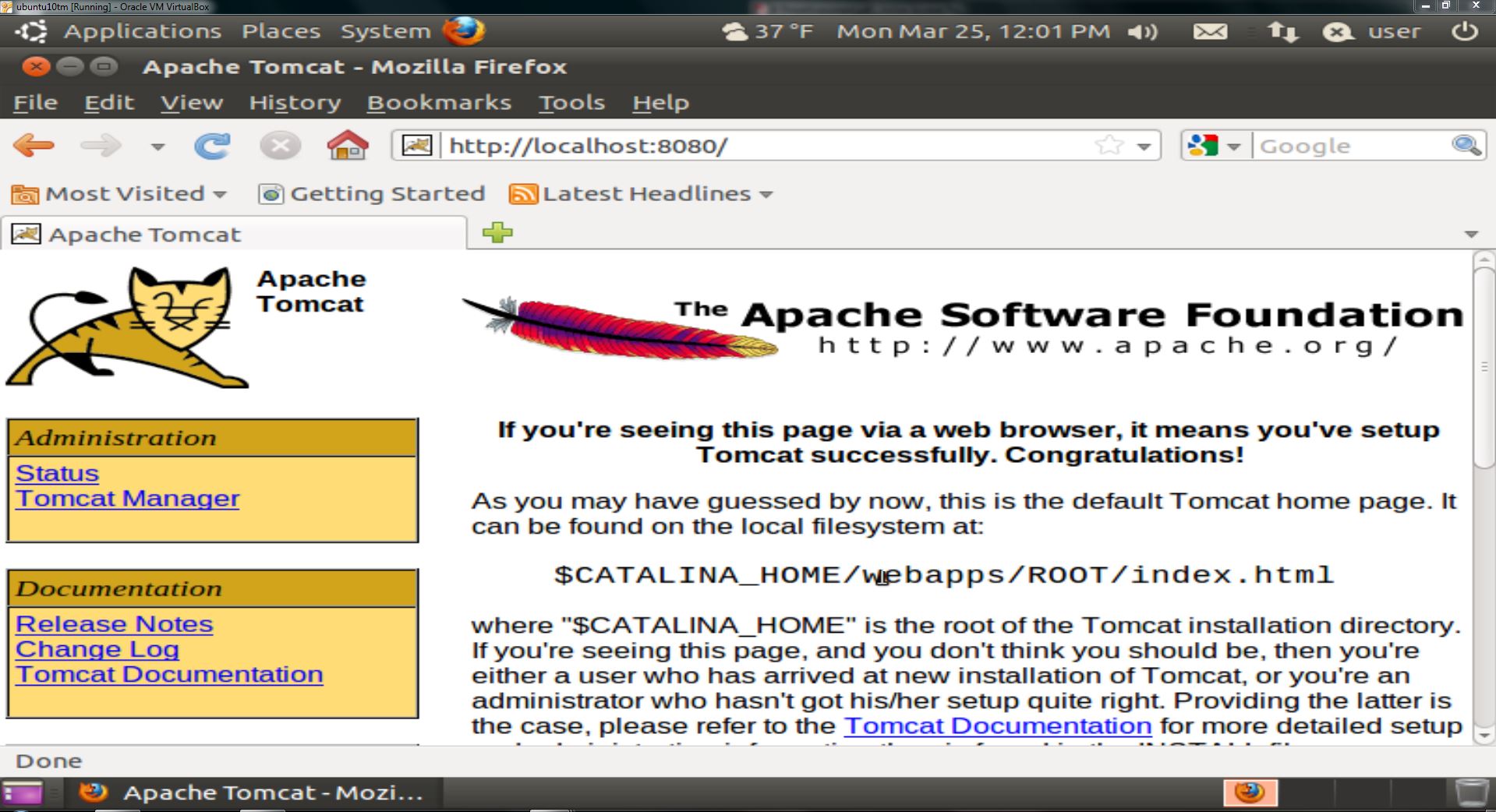
Erich Viebrock

ECPE 178

Lab #7: Threat Assessment

1. **Paste a screenshot of the Apache Tomcat welcome page from the browser.**



1. **What is the HTTP command used in the first transaction between the browser and WebGoat?**

GET http://localhost:8080/WebGoat

1. **What is the HTTP version?**

1.1

1. **The value for person is**

Erich

1. **The value for submit is**

Go!

