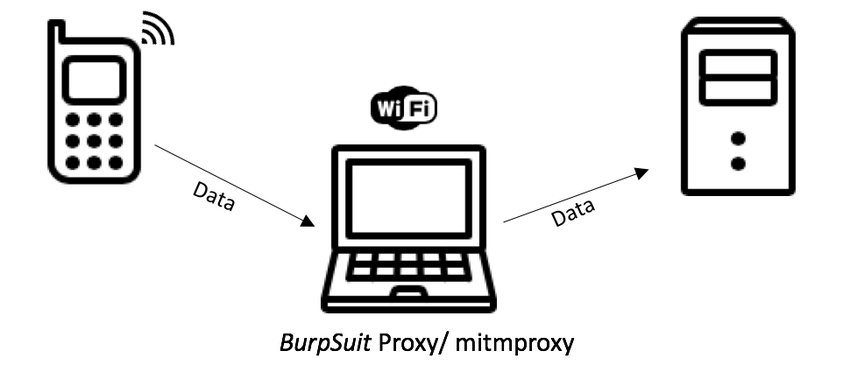
**BURP SUITE**

* Burp Suite is a java application that can be used to secure or penetrate web applications. The suite consists of different tools, such as a proxy server, a wide spider, intruder and repeater.
* Burp suite works as a middle-man.



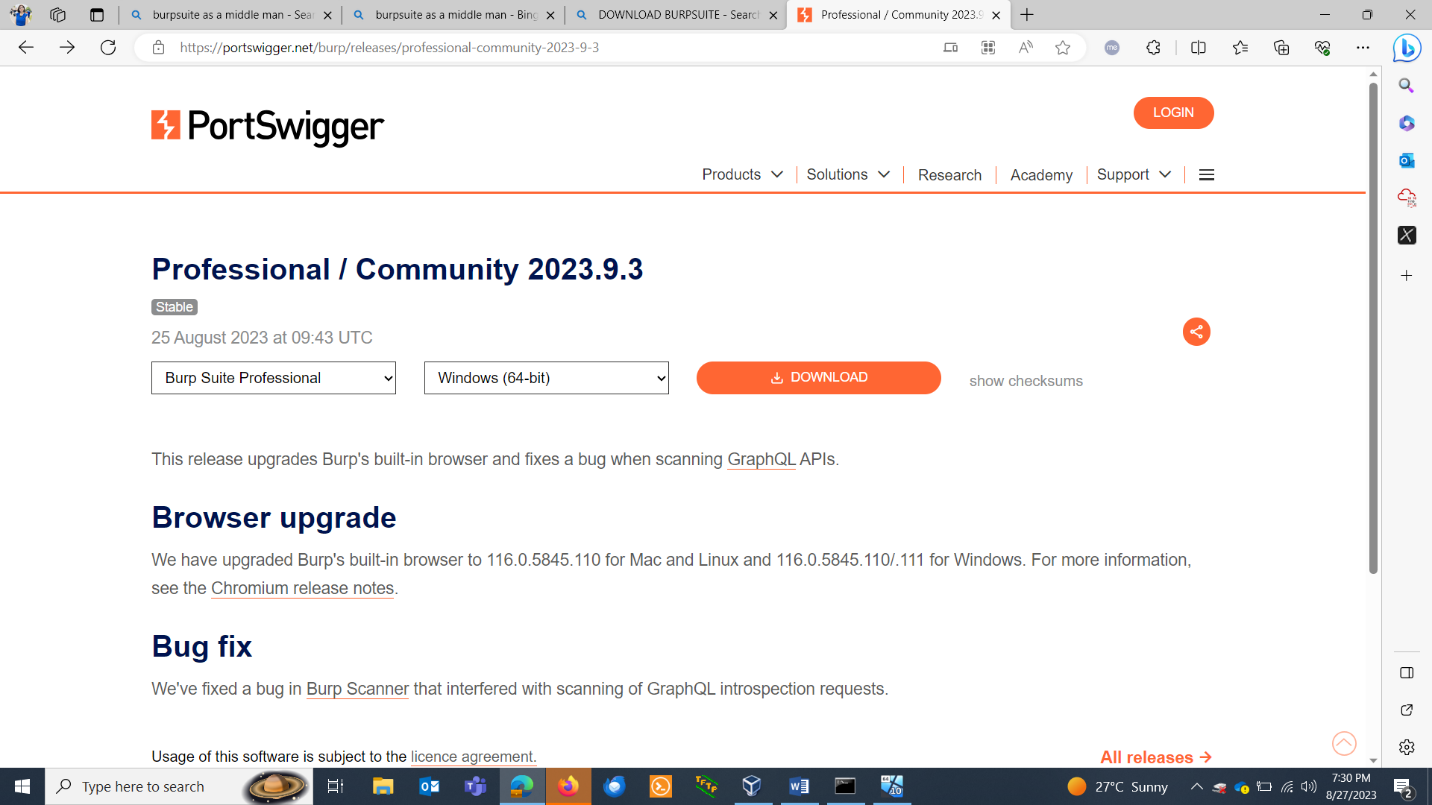
USES OF BURP-SUITE:

* Monitoring websites.
* Monitoring and analyzing requests.
* Finding vulnerabilities

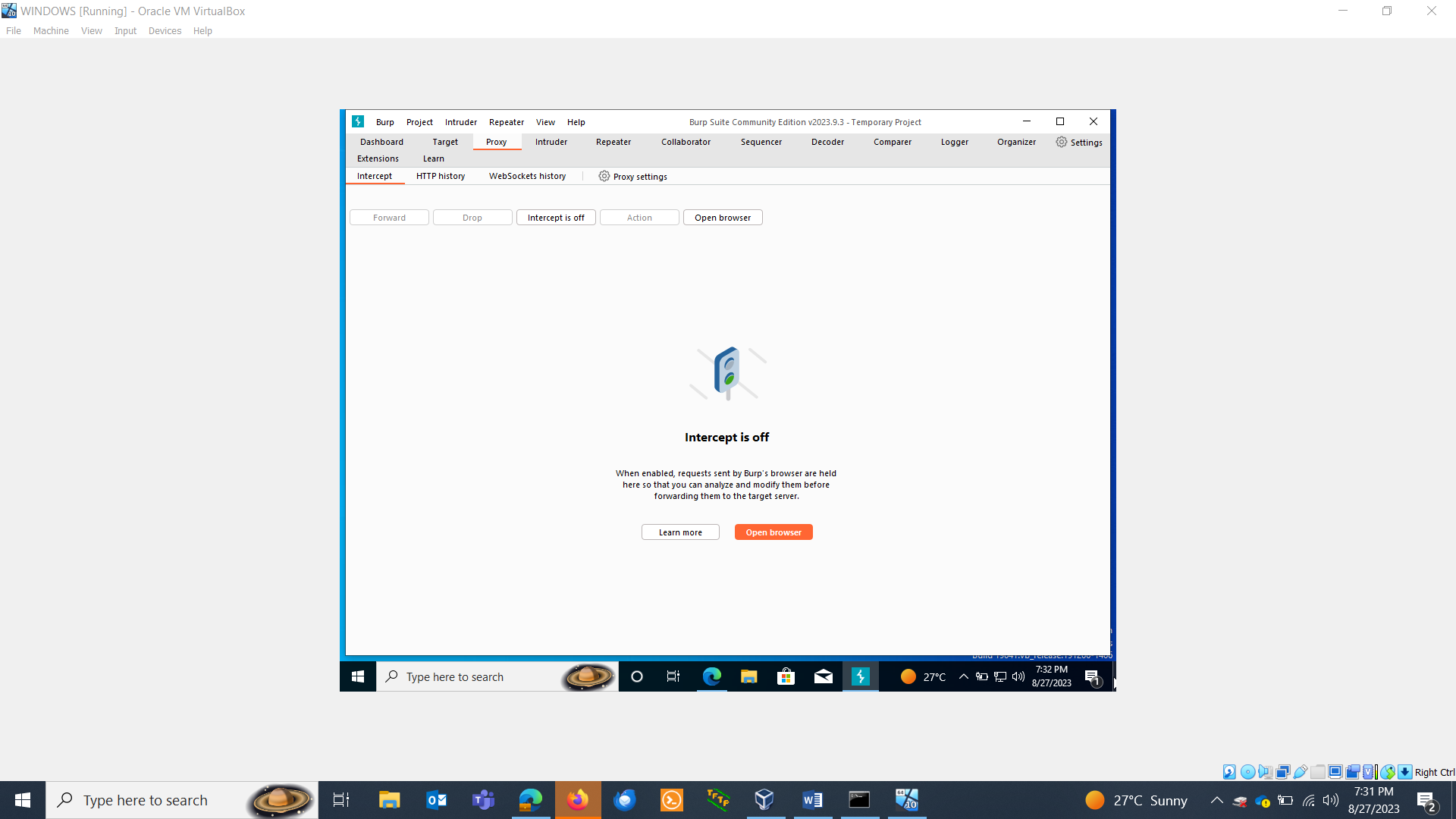
It will only run in java -installed system.

BURP SUITE INSTALLATION:

[Professional / Community 2023.9.3 | Releases (portswigger.net)](https://portswigger.net/burp/releases/professional-community-2023-9-3)

