Burp Suite

Name: Alizeh Jafri

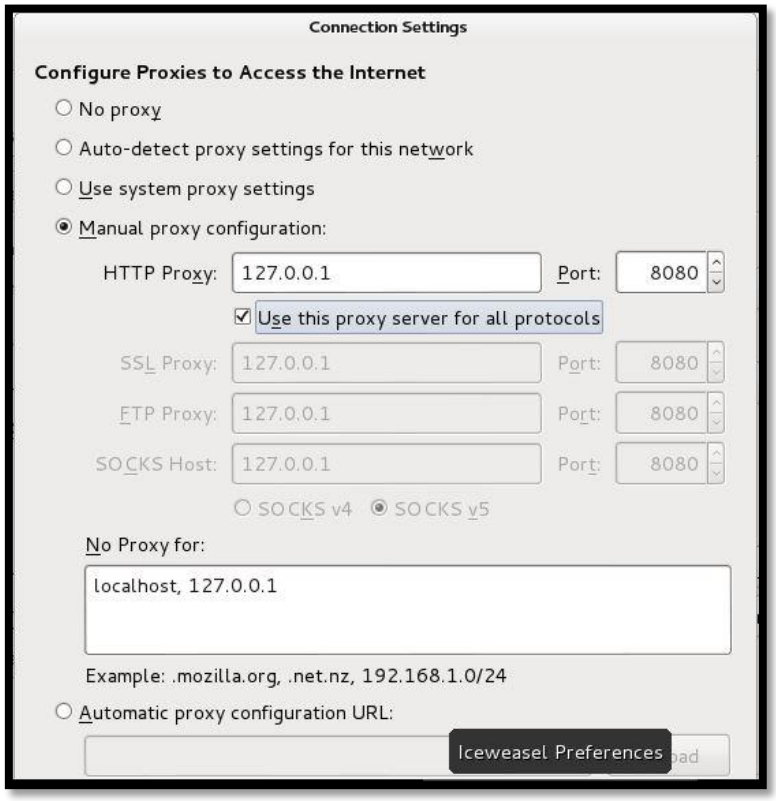
Task 1: In the web server hosted by your Windows 7 virtual machine, the usernames and

passwords of all users for the Bookservice website are stored in an XML file, whose path is "C:\inetpub\wwwroot\Book\AuthInfo.xml".

In this task, you need to figure out the content of the file "AuthInfo.xml".

Firstly, I opened kali linux and clicked on the path applications → kali linux → web applications → application fuzzers → burpsuite.

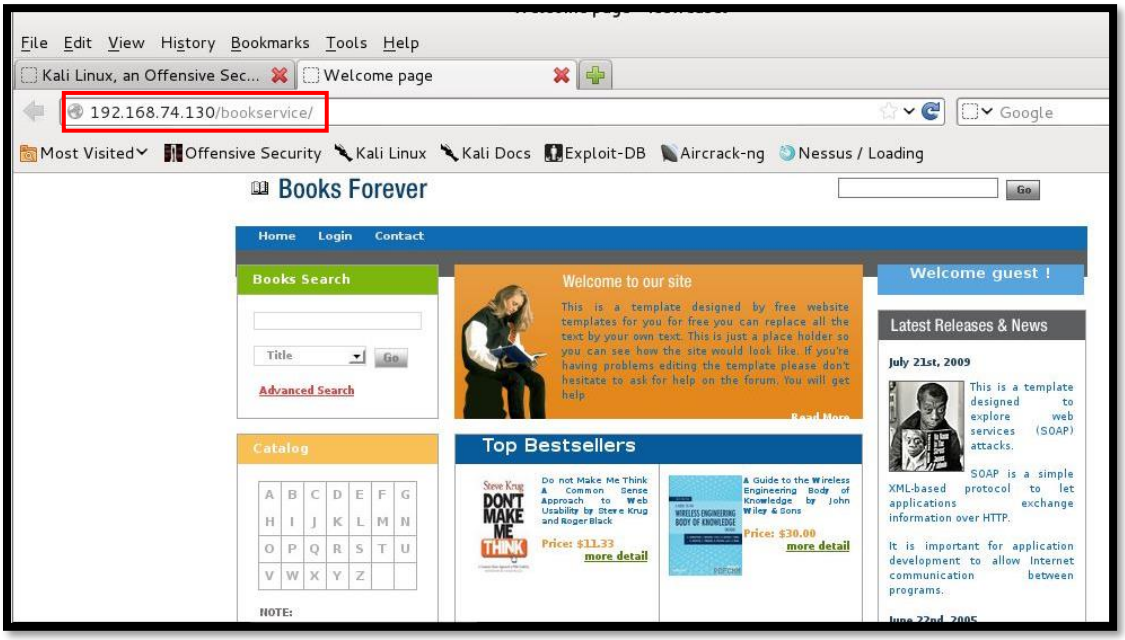
Next, I needed to tell my browser in kali to proxy the web traffic via Burp suite. For that I changed the settings shown below:



Then, I clicked the forward button:

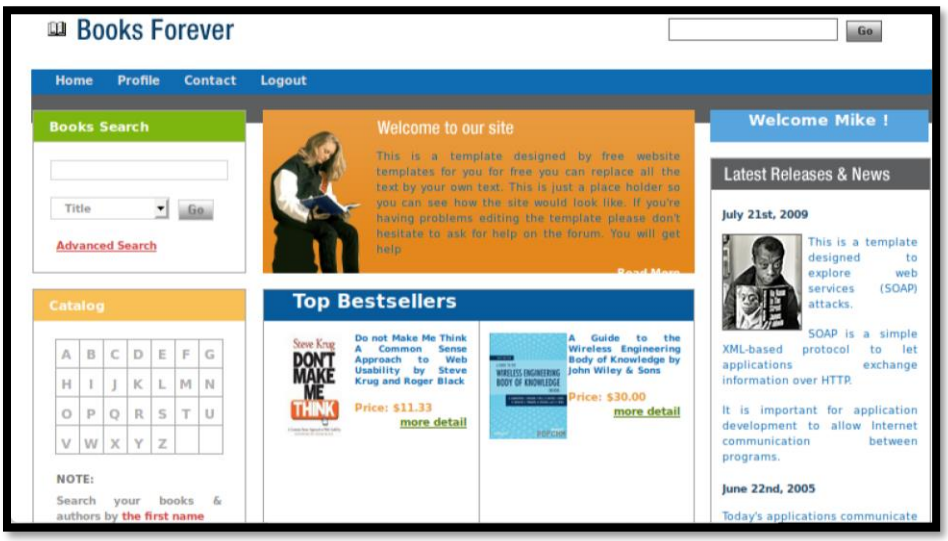
And then, I typed the URL to make sure the iceweasel will proxy all the traffic via burp suite. After

entering the URL Bookservice on the target windows 7, the webpage opened:



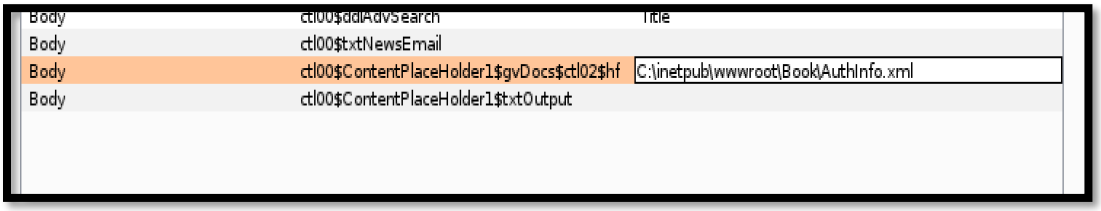
I created Mike's account by clicking on new user and logged in. Then I performed "SQL INJECTION" for user name and for password I put. Next, I went to View Newsletters and clicked it and forwarded the request Burp Suite.

I can view Mike's welcome page:

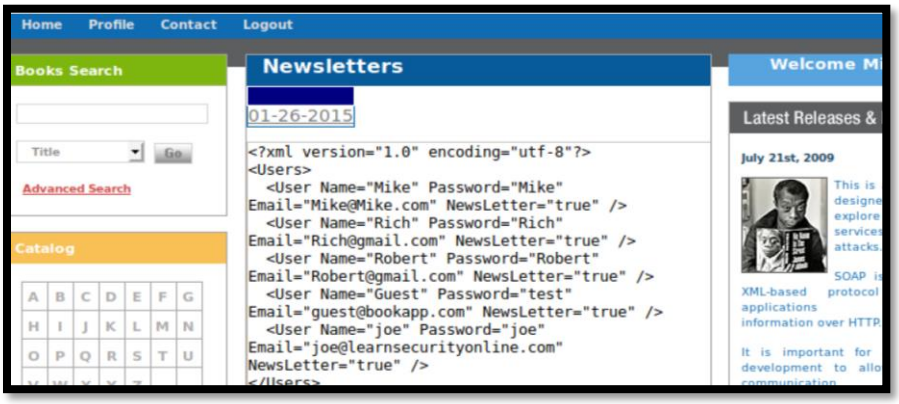


It is empty in the newsletter box:

I changed the request in Burp Suite to “C:\inetpub\wwwroot\Book\AuthInfo.xml”.



Got this output:

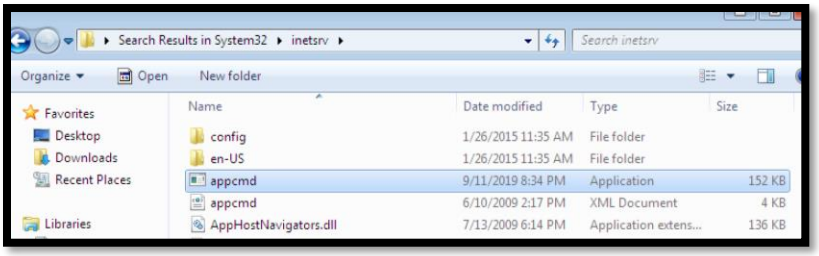


Task 2: As shown in our lecture, we are able to utilize the "Newsletter Signup" filed in the Bookservice website to execute your commands. In this task, you need to use one input in the "Newsletter Signup" filed to create a folder called "example" under C:\, and copy the file "appcmd.xml" in "c:\windows\system32\inetsrv" to the example folder you created.

Hint: you can use multiple & to separate and execute multiple commands at the same time.

alizeh@jafri.com & I used mkdir c:\ example & Copy c:\windows\system32\inetsrv\appcmd.xml" "C:\example.

Next, from windows 7, I checked if the file is present as shown in the below screen shot:



Task 3: Suppose we have a website that has three fields for login:

username:_____
email:n ' ' or 1=1 –'_____
password: _____

The authentication for login is based on the following query

SELECT id from Users where (username = '$user' or email = '$email') and pass='$password';

How cloud you bypass the authentication by **only entering** inputs in the email field? Hint: try to skip the checking of password using the "Comments out" syntax in SQL

If you are not familiar with SQL, you can get more idea at: https://www.w3schools.com/sql/

What to submit:

- Your input for the email field

My input for the email field would be :

Email input : 'or 1=1--