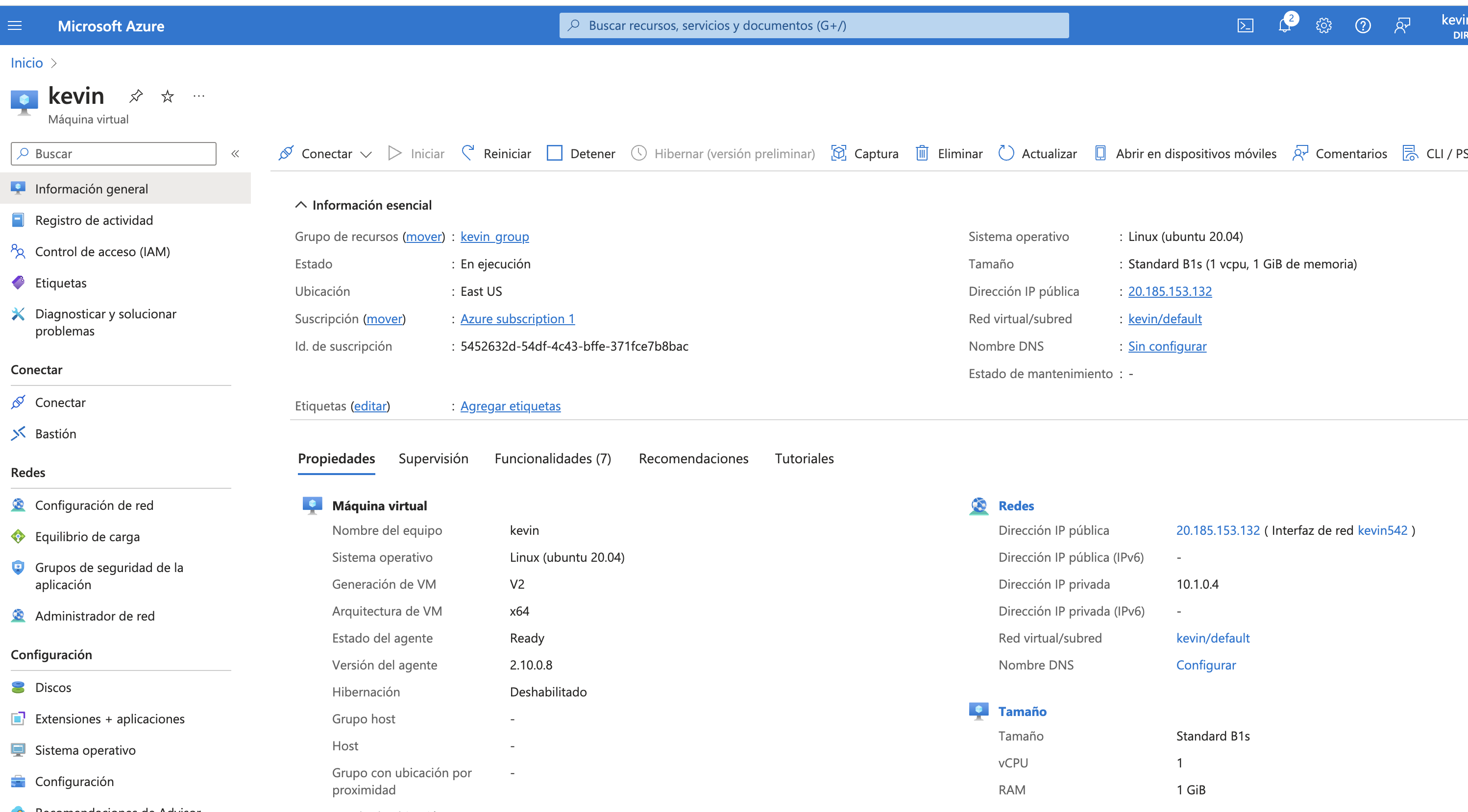
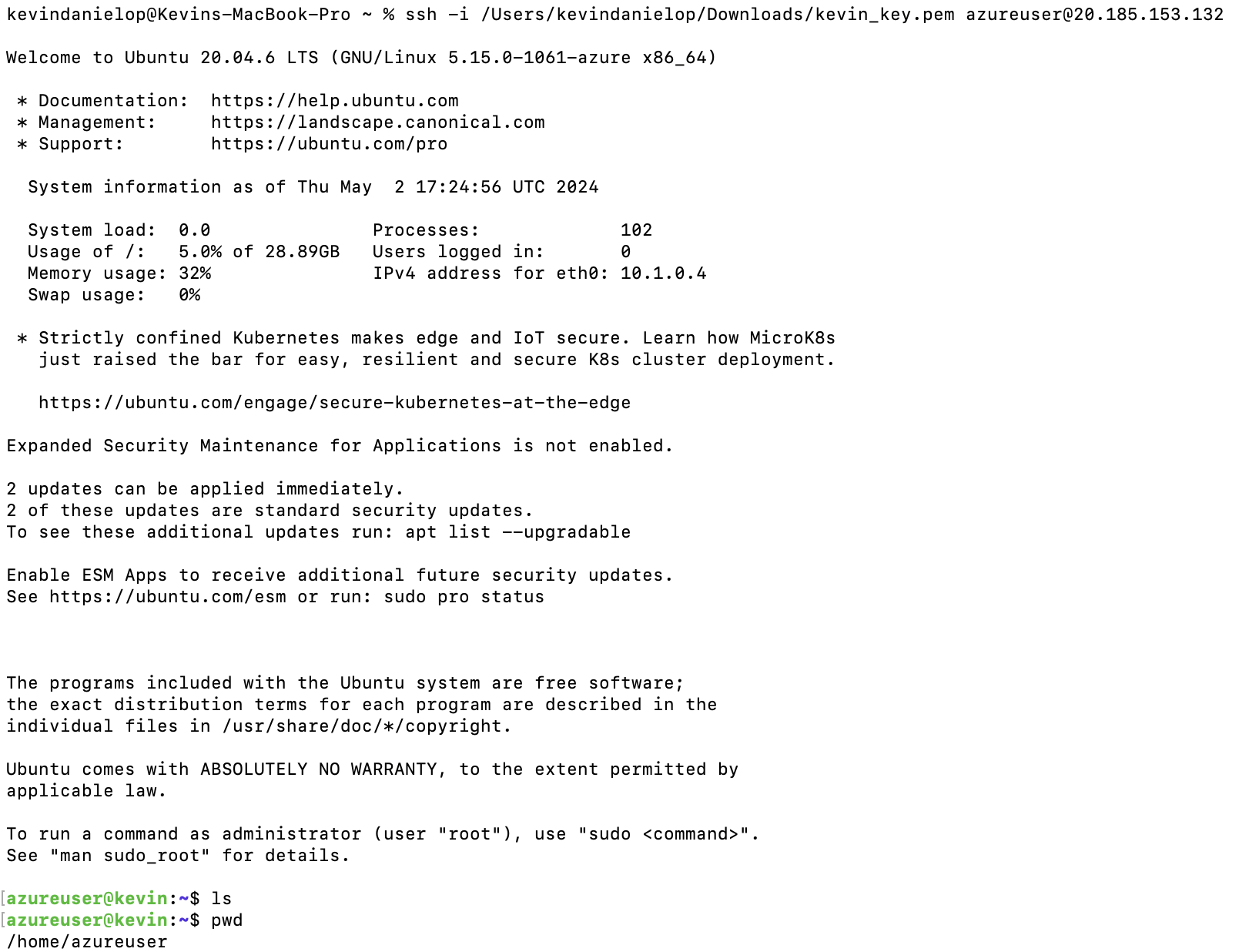
**Procedure for Creating the Virtual Machine and WAF. An example attacks.**

