# Lab 5: VM and Burp Suite

Overview

The objective of this lab is to install VM and install windows machine on the VM. After the successful installation of windows machine, we will download various security tools inside the windows machine.

a. Install Virtual box and Windows machine

I installed oracle virtual box and downloaded windows iso image. From the VM menu, I created new windows machine with appropriate settings, and renamed it with my GMU id as shown in the screenshot below. My windows VM name is 'dachary' as we can see in the screenshot.
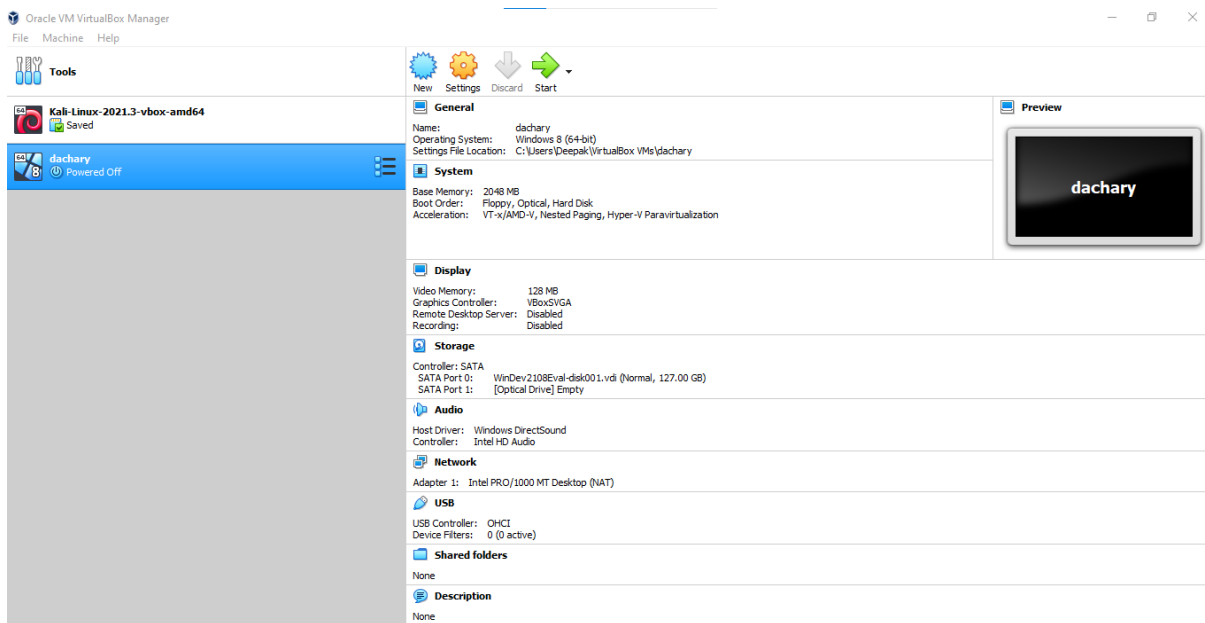

b. Installation of Java JDK

After installing the windows machine on VM, I downloaded the Java JDK following the instruction provided in the link. I set the correct path for that, and finally checked the Java version which is 17.0.1 as shown in the screenshot below.
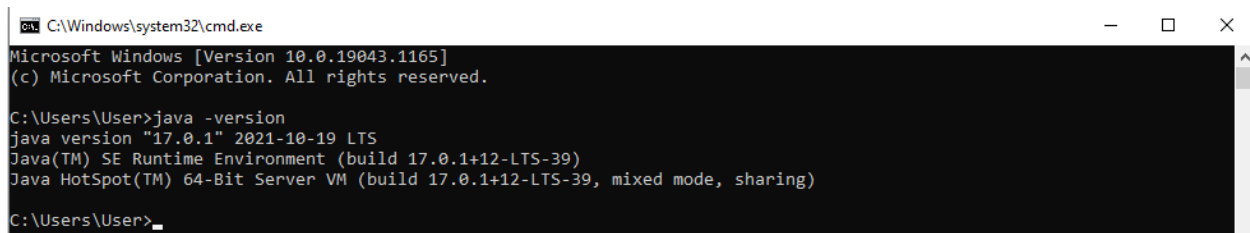