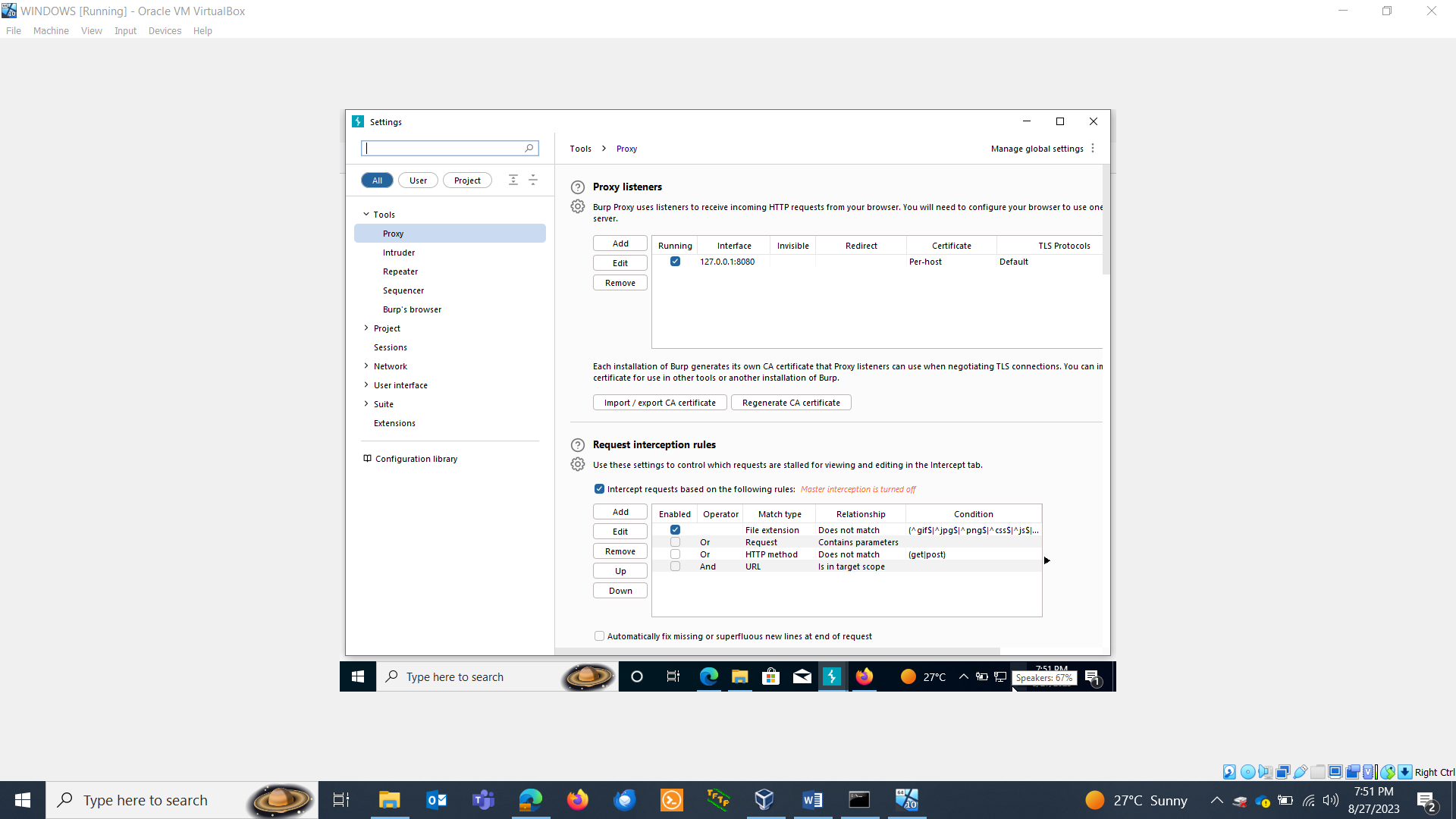


Initial screen:



Lets go to proxy settings and set burpsuite on some ports.

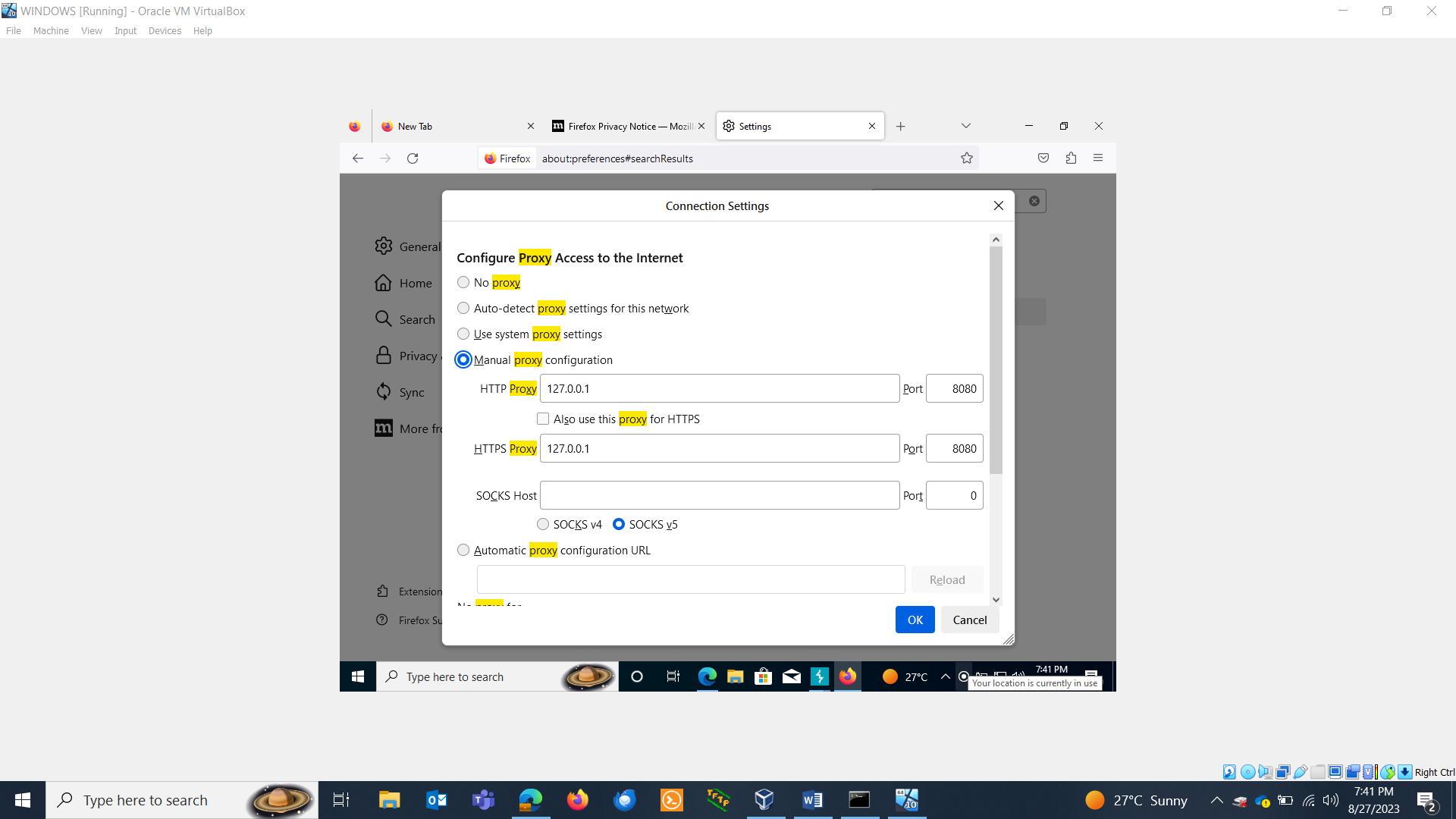
By default proxy is at 8080 port.



Download firefox.

Lets install install proxy on it.

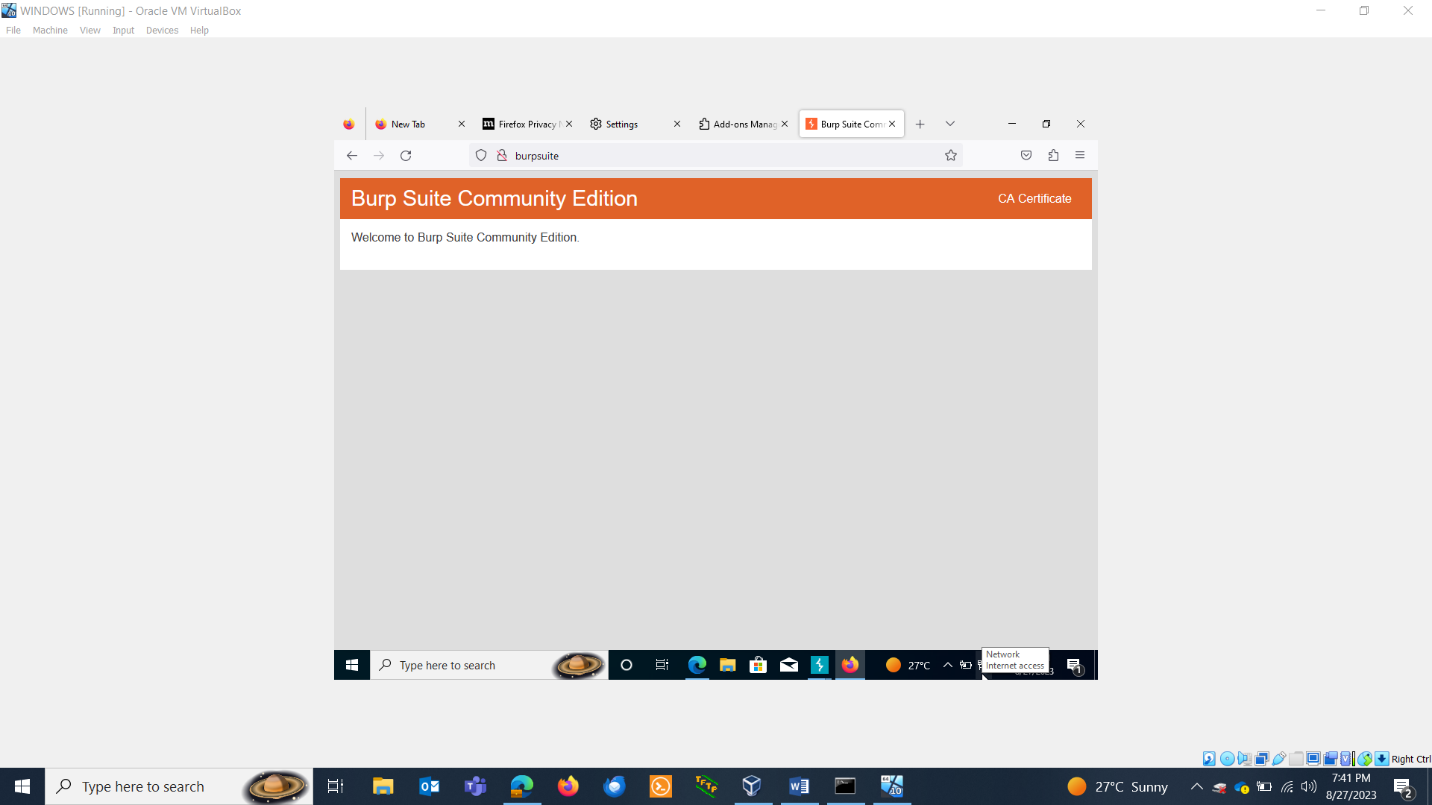
Go to settings> proxy. Set proxy at the same ip address.



You also need to download certificate.

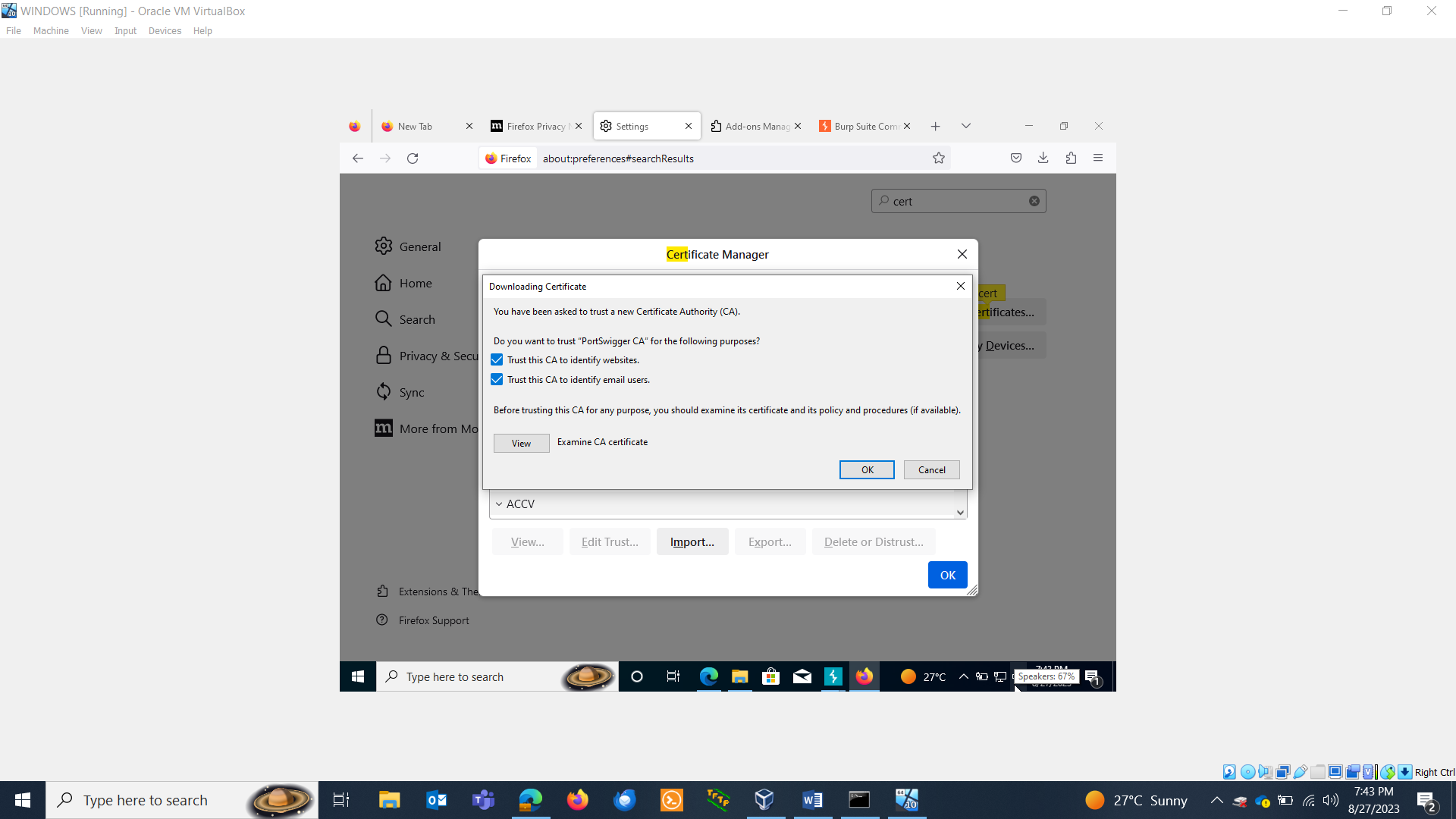
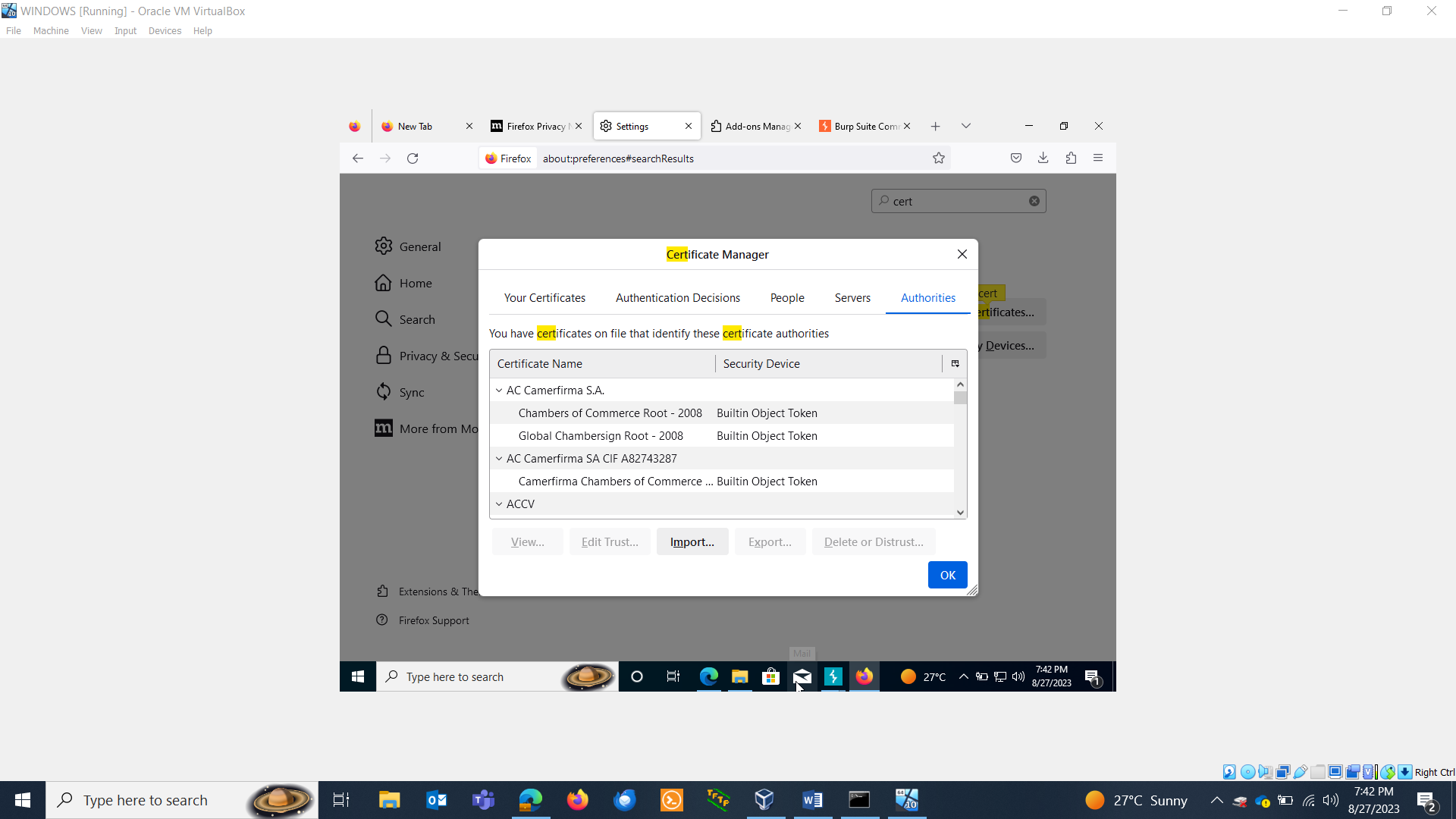
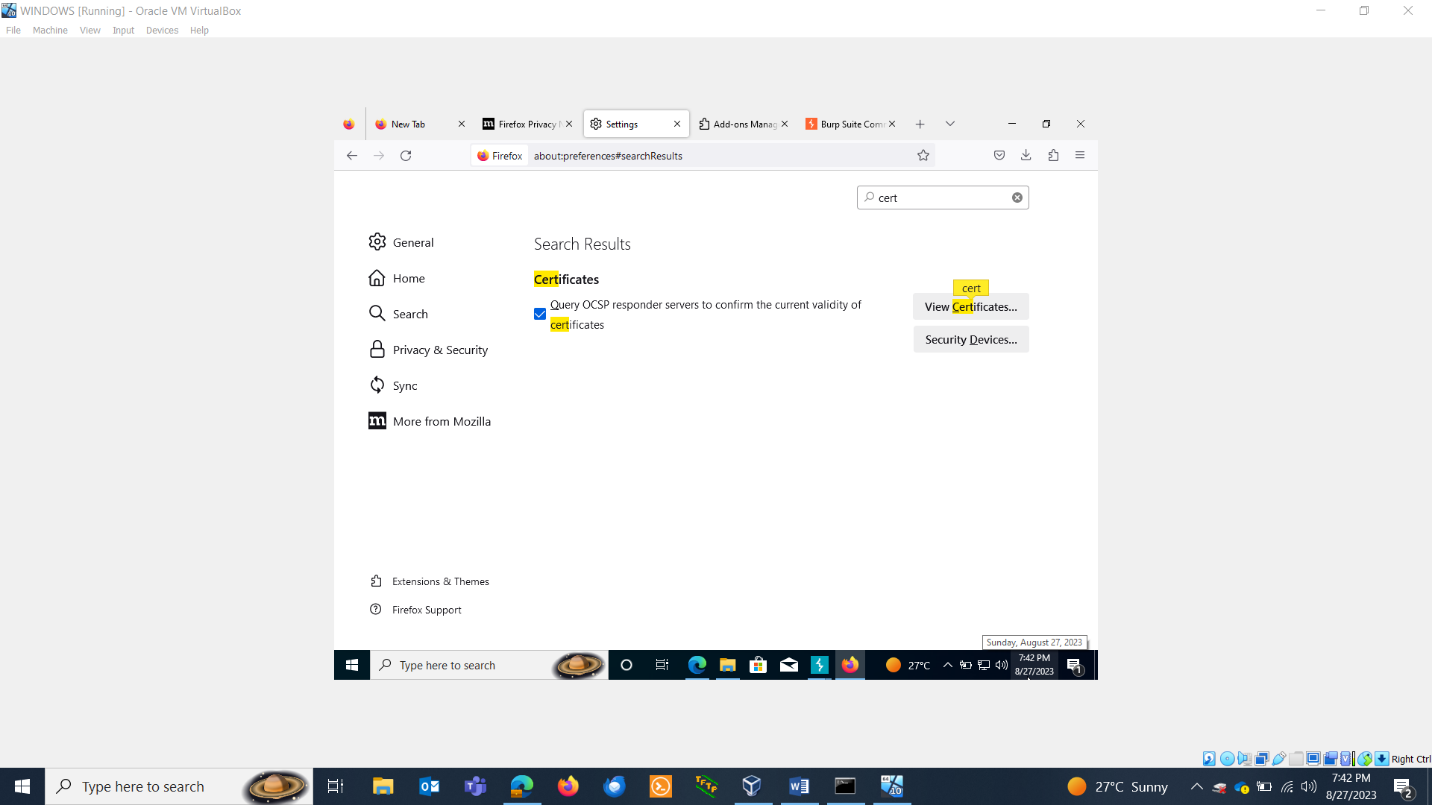
Type : http:burpsuite

Click on CA certificate and download the certificate.