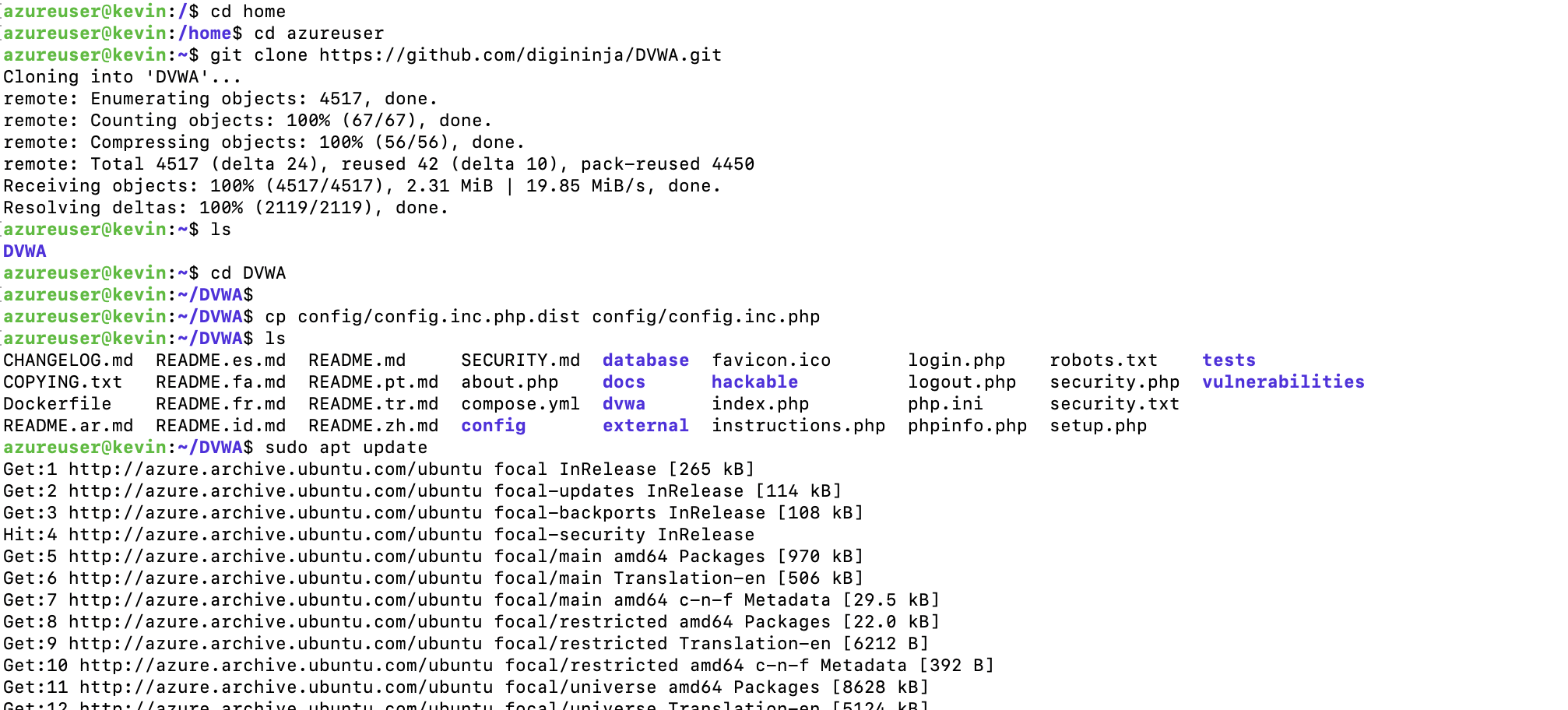
**Name**: Kevin Huertas

**---------Procedure-------**

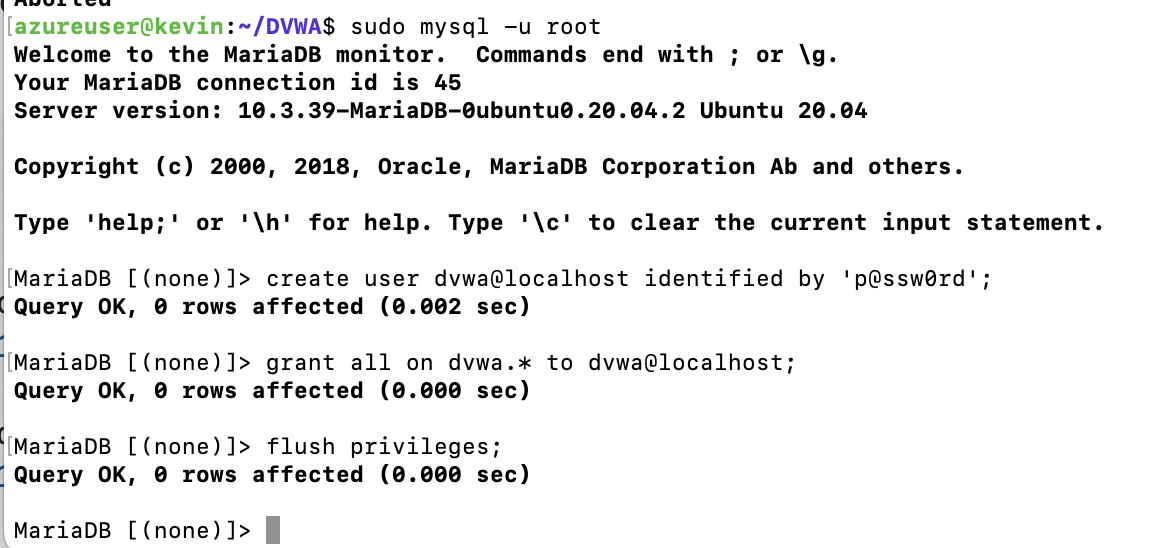
Starting VM on Azure::  


Once the virtual machine is created, I connect to it through my terminal using the SSH key.

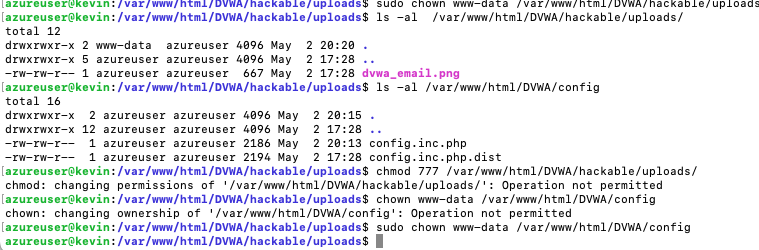
Once connected, I proceed to clone the DVWA project and follow the steps outlined in the GitHub Readme.