c. Burp Suite installation

Then, I downloaded the Burp Suite and installed it. The launch of the burp suite is shown in the screenshot below.
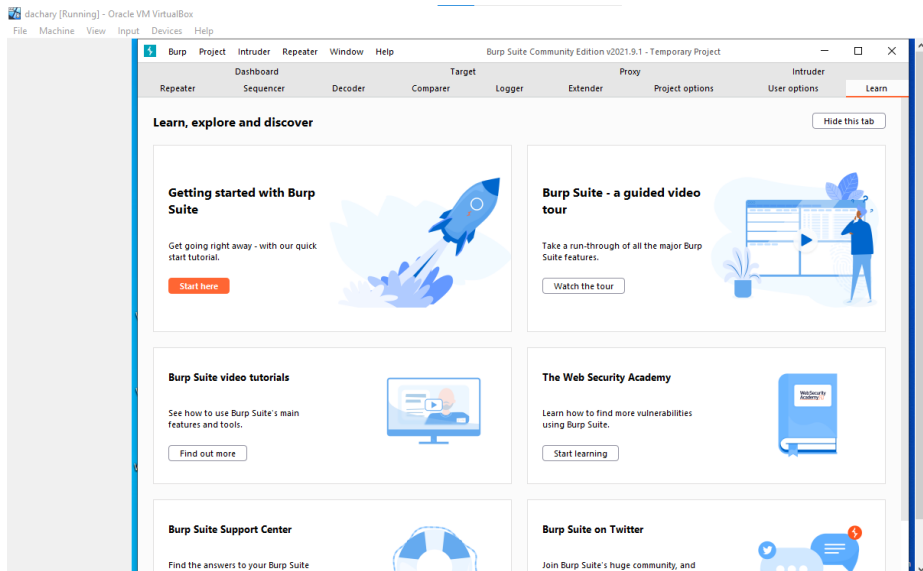
d. Intercept Request

I went to the Proxy > Intercept tab and clicked Open Browser. This launches Burp's embedded Chromium browser, which is preconfigured to work with Burp right out of the box. I positioned the windows so that I can see both Burp and the browser. I made sure the intercept is on. Using the embedded browser, I tired visiting https://portswigger.net and observed that the site doesn't load. Burp Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server. I saw this intercepted request on the Proxy > Intercept tab. After I pressed the forward button for couple times the page loaded as the intercepted request is shown in the screenshot below.
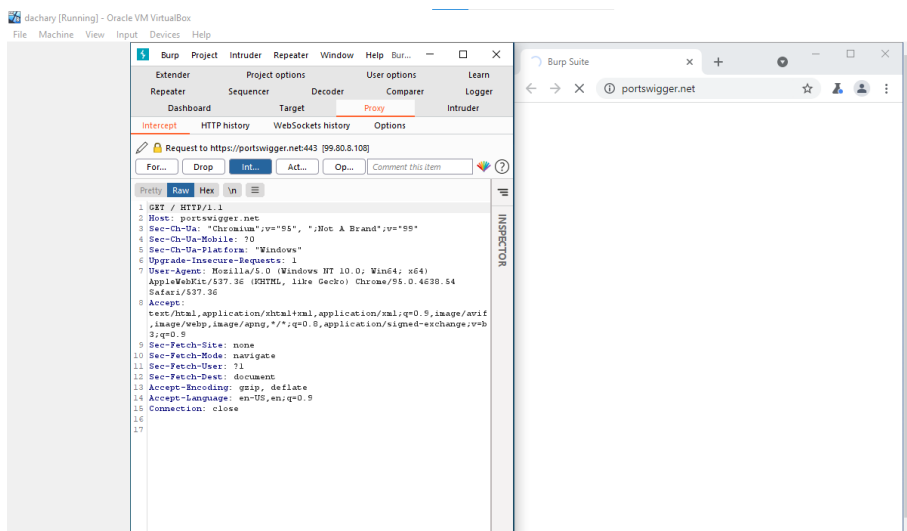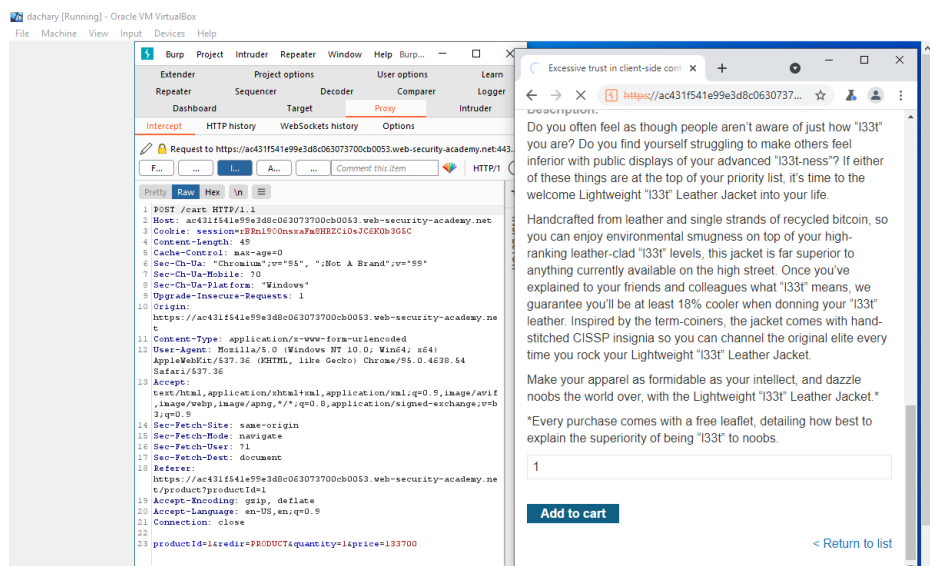

