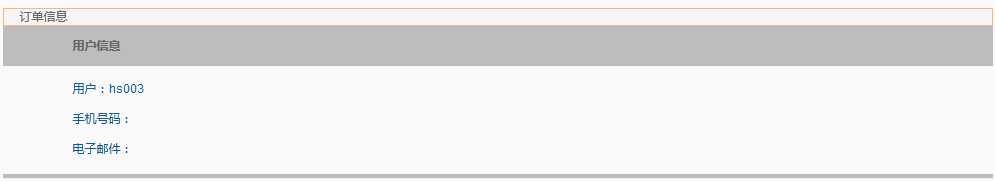
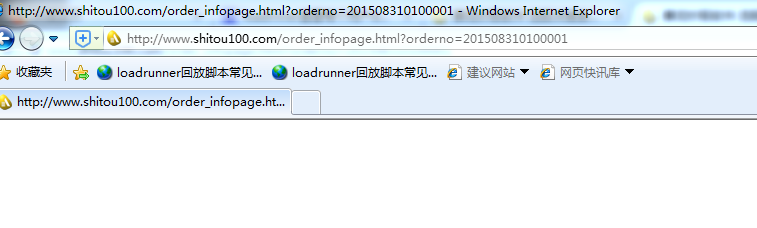
漏洞测试方法：  
石头网的用户个人信息修改处及用户订单删除功能处并未添加Token保护，这将导致这两个敏感操作表单处存在CSRF攻击的风险。  
URL：http://www.shitou100.com/doChange.do  
 http://www.shitou100.com/orderlist\_infopage.html?delorderno=

C:\Users\linlong\AppData\Roaming\Tencent\Users\1179956065\QQ\WinTemp\RichOle\TNFYC[EJ3NFDBPI0FDBIM`E.png

石头网提供部分收费课程给用户使用，用户在购买的流程中会形成一个订单。查看订单信息可通过点击“我的订单”进行查看。  
URL：http://www.shitou100.com/order\_infopage.html?orderno=  
参数orderno是订单的编号，服务端通过该参数进行不同订单的判断。但是服务端并未对用户身份进行识别，我们可以通过遍历的方式查询他人的订单信息。订单信息会泄露整站所有用户的购买信息，用户名，手机号及邮箱。例如：通过复制此链接可以查看到如图信息：



解决方案：在后台上随机产生Token传至页面，后台验证,订单删除，用户信息修改，修改密码功能都加上随机ID验证防止重复提交和CSRF劫持攻击.



查看不到用户信息。问题成功解决！