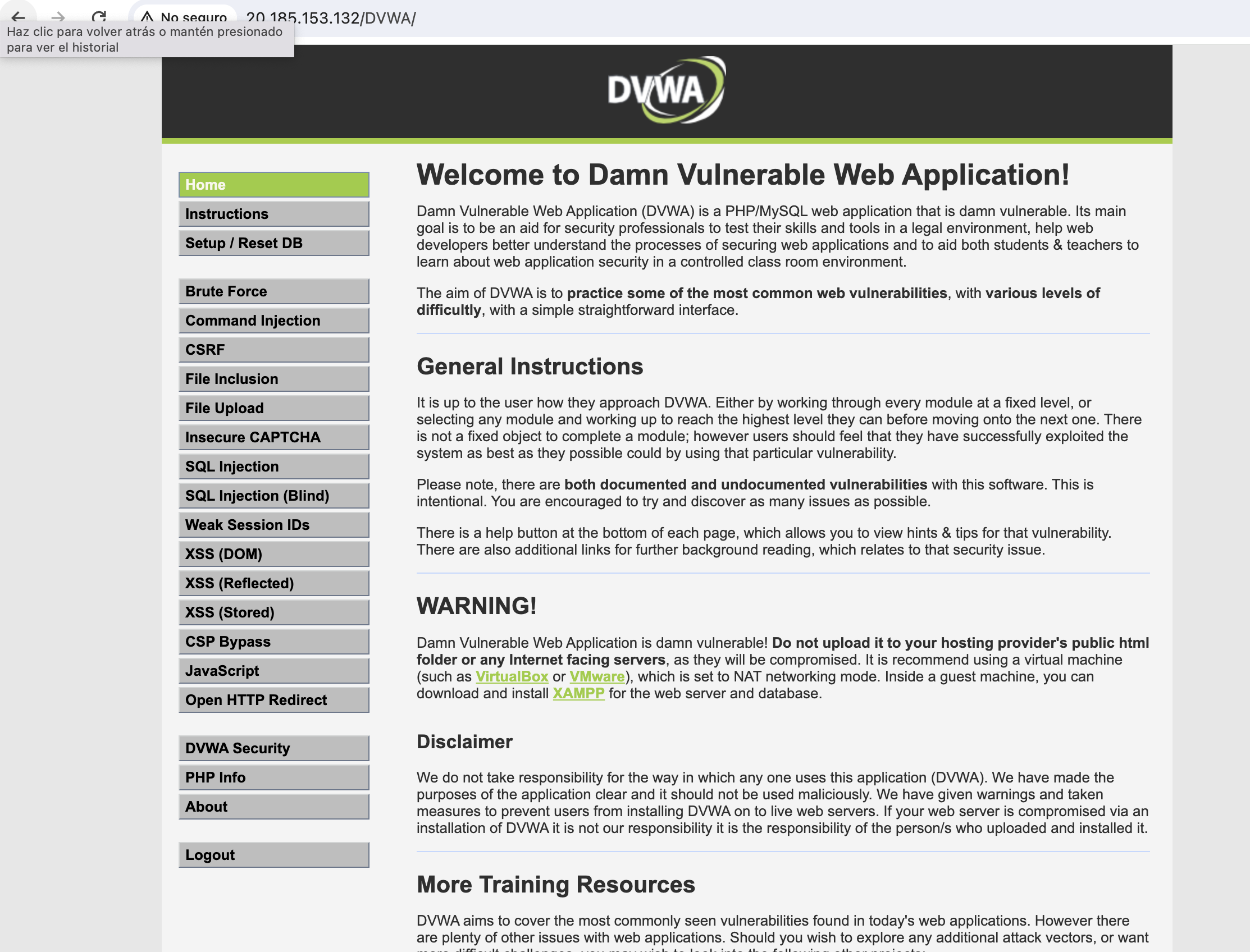


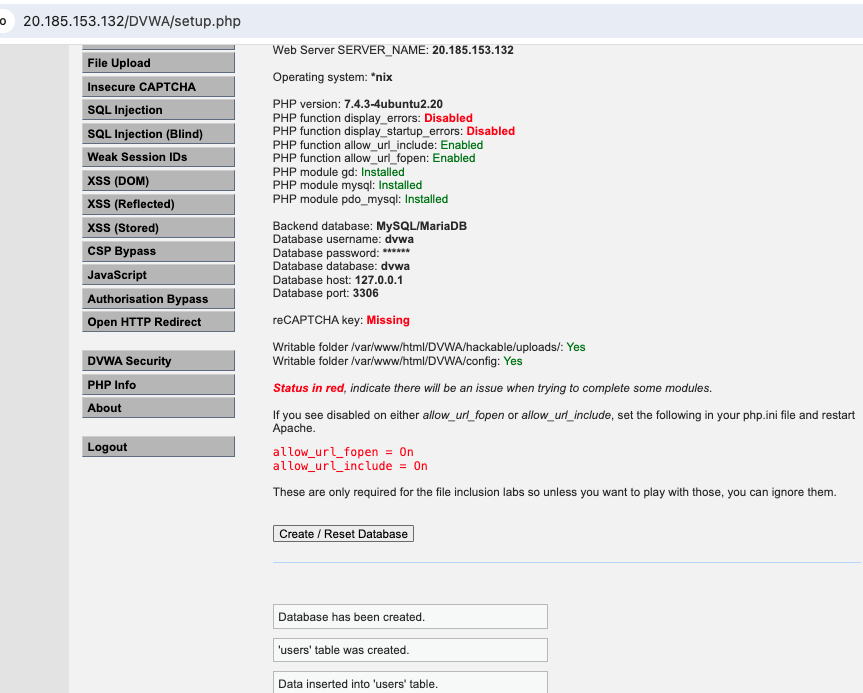
I start the database with the configuration provided in the Readme.q

