

HIT

Introduction to Information Security

Lab 2

## class：1403201

## Student number：1130320118

## Name：Yang Yi

1. Purposes

1）深入理解跨站脚本攻击概念；

2）掌握形成跨站脚本漏洞的条件；

3）掌握对跨站脚本的几种利用方式。

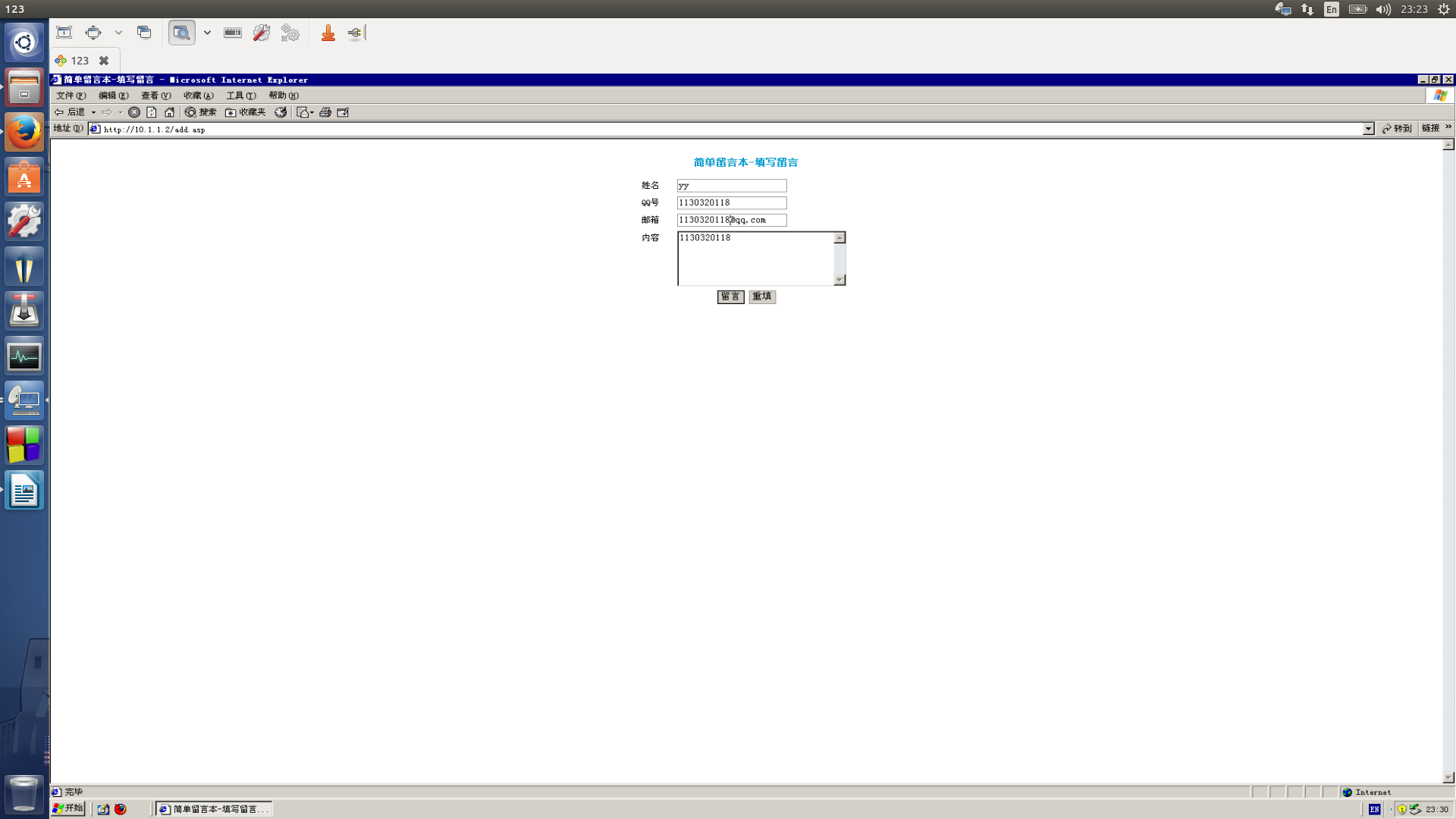
1. Procedure

# 熟悉留言系统

* 1. login windows and open [http://10.1.1.2](http://10.1.1.2/)