1. **Explain the functions of the POST command with the two parameters.**

Requests server to accept enclosed data for later storage.

1. **What is the administrator’s user name?**

webgoat.

1. **What is the password?**

webgoat.

1. **Describe one method to improve the login security here.**

Choose a more specific question, like “What is the name of your 3rd grade teacher?

1. **Explain what you have learned from this exercise.**

With simple forgot password authentication questions, accounts are easily exploitable.

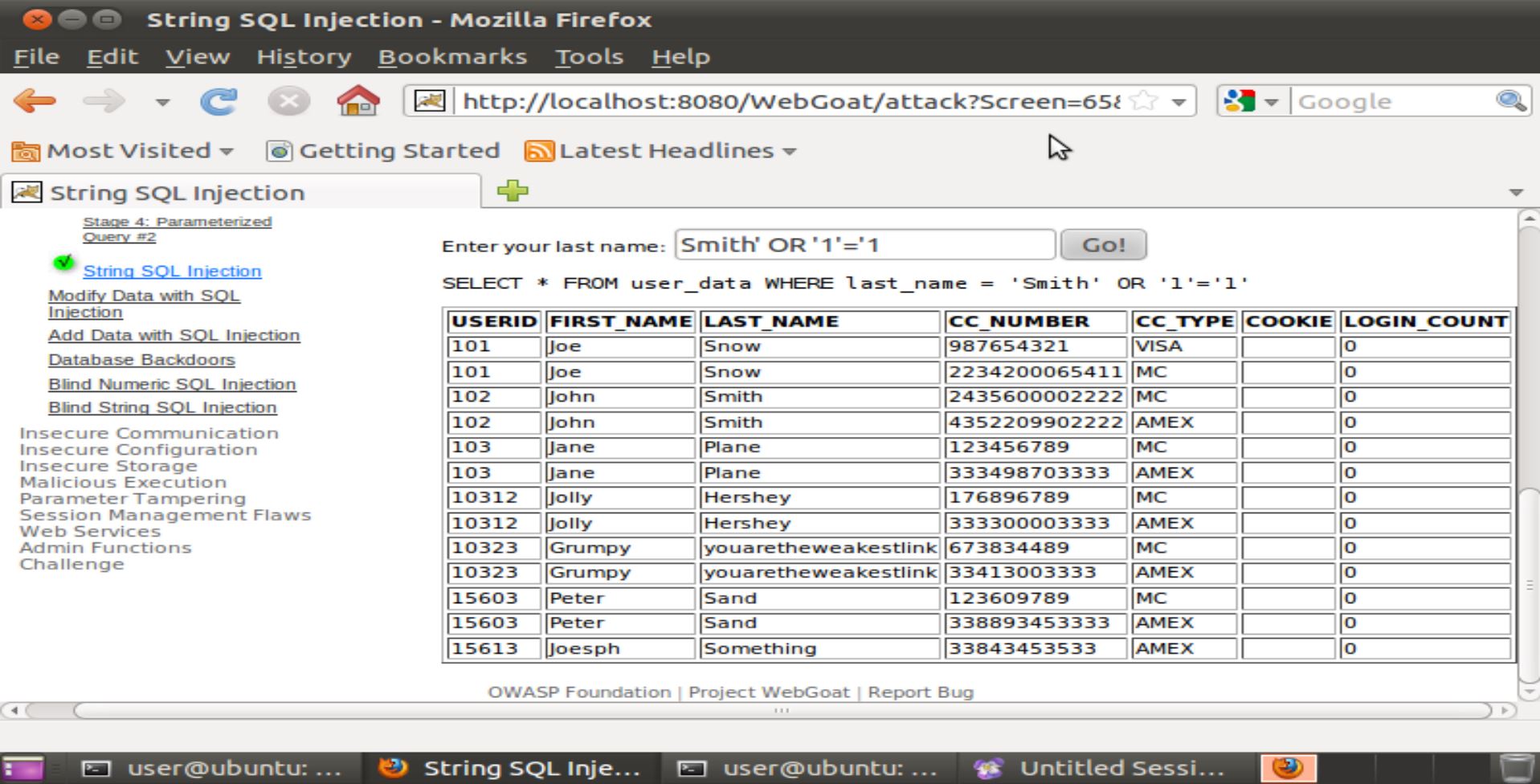
1. **How many entries have you obtained?**

2.

1. **Are they all information regarding theh user “Smith”?**

Yes, they all pertain to the user “John Smith”.

1. **Paste a screenshot of your results.**



1. **What is the security implication of your results?**

Because the statement 1=1 is always true, the server will return all entries in the database.

1. **Describe a method to fix the vulnerability in this exercise.**

By eliminating “=” in the search field, a user will no longer be able to make searches that are universally true.

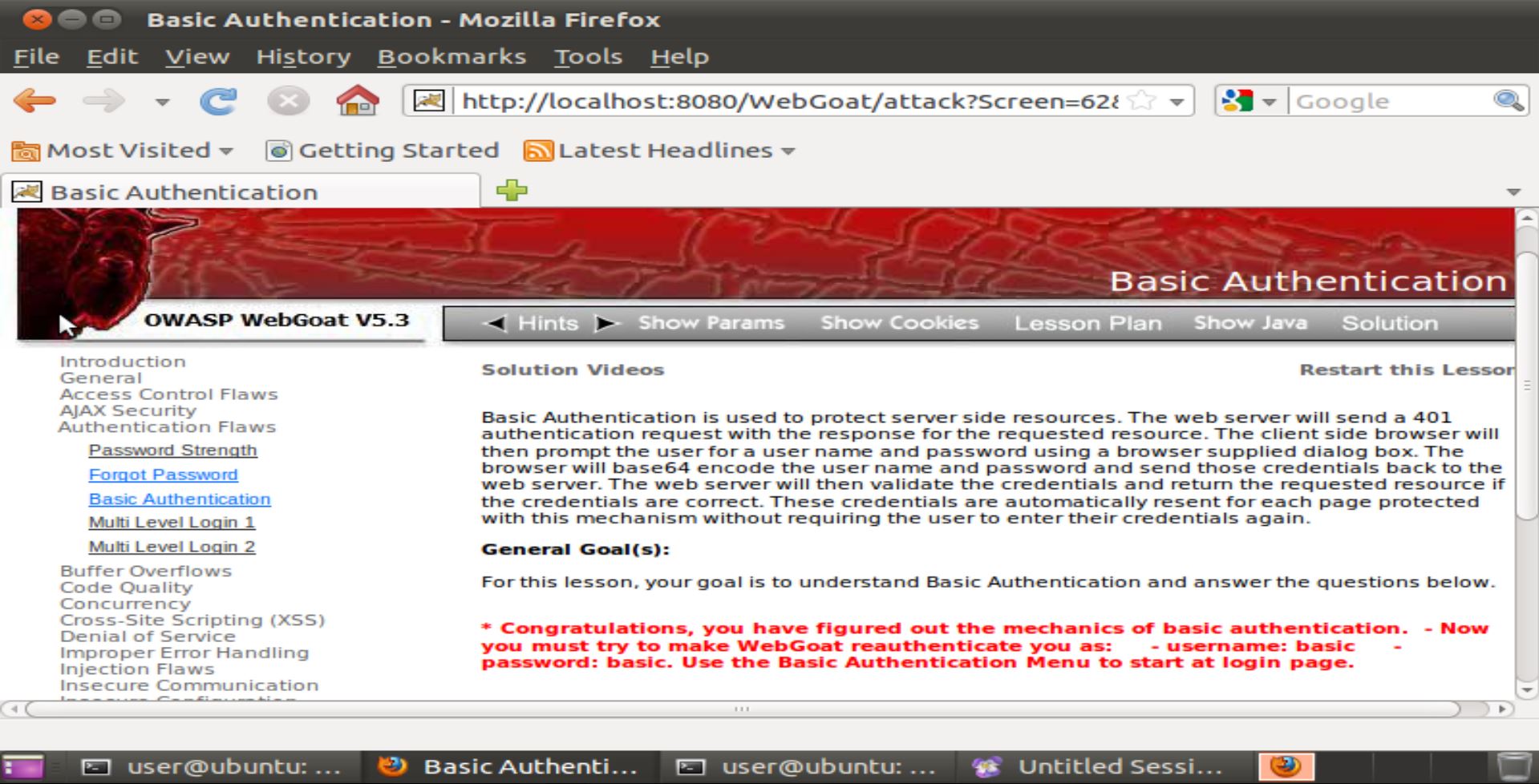
1. **Write down the code here.**

**Z3Vlc3Q6Z3Vlc3Q=**

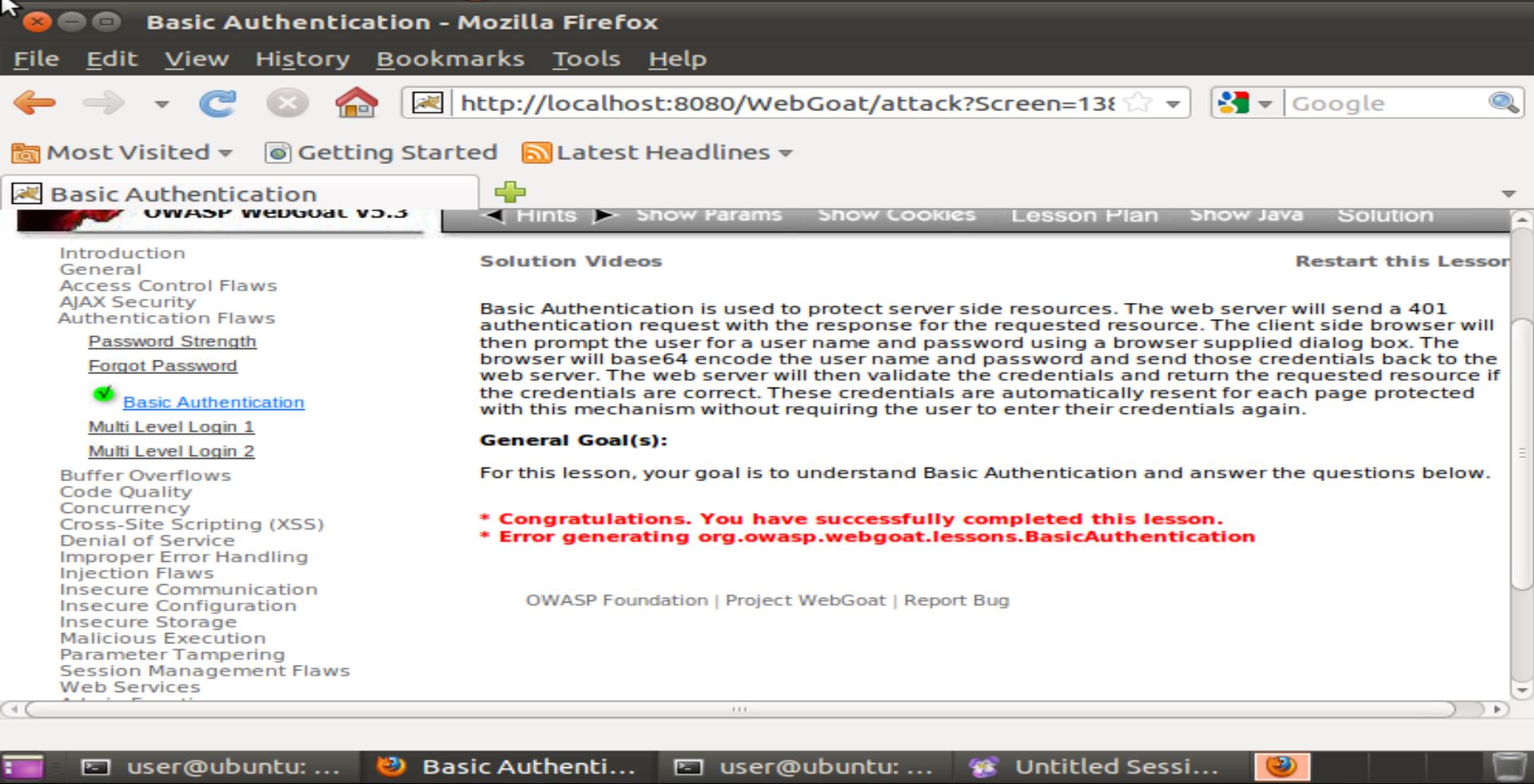
1. **What is the plain text value of the authentication header that you have just decoded?**

guest:guest

1. **Once you have successfully finished this exercise, paste a screen shot below.**

****

1. **Paste a screen shot below that shows you have completed the Basic Authentication exercise.**



1. **Describe what you have learned from this exercise.**

I learned how to use a proxy server, as well as some exploits a proxy server can enable a user to implement. I found changing some of the server requests very interesting, did not think that was possible!