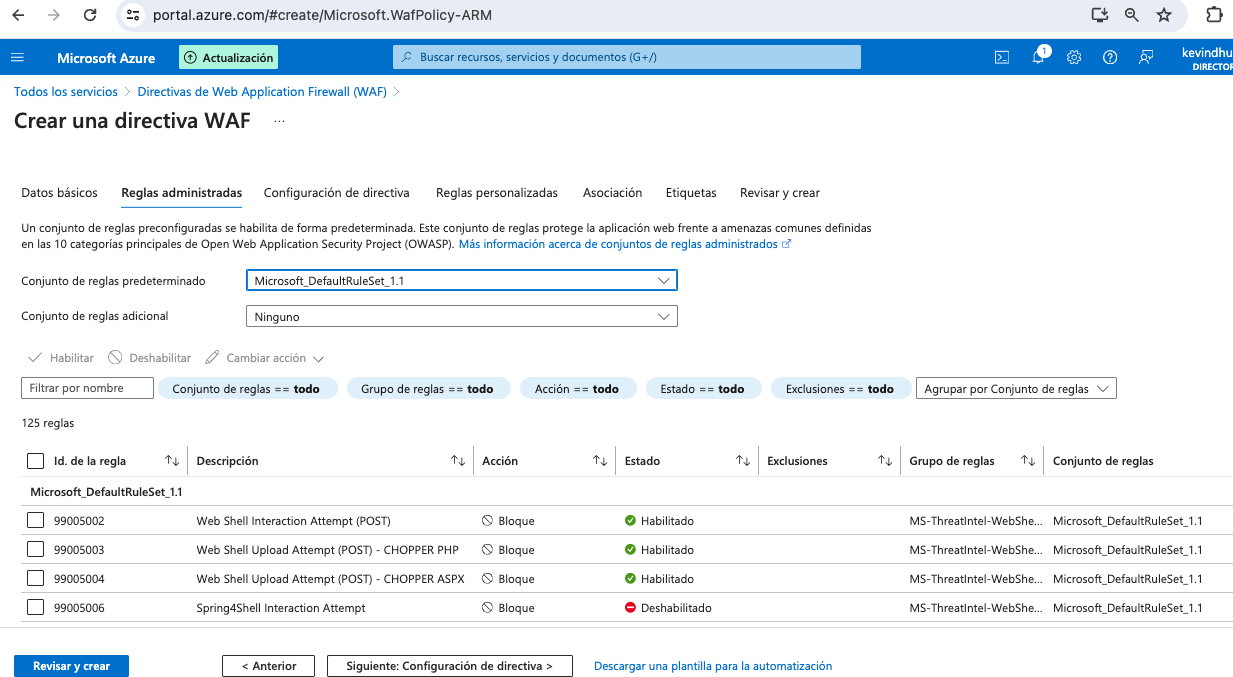
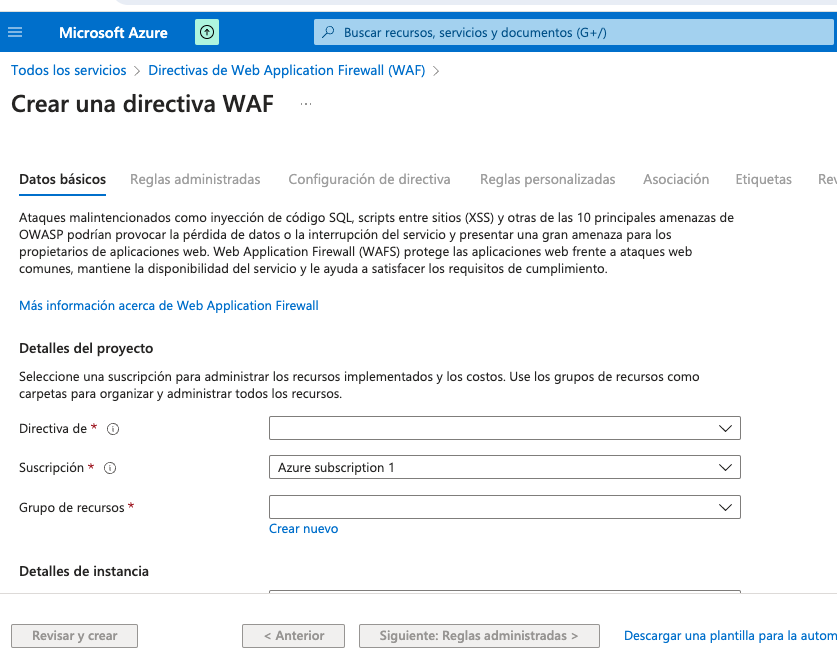