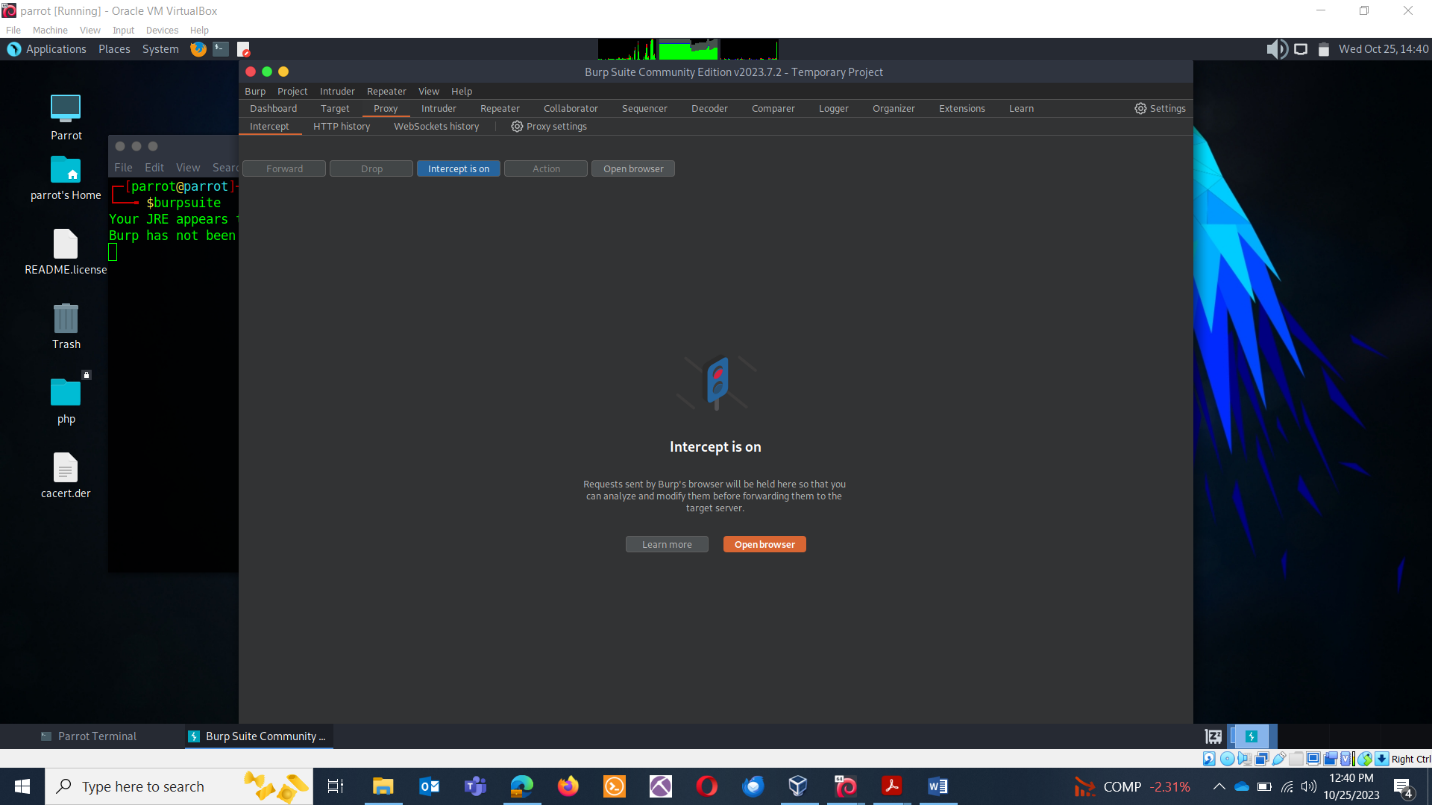
Now install it in the browser:

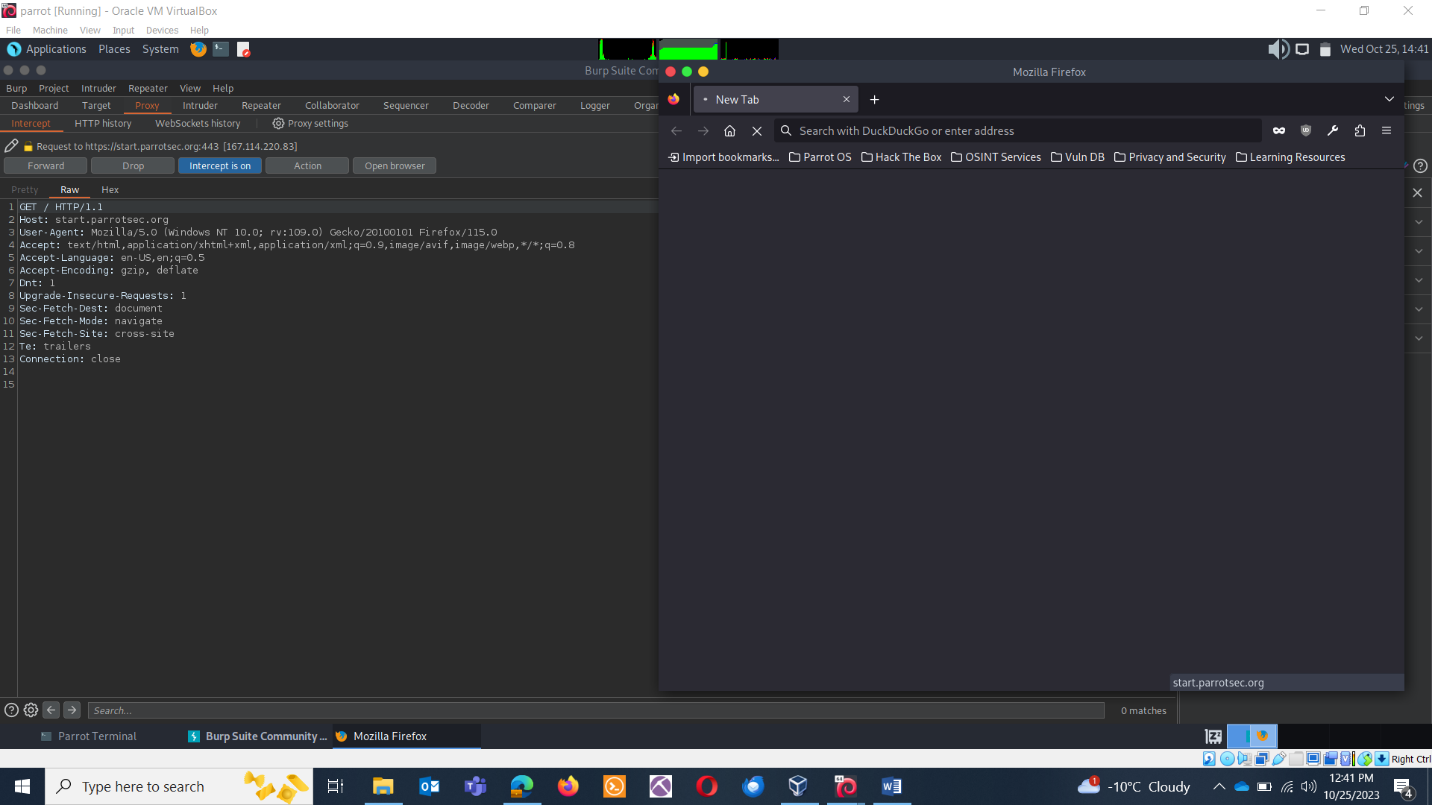
Settings> certificate> view certificate>import the certificate



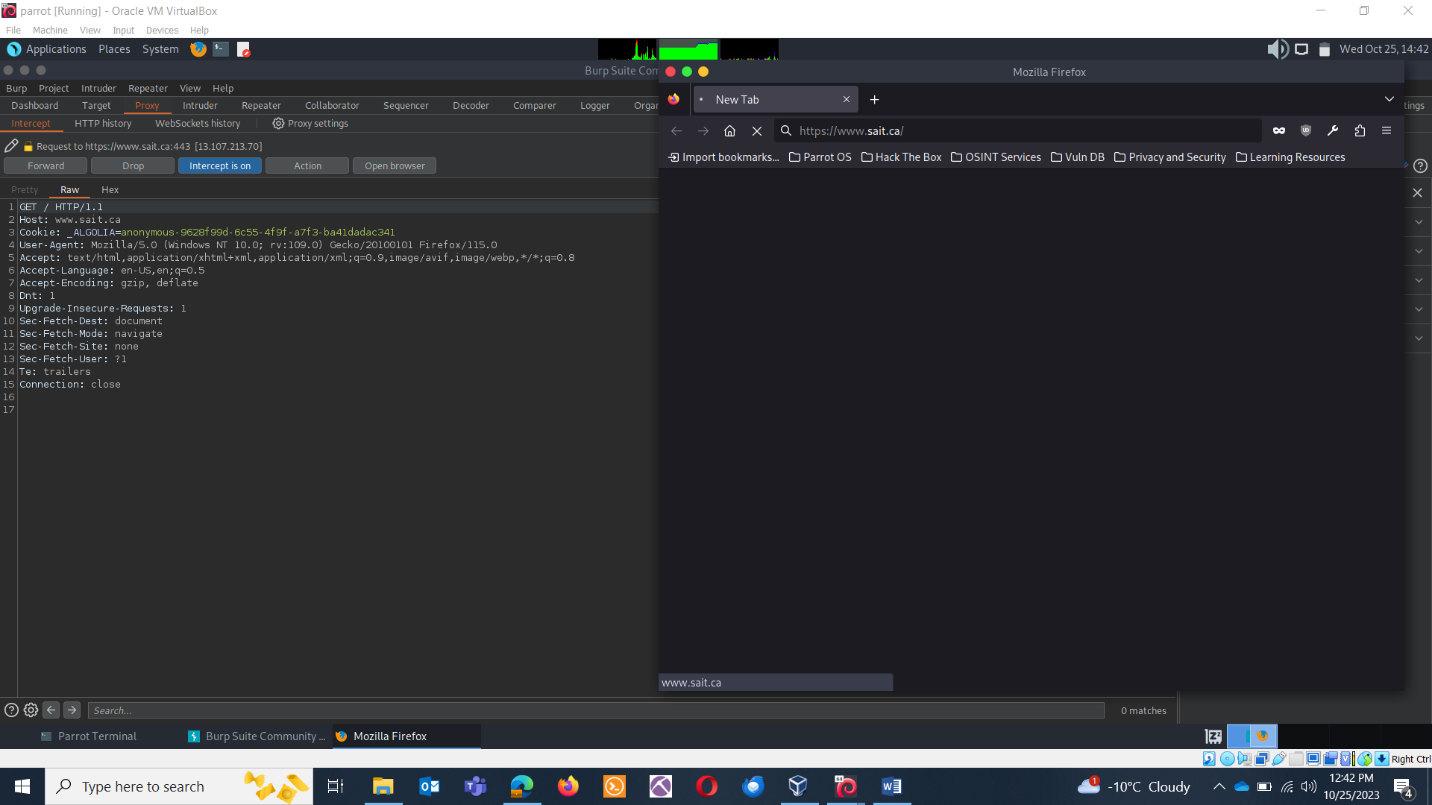
INTERCEPTING TRAFFIC:

* Set proxy in browser.
* Turn the intercepter on.