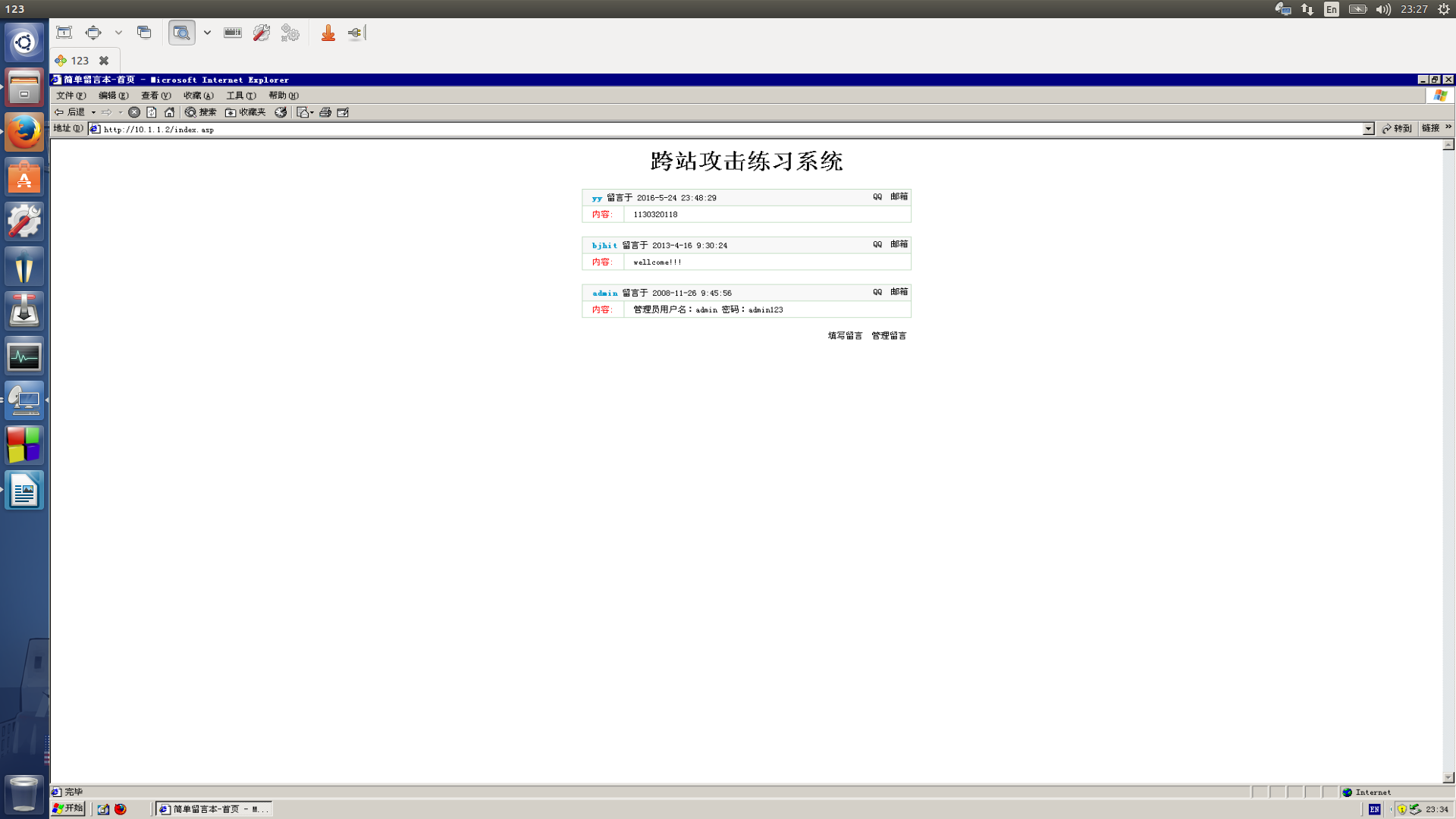


* 1. leave some massage on the site

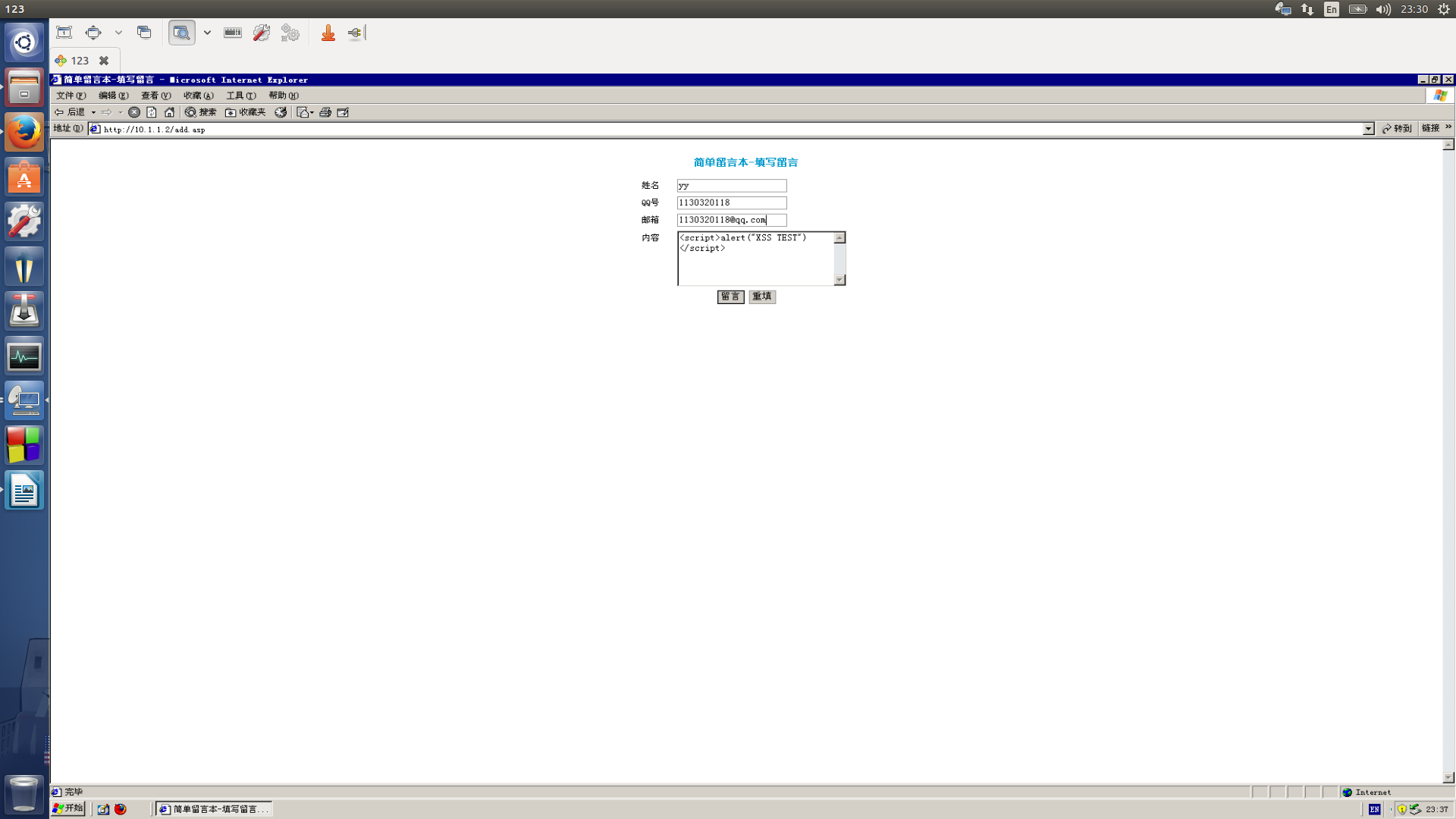


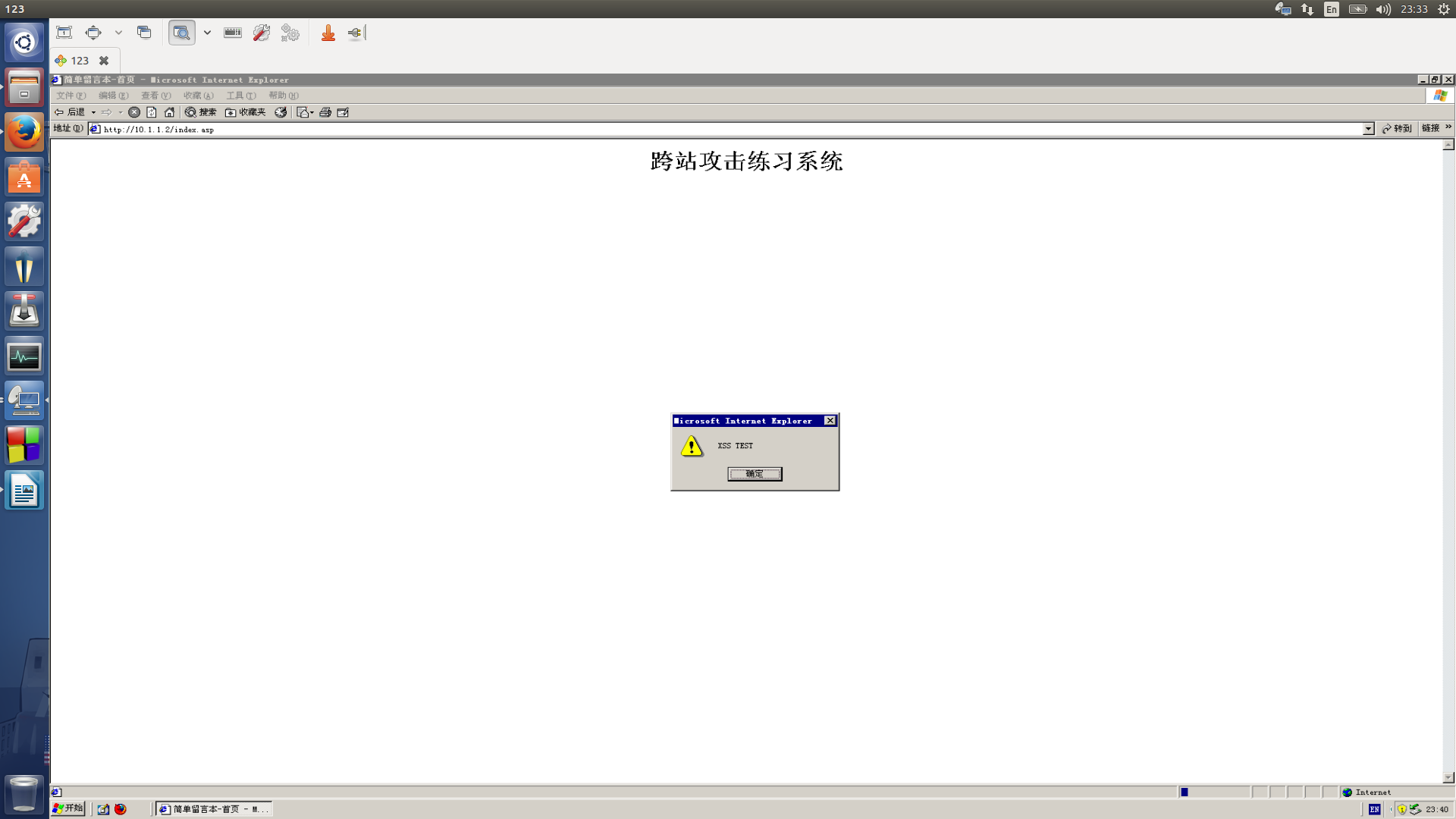
# 存储式跨站脚本测试

* 1. open the bbs



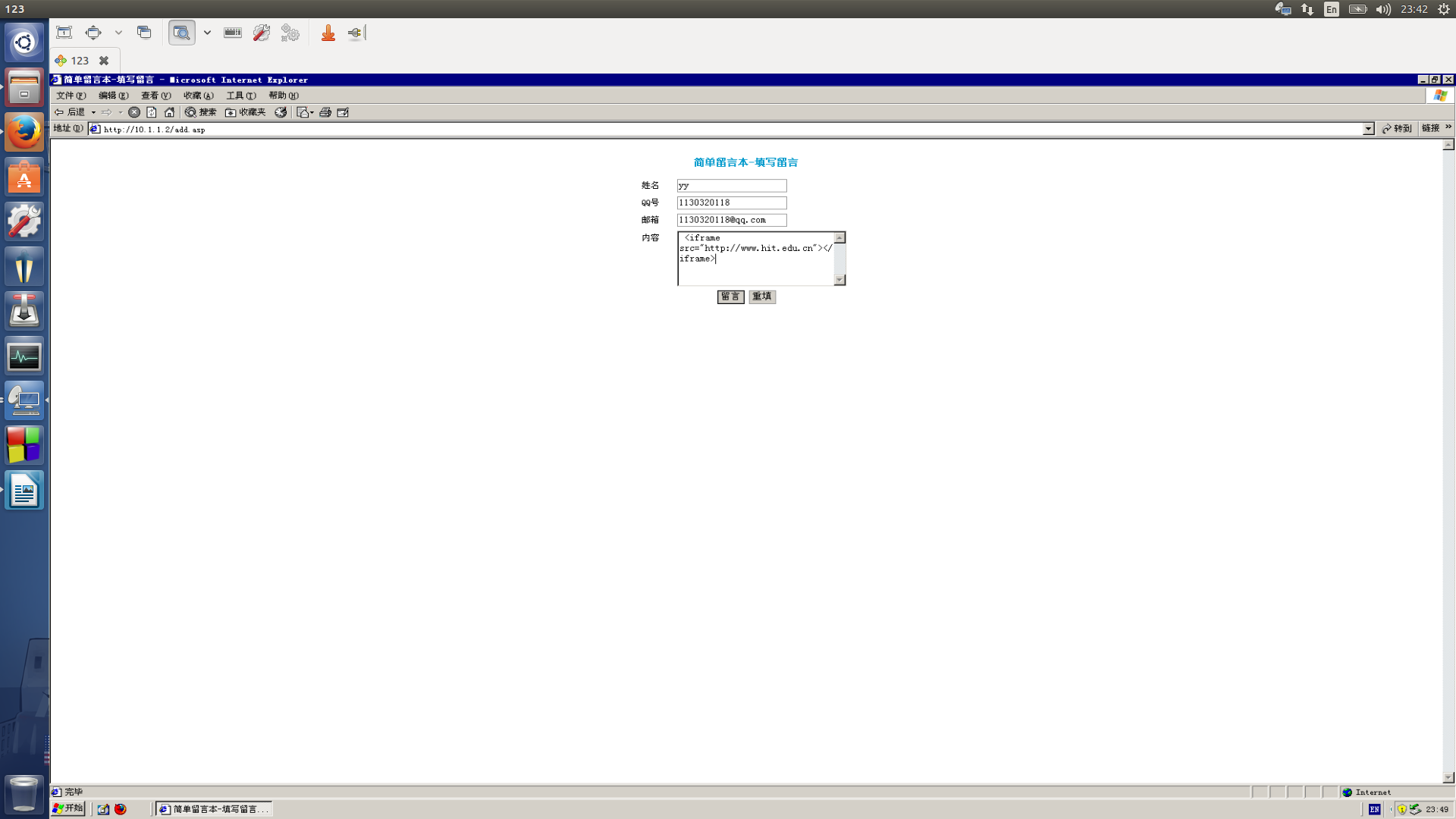
* 1. 在留言内容中填写包含有跨站测试的脚本，提交后观察返回效果。