e. View HTTP History

In Burp, I went to the Proxy > HTTP history tab. Here, we can see the history of all HTTP traffic that has passed through Burp Proxy, even while interception was switched

off. WE can see all the entries in the screenshot, if we click one of the entries in the history to view the raw HTTP request, along with the corresponding response from the server.
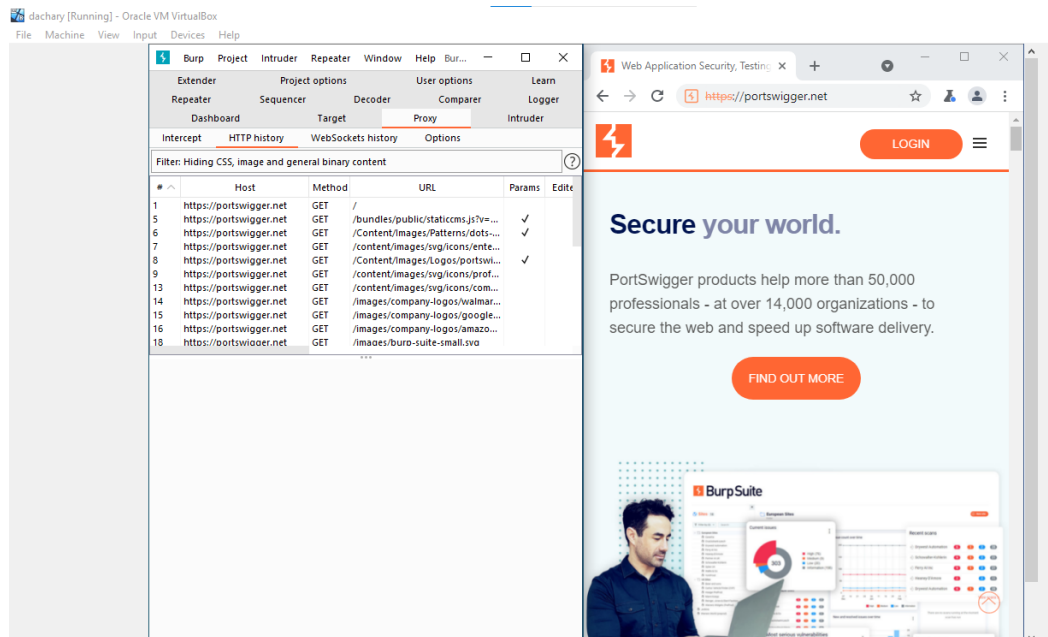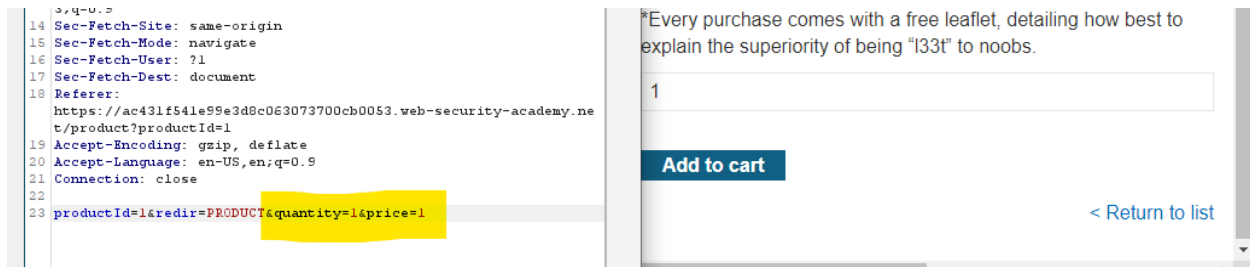

