



Prince Sultan University
College of Computer and Information Sciences
CYS401 – Fundamentals of Cybersecurity

Practical 7: Hacking Web Application - Perform Parameter Tampering using Burp Suite in Kali Linux

***Disclaimer:** All the labs in this course are prepared for educational purposes. we can't harm anyone all the commands are done within our own system and network.*

Instructions:

- a. The assignment must be done individually.
- b. The assignment is of 10 marks. You'll have to demonstrate the assignment on your PC OR submit a report. For each assignment, there will be an assessment.
- c. The assignment should preferably be done on a laptop.
- d. Required Tools: Kali- Linux, Burp Suite (available in kali Linux).

Lab Details:

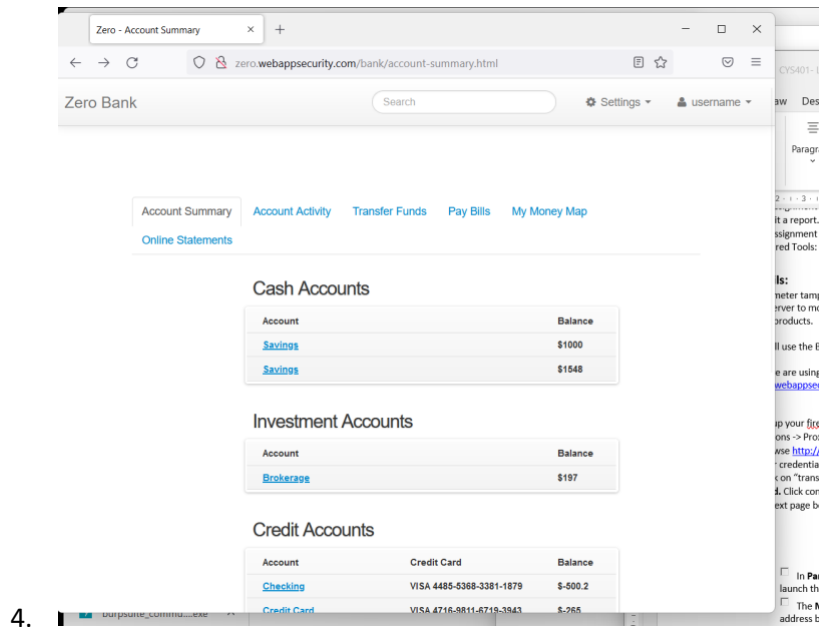
A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

Here, we will use the Burp Suite tool to perform parameter tampering.

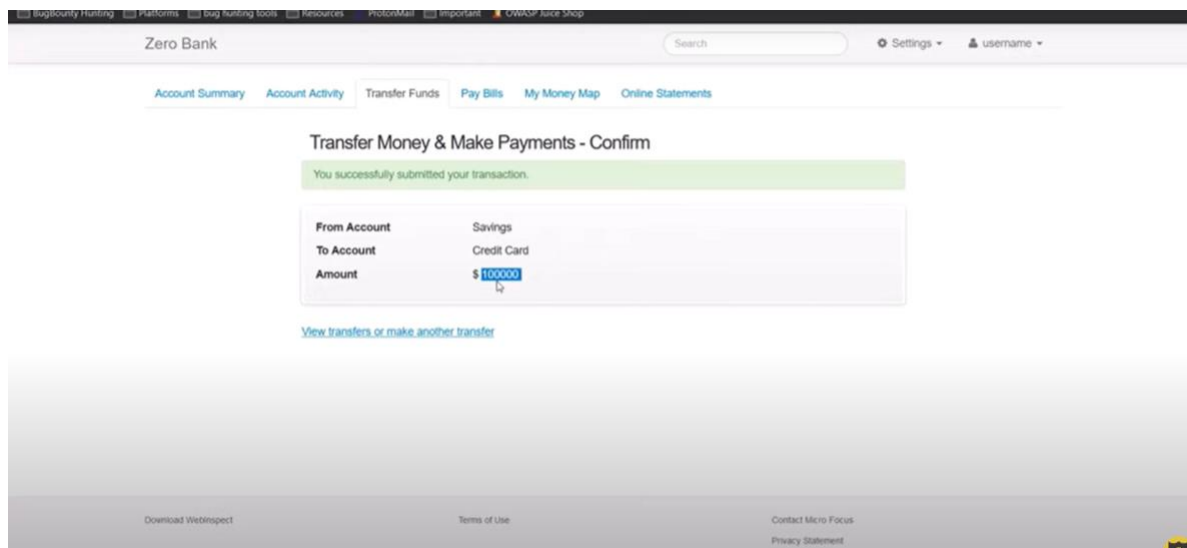
In this lab we are using a buggy web application available on internet i.e., zero bank website
http://zero.webappsecurity.com/login.html?login_error=true

Steps:

1. Setup your firefox proxy in order to allow it to work with burpsuite. Firefox-> settings -> options -> Proxy -> set proxy -> 127.0.0.1 and port -> 8080, Check box -> Sock 5.
2. Browse http://zero.webappsecurity.com/login.html?login_error=true in firefox and enter user credentials: login = username, Password = password. Click signin.
3. Click on "transfer funds" tab. Keep **From Account** as it is and change **To Account** to **Credit Card**. Click continue button



5. In next page before clicking **Submit**. Go to Burp suite -> click “**Intercept is on**”. Click submit in firefox. Now you intercept the traffic. In Burp Suite, tamper the payment amount to \$10000 and click on **forward** button. You will see the tampered value on the bank website.

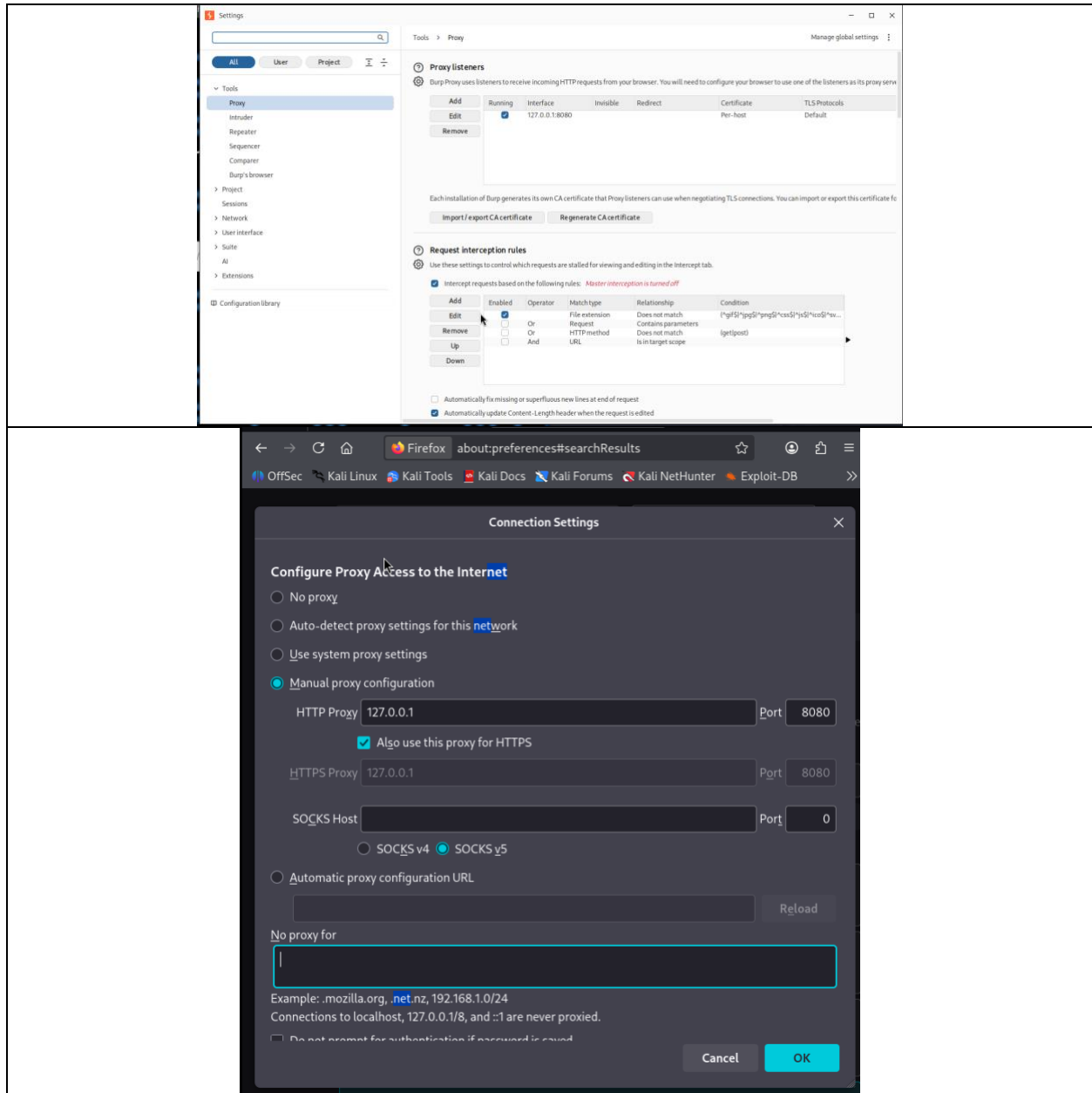


Bonus Marks:

Task:

Find your own vulnerable site that runs on “http”, perform the same lab on that site.

You Successfully Tamper the Value and Paid your Credit Card Bill 😊



For the bonus: