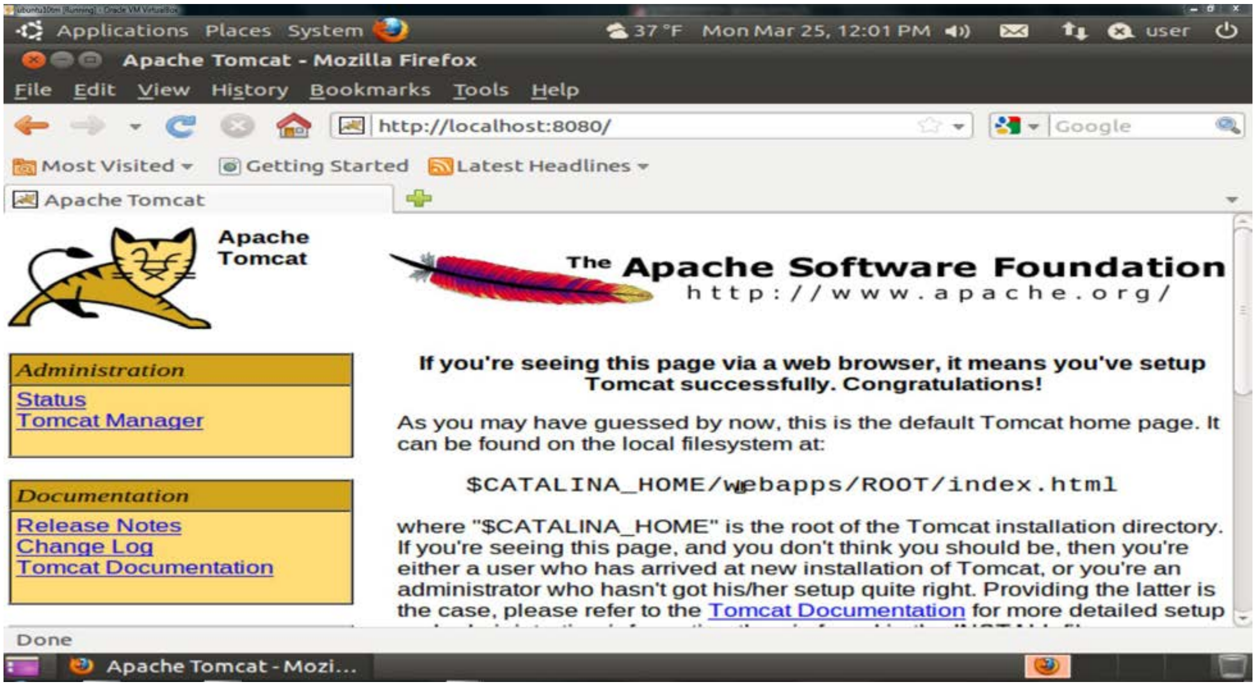
Erich Viebrock

ECPE 178

Lab #7: Threat Assessment

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



If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.html
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup

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

   GET http://localhost:8080/WebGoat

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

   1.1

4. **The value for person is**

   Erich

5. **The value for submit is**

   Go!

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

   Requests server to accept enclosed data for later storage.

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

   webgoat.

8. **What is the password?**

   webgoat.

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

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

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

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

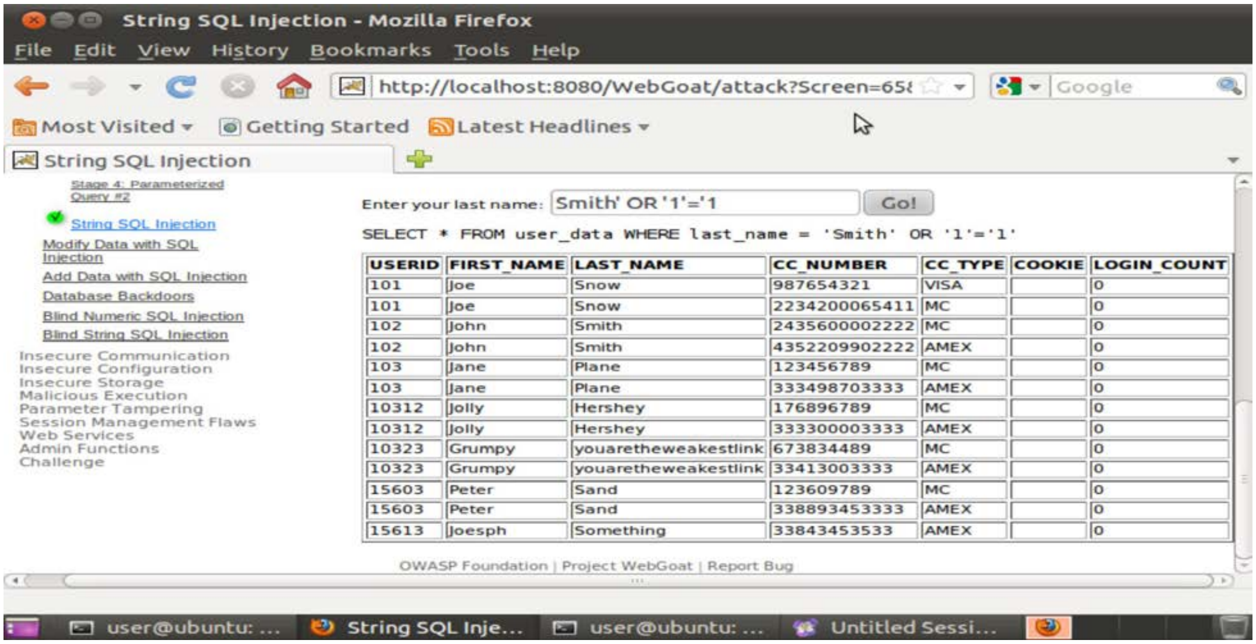
11. **How many entries have you obtained?**

    2.

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

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

13. Paste a screenshot of your results.



Enter your last name: Smith' OR '1'='1

```
SELECT * FROM user_data WHERE last_name = 'Smith' OR '1'='1'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
101	Joe	Snow	987654321	VISA		0
101	Joe	Snow	2234200065411	MC		0
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0
103	Jane	Plane	123456789	MC		0
103	Jane	Plane	333498703333	AMEX		0
10312	Jolly	Hershey	176896789	MC		0
10312	Jolly	Hershey	333300003333	AMEX		0
10323	Grumpy	youaretheweakestlink	673834489	MC		0
10323	Grumpy	youaretheweakestlink	33413003333	AMEX		0
15603	Peter	Sand	123609789	MC		0
15603	Peter	Sand	338893453333	AMEX		0
15613	Joesph	Something	33843453533	AMEX		0

14. 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.

15. 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.

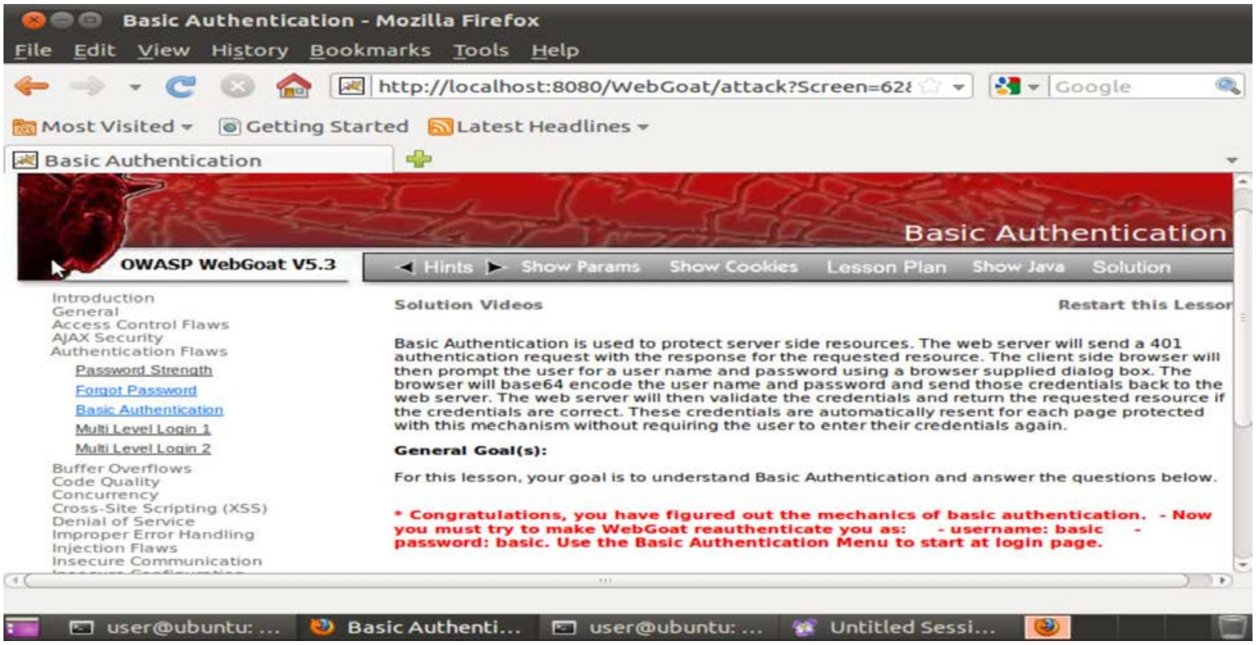
16. Write down the code here.

Z3Vlc3Q6Z3Vlc3Q=

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

guest:guest

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



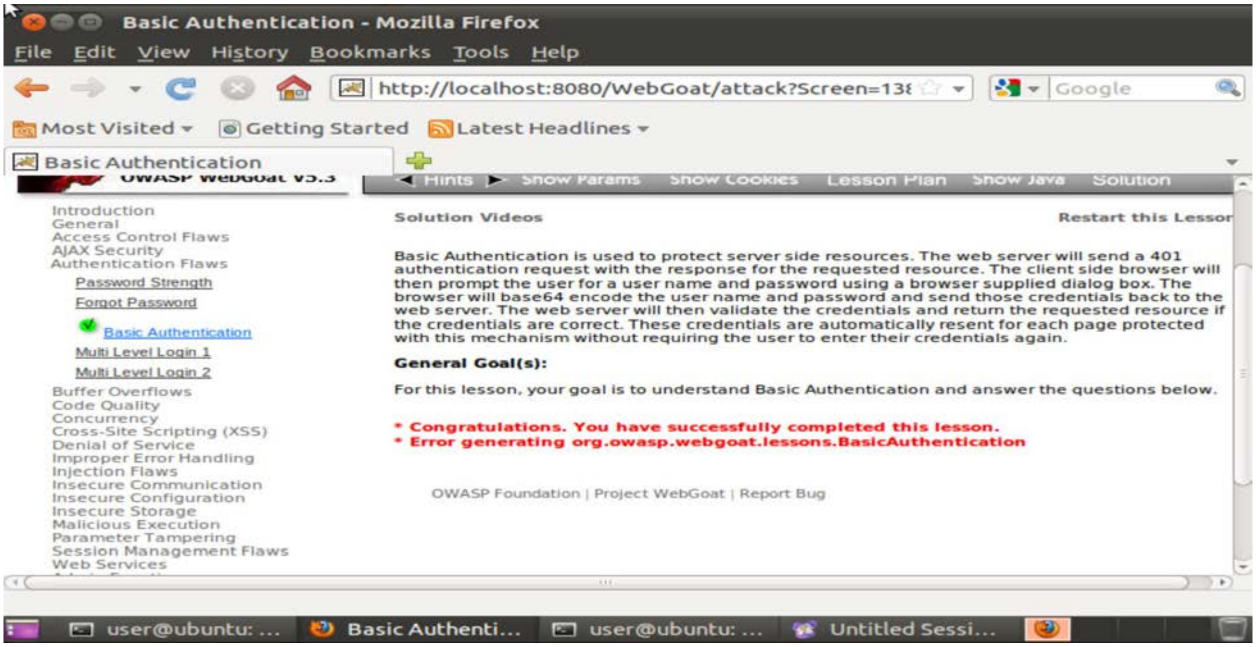
Basic Authentication is used to protect server side resources. The web server will send a 401 authentication request with the response for the requested resource. The client side browser will then prompt the user for a user name and password using a browser supplied dialog box. The browser will base64 encode the user name and password and send those credentials back to the web server. The web server will then validate the credentials and return the requested resource if the credentials are correct. These credentials are automatically resent for each page protected with this mechanism without requiring the user to enter their credentials again.

General Goal(s):

For this lesson, your goal is to understand Basic Authentication and answer the questions below.

* Congratulations, you have figured out the mechanics of basic authentication. - Now you must try to make WebGoat reauthenticate you as: - username: basic - password: basic. Use the Basic Authentication Menu to start at login page.

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



Basic Authentication is used to protect server side resources. The web server will send a 401 authentication request with the response for the requested resource. The client side browser will then prompt the user for a user name and password using a browser supplied dialog box. The browser will base64 encode the user name and password and send those credentials back to the web server. The web server will then validate the credentials and return the requested resource if the credentials are correct. These credentials are automatically resent for each page protected with this mechanism without requiring the user to enter their credentials again.

General Goal(s):

For this lesson, your goal is to understand Basic Authentication and answer the questions below.

* Congratulations. You have successfully completed this lesson.
* Error generating org.owasp.webgoat.lessons.BasicAuthentication

20. 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!