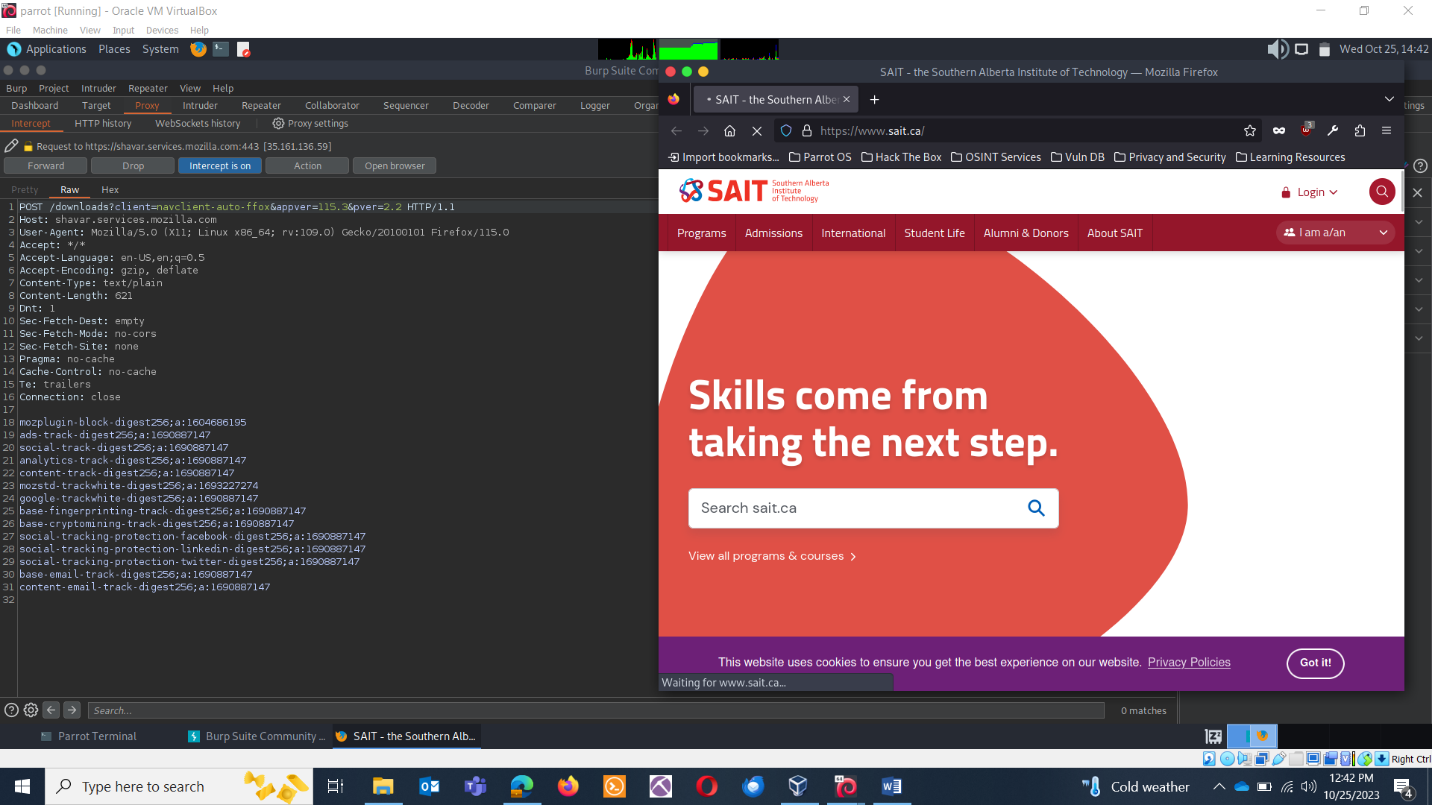




Forward the traffic.



Forward the traffic.



HTTP & HTTPS IN BURPSUITE

* HTTP stands for hyper text transfer protocol and is used to transfer data across the Web.
* The default port is TCP 80.
* HTTP is a stateless protocol, meaning the server isn’t required to store the session information, and each request is independent of the other.
* Sessions are maintained by the cookies.
* Two main parts:
  + **Request:** A command or request + optional header + optional body content
  + **Response:** A status code + optional headers + optional body content



**HTTP REQUEST:**

GET(Method) /(Path) HTTP/1.1(Version of protocol)

Host : developer.mozilla.org(Headers)

Accept-Language: fr(Headers)

HTTP METHODS:

* GET: the GET method requests a representation of the specified resource. Requests using GET should only retrieve data.
* HEAD: the HEAD method asks for a response identical, to a GET request, but without the response body.
* POST: The POST method submits an entity to the specified resource, often causing a change in state or side effects on the server.
* PUT: the PUT method replaces all current representations of the target resource with the request payload.

SET UP JUICE SHOP: DIY

Proxy: Understand how to configure Burp Suite as a proxy to intercept and analyze HTTP requests and responses.

Repeater: Practice sending and modifying individual requests for testing.

Intruder: Explore the tool for performing automated attacks, such as brute force or fuzzing.

**BURPSUITE REPEATER**

In Burp Suite, the "Repeater" is a powerful and versatile tool used for manual testing and analysis of HTTP requests and responses.

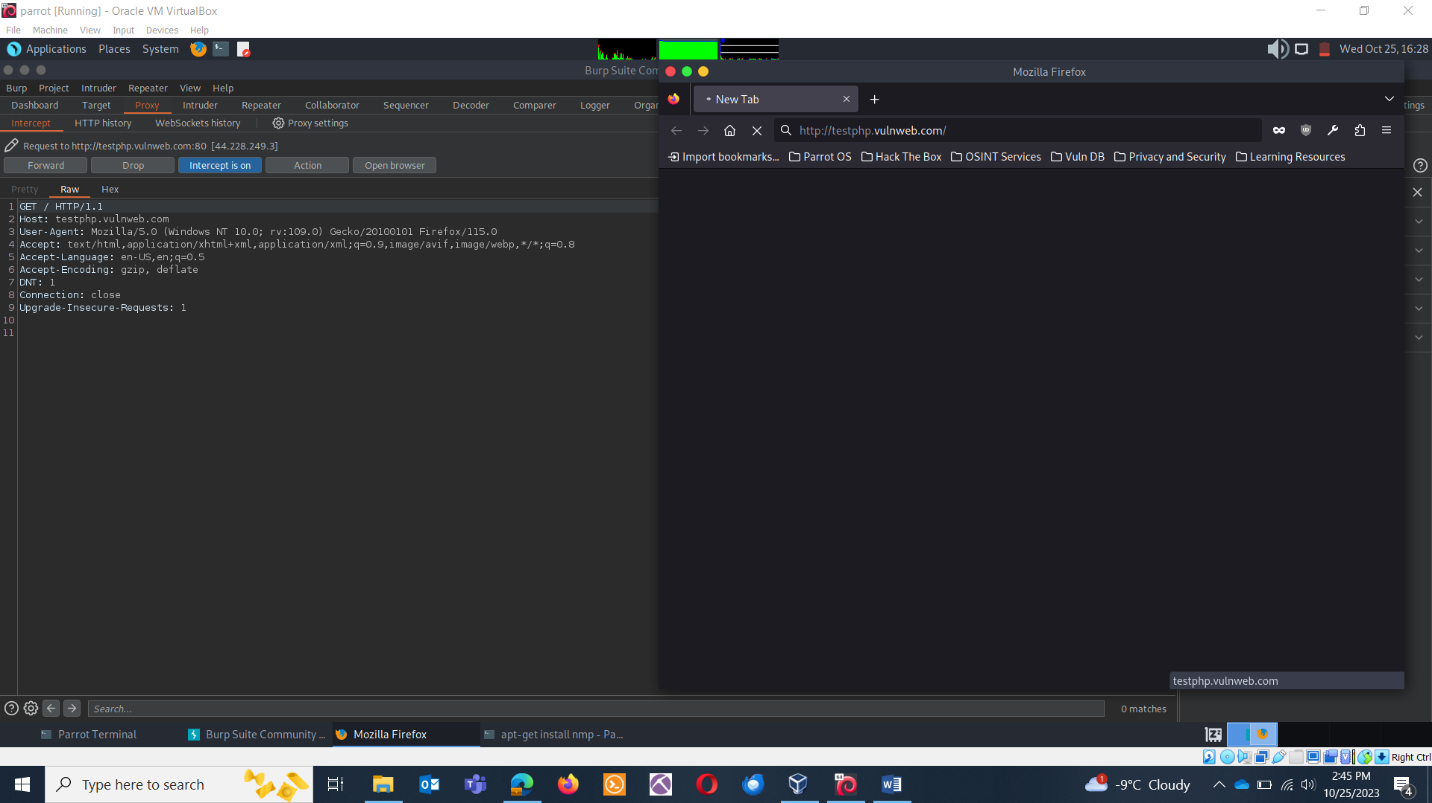
**1. Intercept and Modify Requests:** When you're using Burp Suite's proxy or other interception features, you can capture HTTP requests as they are sent to the target web application. The Repeater tool allows you to intercept and modify these requests before they reach the server. This is extremely useful for testing various aspects of web applications, such as input validation, authentication, and session management.

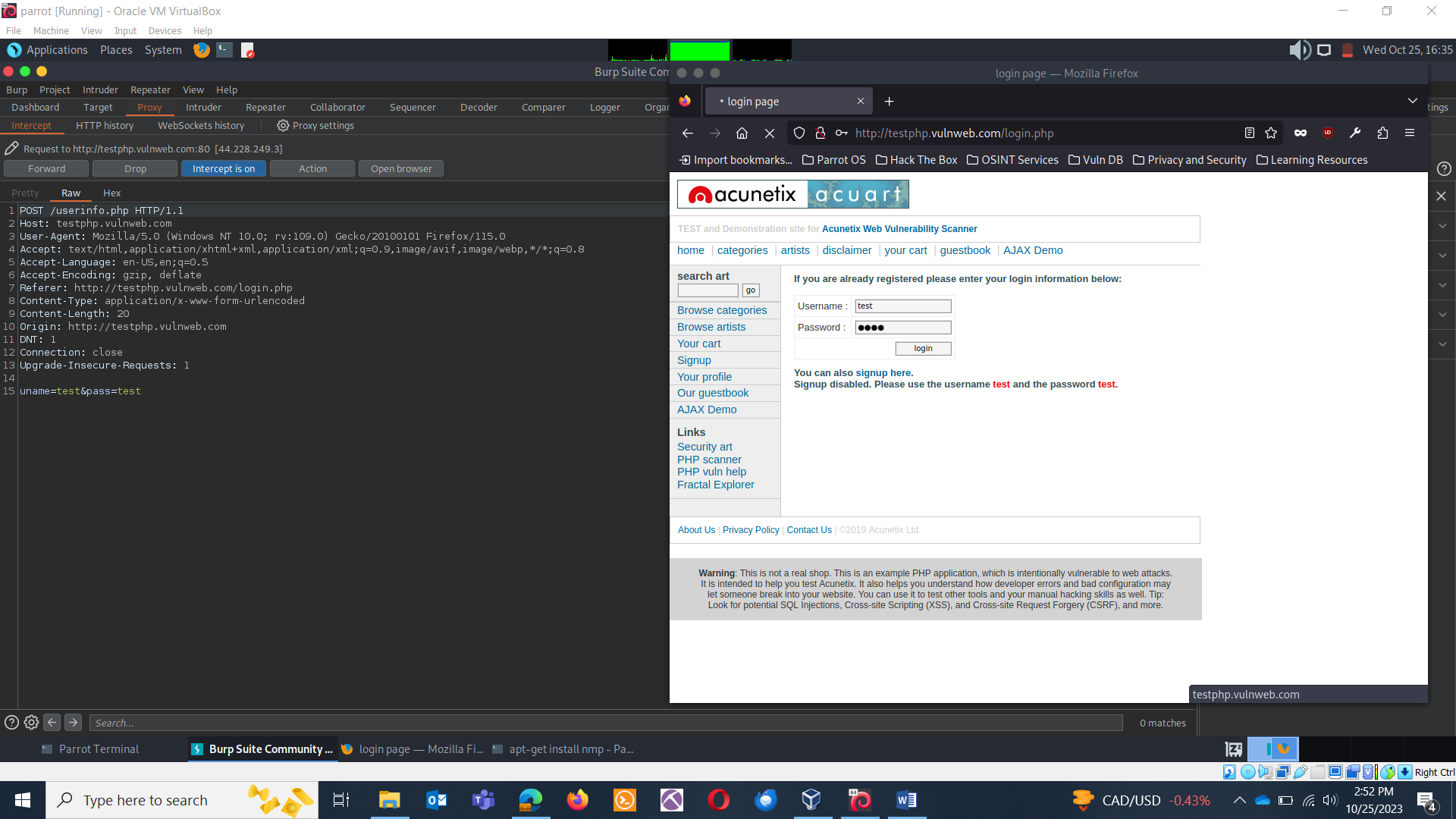
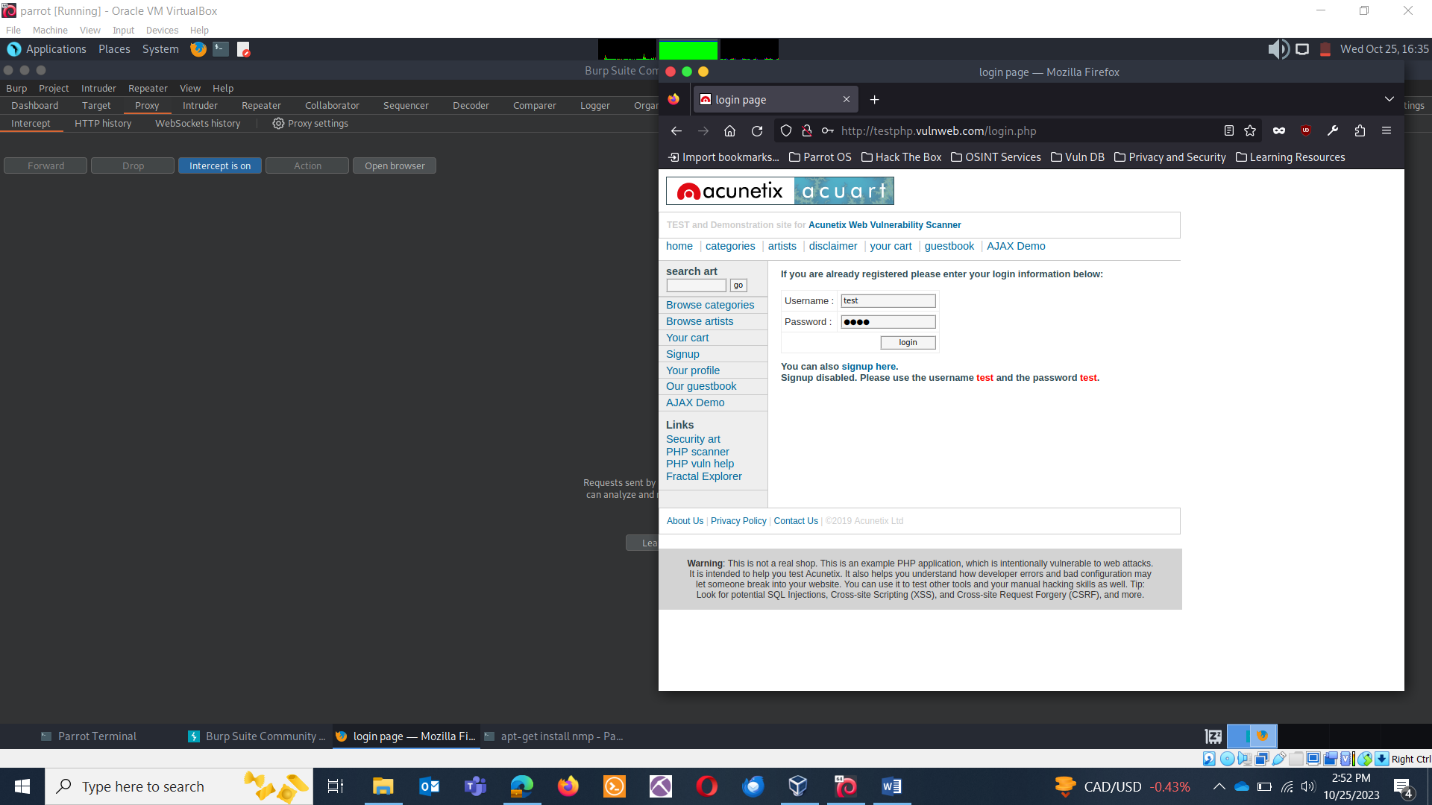
**2. Repeat and Reanalyze:** With the Repeater tool, you can resend intercepted requests multiple times for in-depth testing. You can make small changes to the request parameters, headers, or payloads and observe how the application responds. This iterative process is helpful for identifying vulnerabilities and security issues.

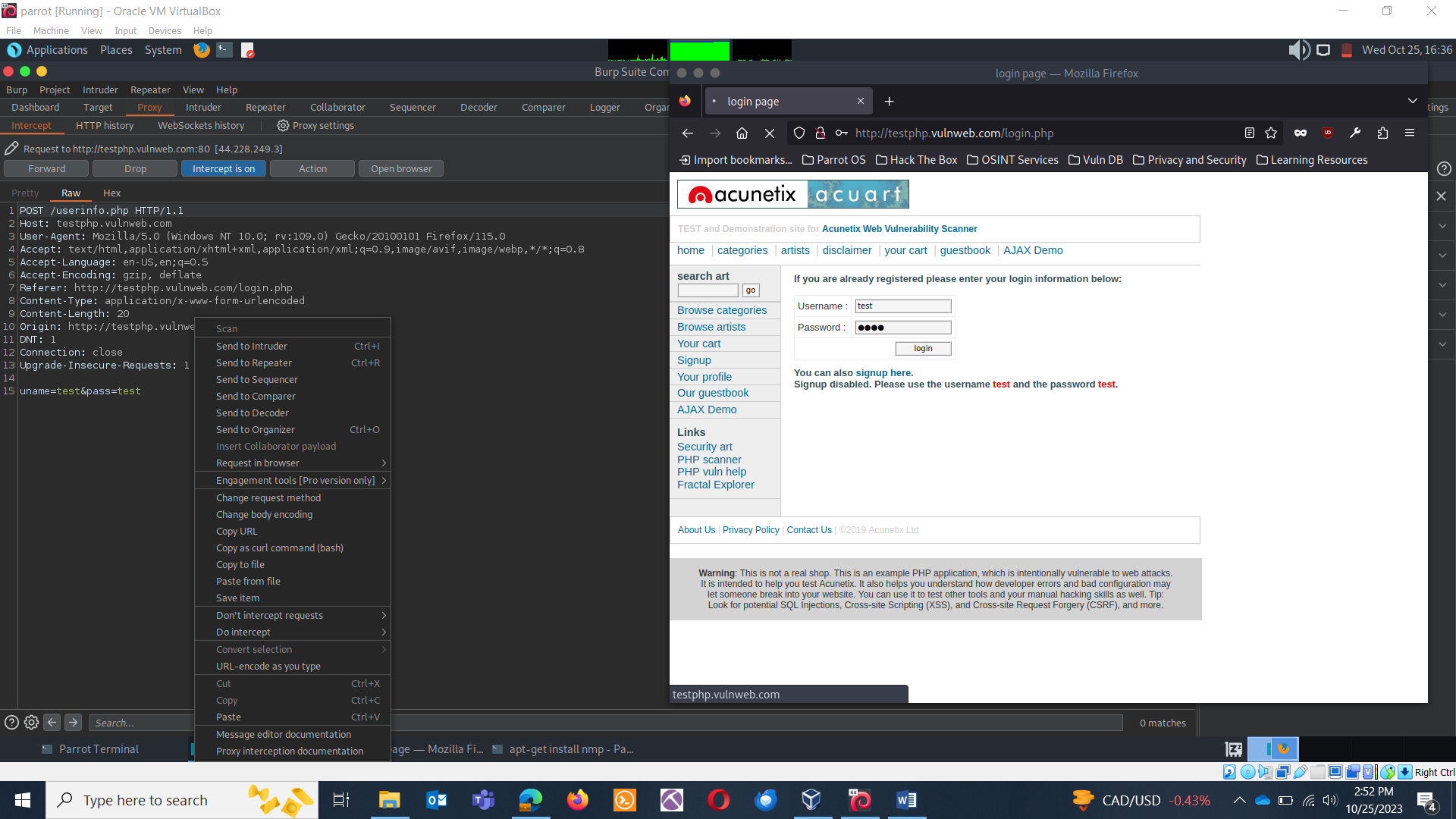
**3. Analyze Responses:** The Repeater tool displays the responses from the server, which allows you to inspect the application's behavior. You can look for error messages, security issues, or any other unexpected behaviors in the responses.

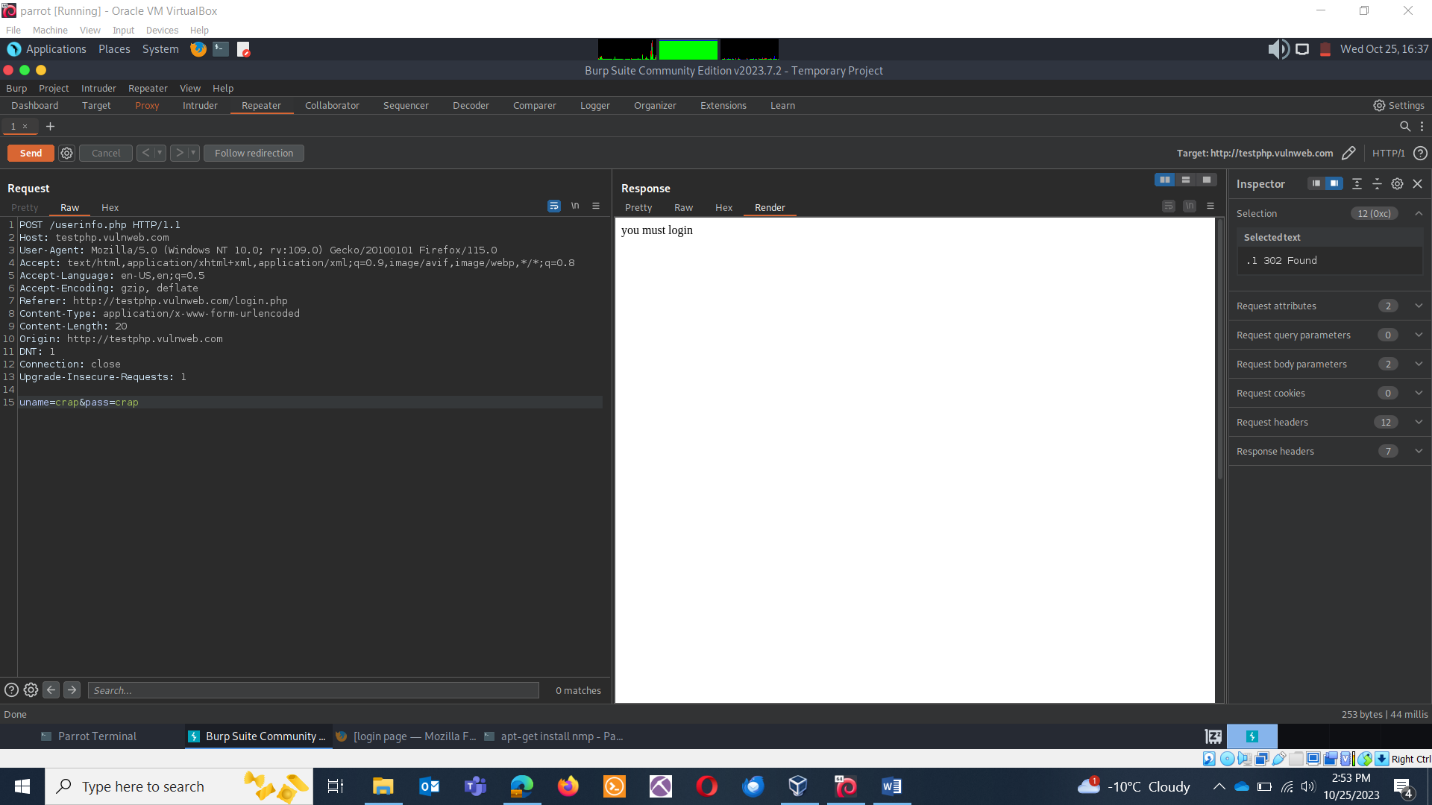
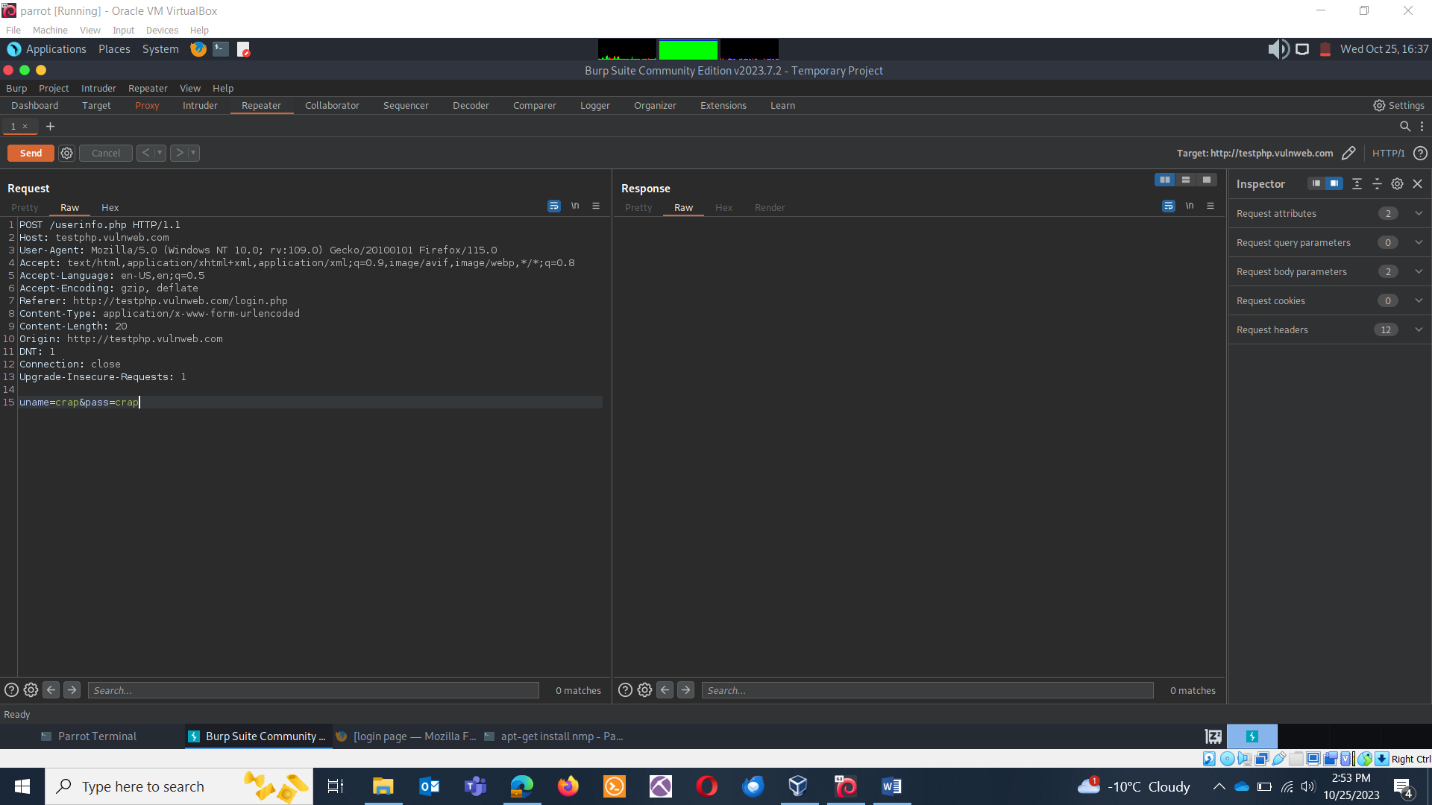
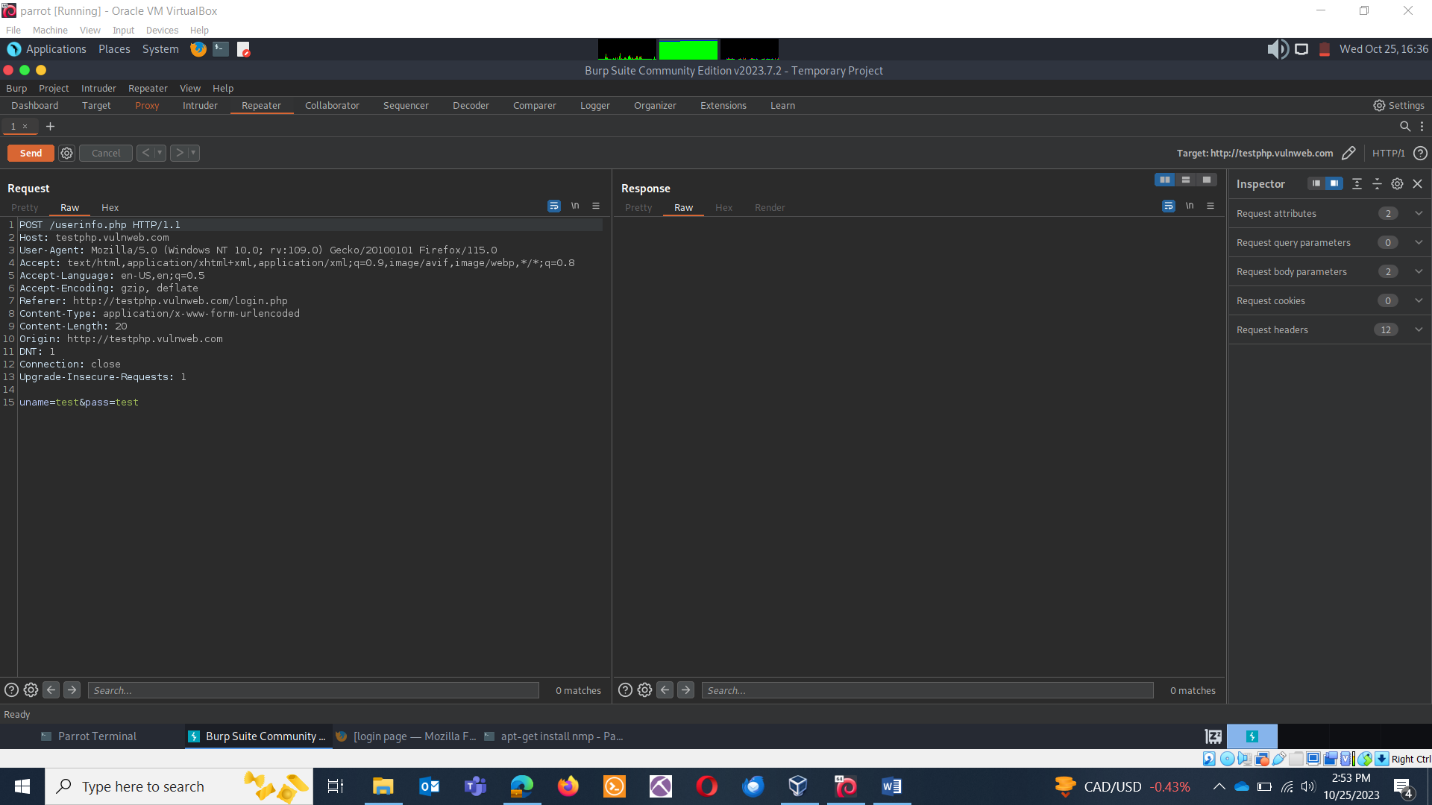
**4. Fine-Tune Testing:** You can use the Repeater tool to fine-tune your testing process. For example, when testing for SQL injection, you might modify SQL payloads and test various injection points within the application. This level of control is essential for detailed security assessments.

**TESTING BURPSUITE:**

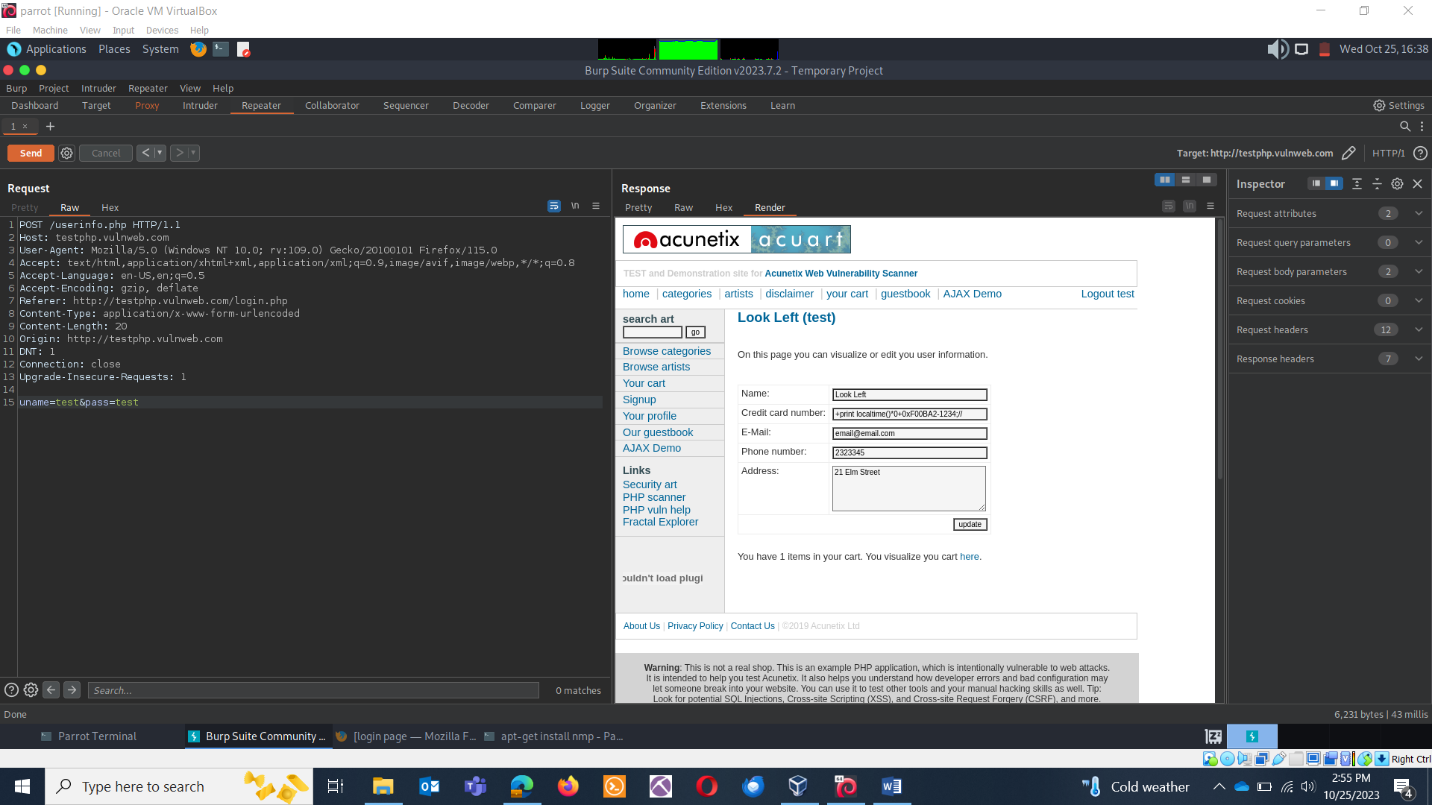
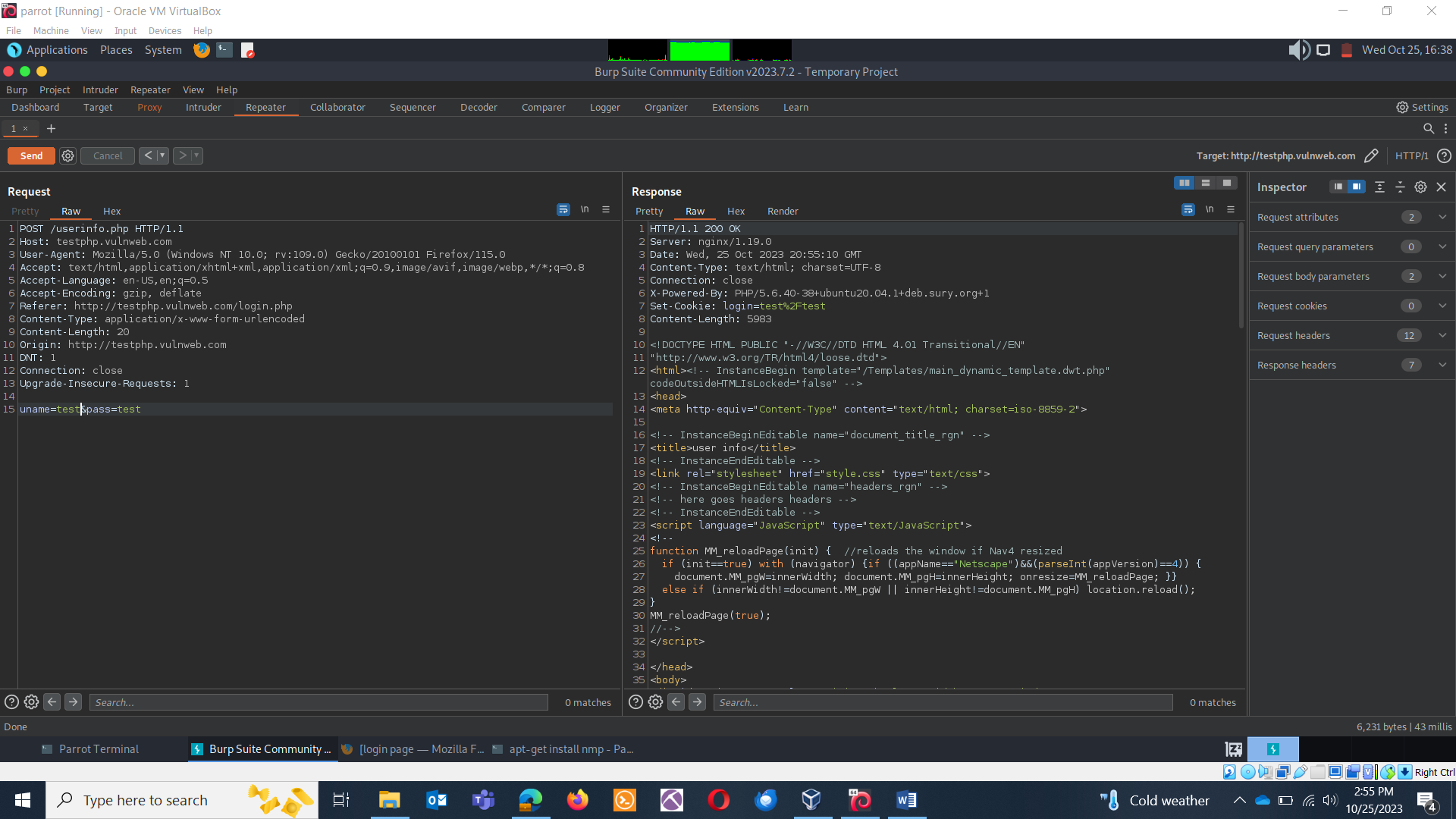
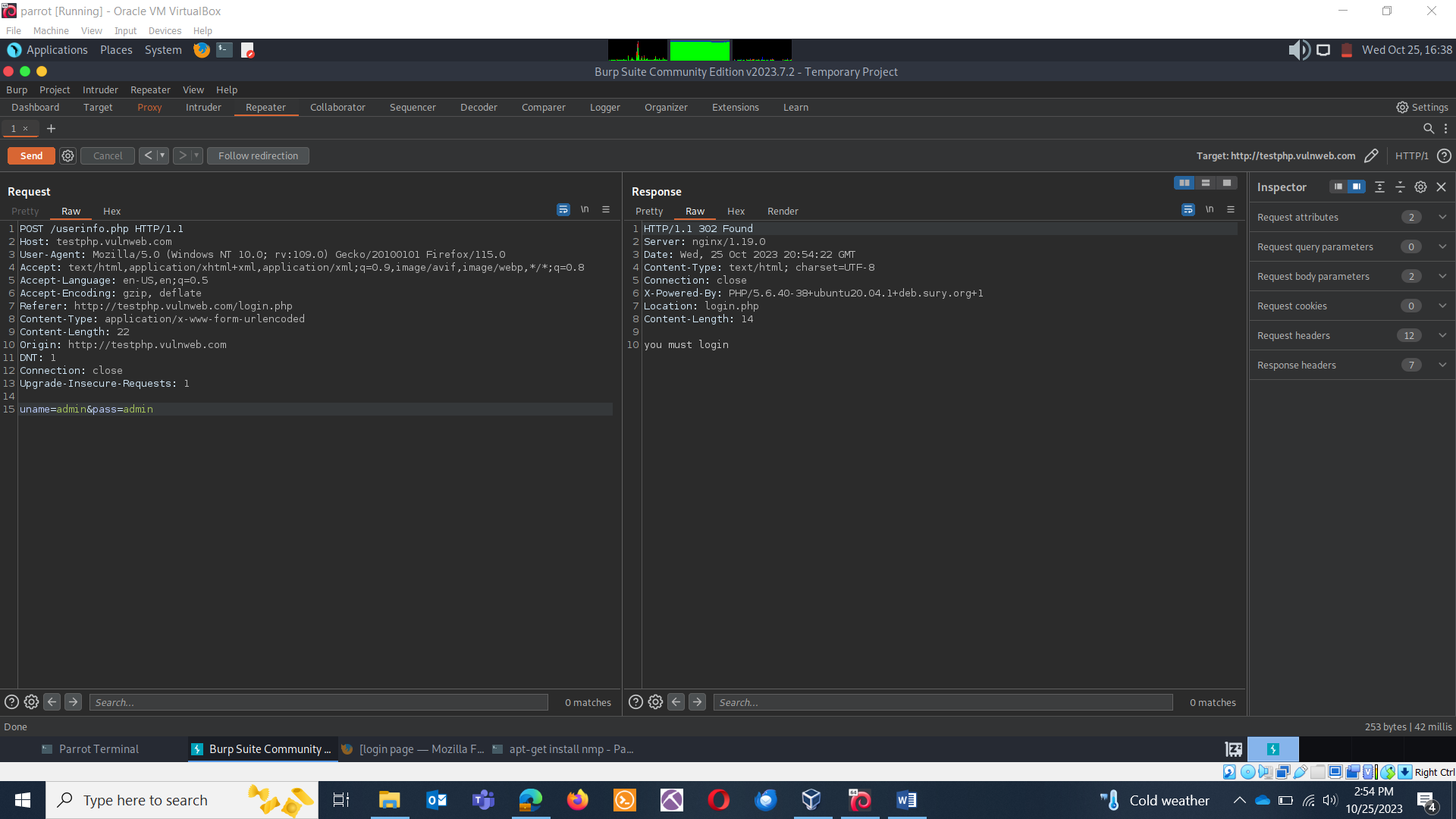




Right click and send it to repeater. 



Successful test logins.



Script injection:

