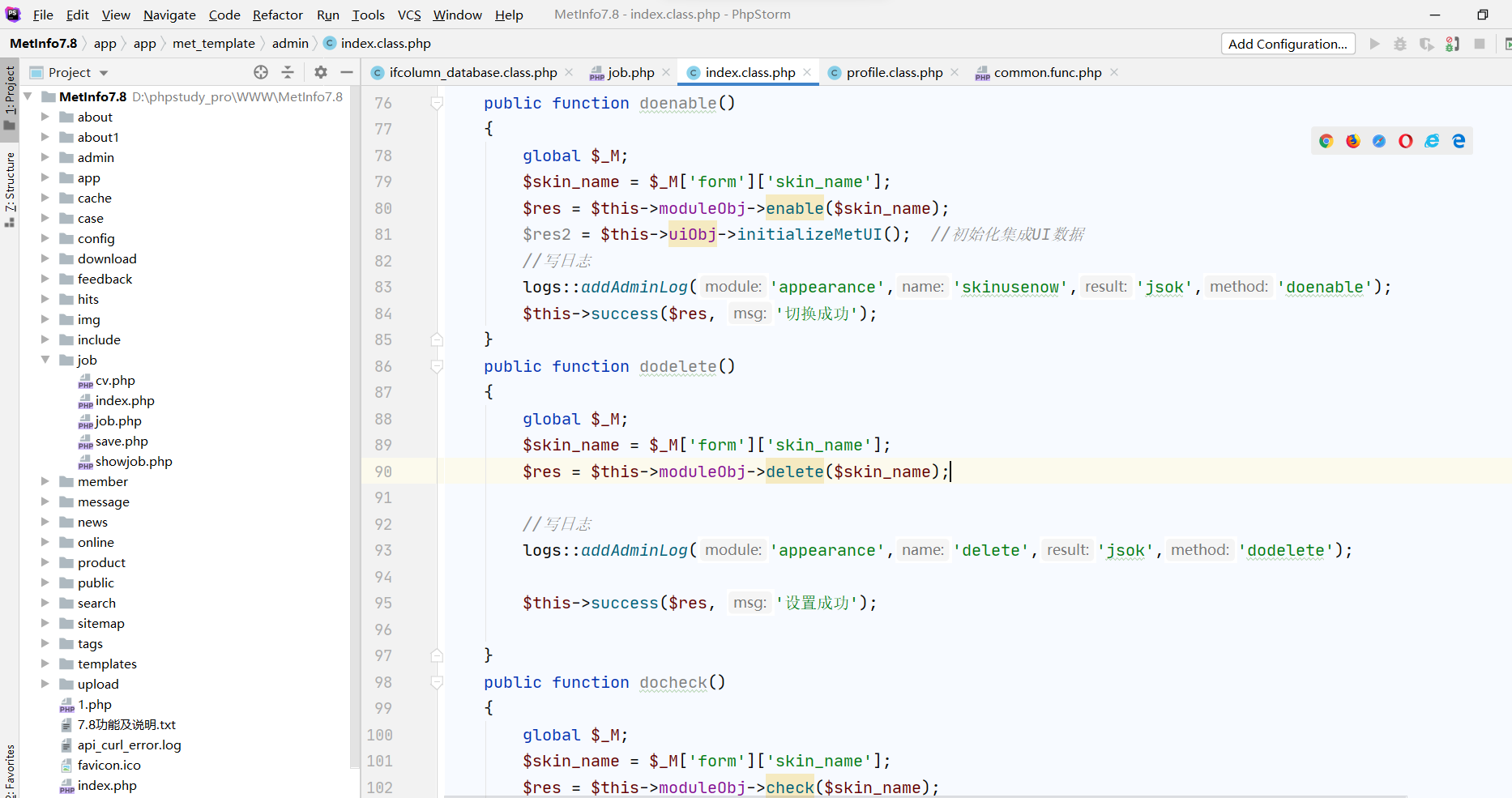
https://www.metinfo.cn/download/

app\app\met\_template\admin\index.class.php The file only determines whether the operation is done with the permission of admin, and there is no judgment on dodelete()

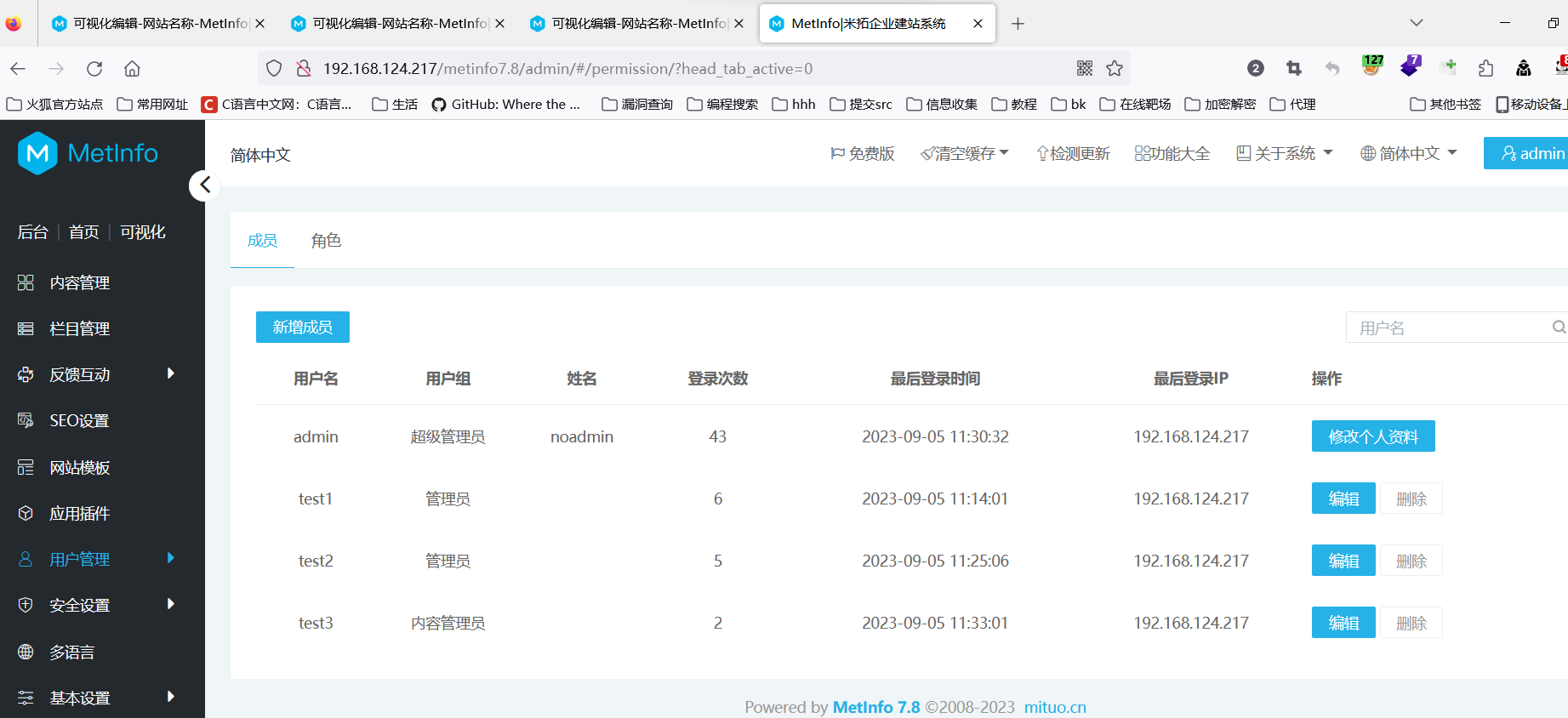


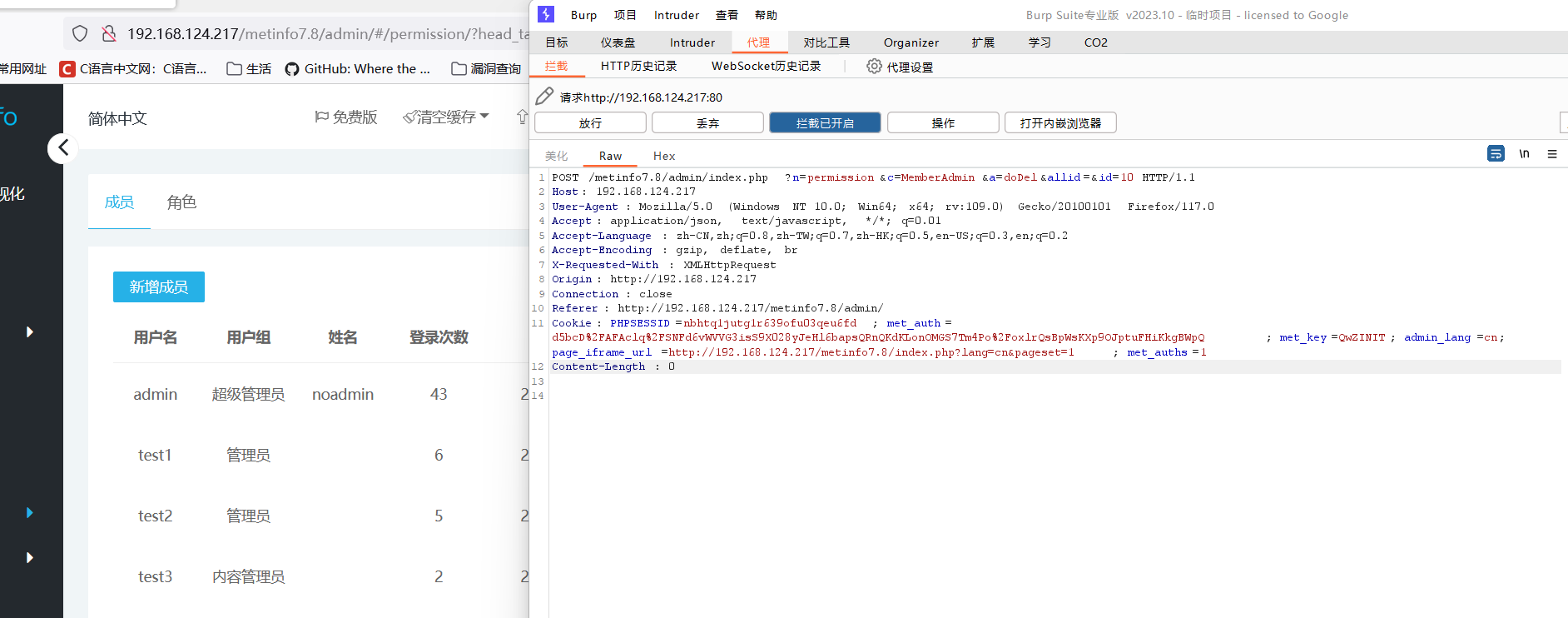


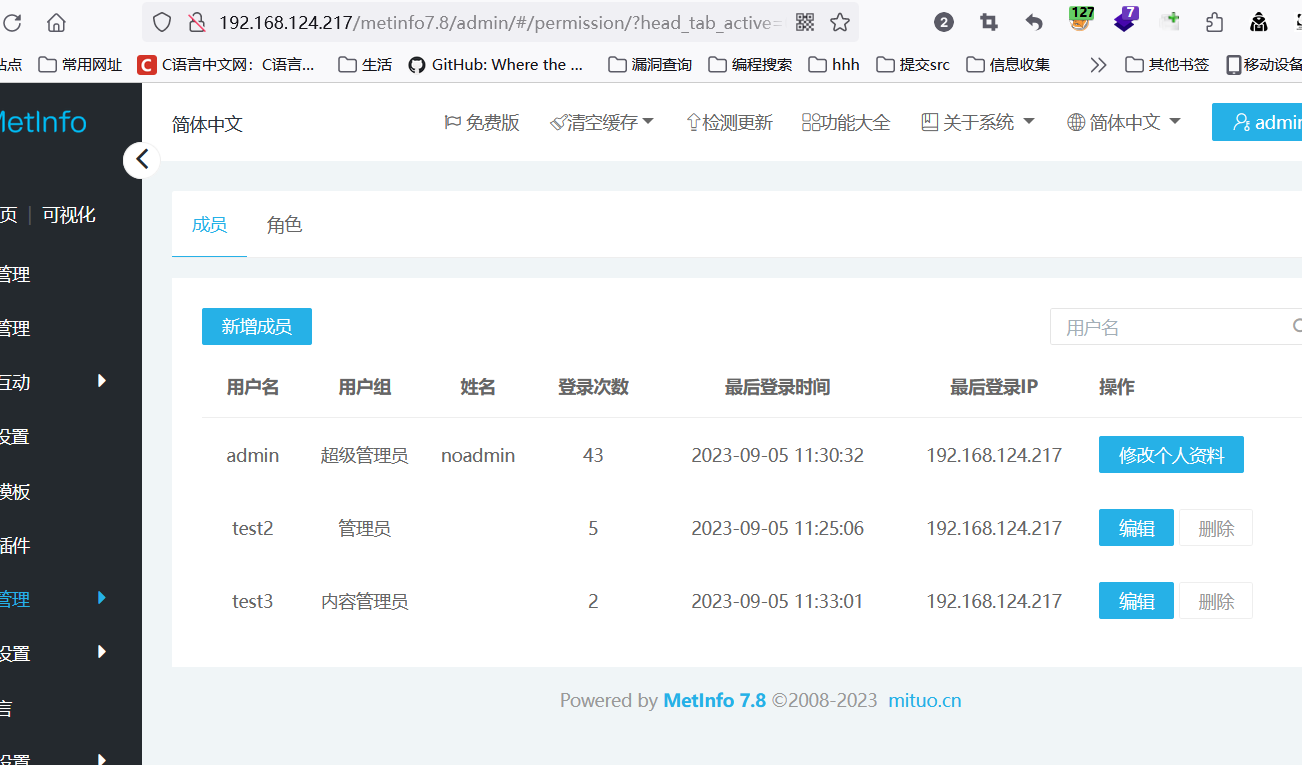
Test1 id is 10, password 123456

Test2 id is 11, password 123456

Test3 id is 12, password 123456



When clicking to confirm deletion, capture the packet and send it to the built-in csrf generation module of BP



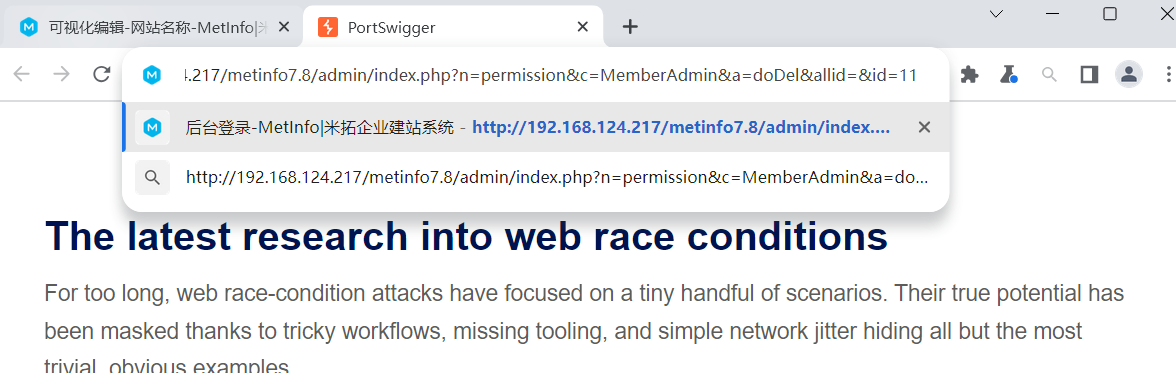
Test1 delete图形用户界面, 文本, 应用程序, 电子邮件

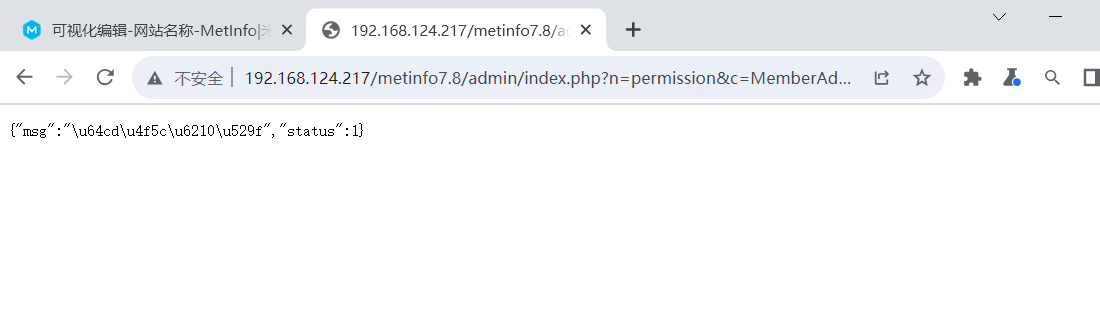
描述已自动生成

Direct access

http://192.168.124.217/metinfo7.8/admin/index.php?n=permission&c=MemberAdmin&a=doDel&allid=&id=11 ID 11 is test2

Change the browser and log in to admin, then access the link