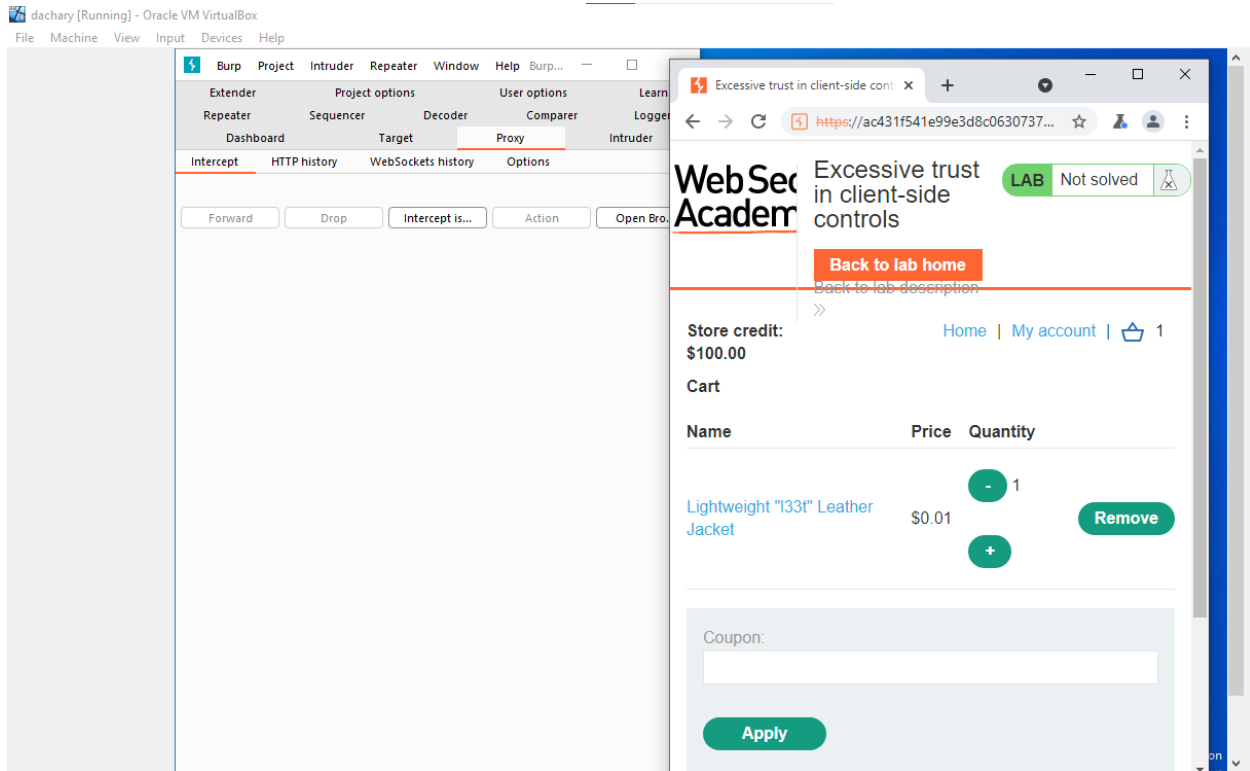
f. Modifying the Request

The screenshot below shows the request before we modify content of the request, which shows that the price is 133700.

Then, I modified the price = 1, as shown in the screenshot below.

```
3,q-0.5
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
   https://ac431f541e99e3d8c063073700cb0053.web-security-academy.ne
   t/product?productId=1
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 productId=1&redir=PRODUCT&quantity=1&price=1
```

*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "l33t" to noobs.

1

Add to cart

< Return to list

The cart, after I forwarded the packet is shown in the screenshot below, which is 0.01.

Conclusion

This way, we successfully downloaded Virtual Box, and then installed the windows machine. We also downloaded all different tools inside the windows machine, including Java JDK and Burp Suite. I ran the burp suite and was able to see all the http request and finally was able to modify request to make the price lower than it appears in the website.