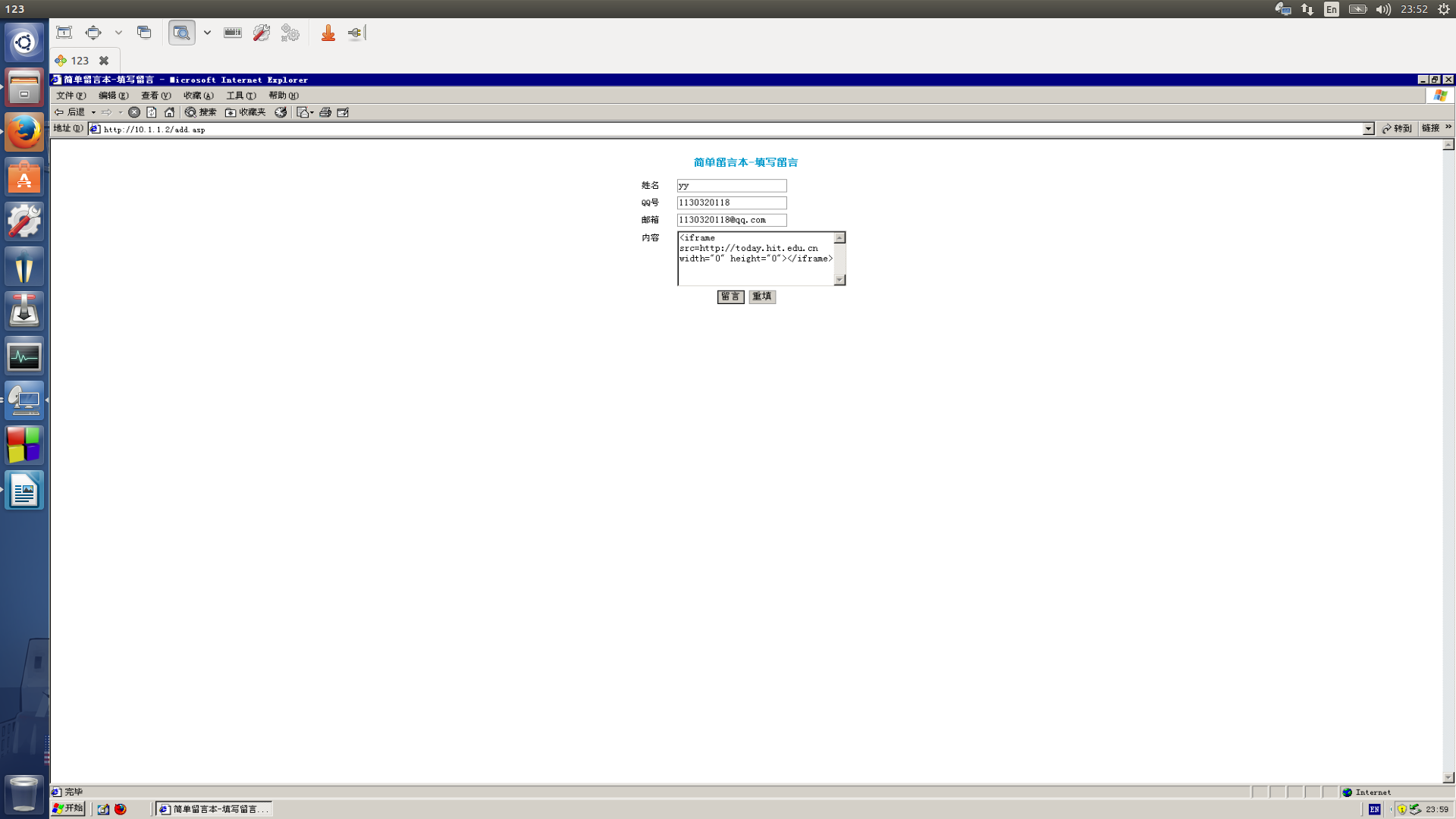
# 储式跨站漏洞的简单利用

* 1. 增加一留言，并在留言内容中改为 <iframe src="http://www.hit.edu.cn"></iframe>



* 1. 测试返回效果





# 

# 利用存储式跨站漏洞窃取用户cookie

1. Conclusion
   1. 1
   2. 1