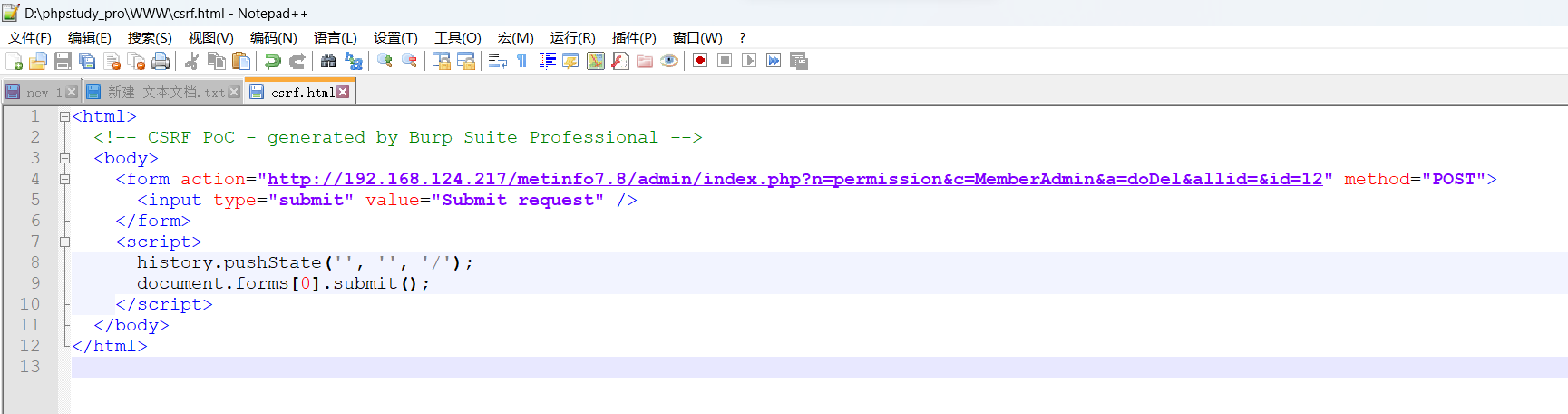




图形用户界面, 文本, 应用程序, 电子邮件, 网站

描述已自动生成

Test2 (id=11) deleted successfully

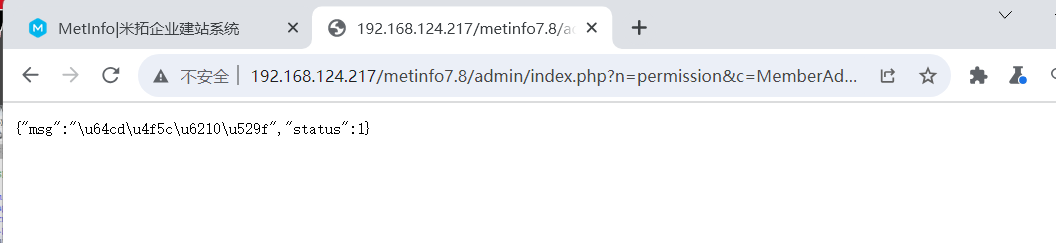
ID changed to 12 (test3) bp generated by the csrf module



Admin access <http://192.168.124.217/csrf.html>

图形用户界面, 文本, 应用程序

描述已自动生成



图形用户界面, 文本, 应用程序, 电子邮件, 网站

描述已自动生成