Once configured, we have our web app up and running. We set everything to carry out the attacks.





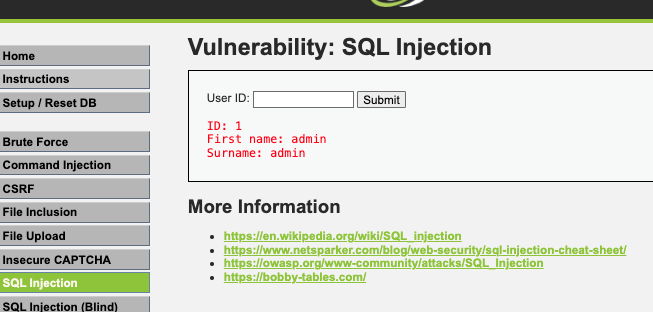
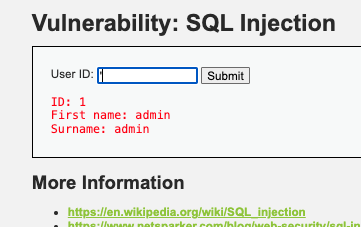
Ahora creamos el recurso WAF en Azure:  


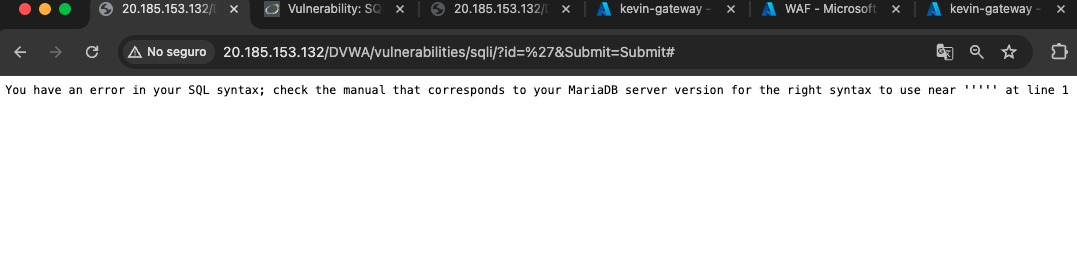
Esta es una forma de hacerlo, pero luego despues de investigar me di cuenta que se puede hacer con un gateway, siendo una manera mas facil de conectar el WAF con la red de nuestra app.

**---------Attacks-------**

Probe con SQL Injection.

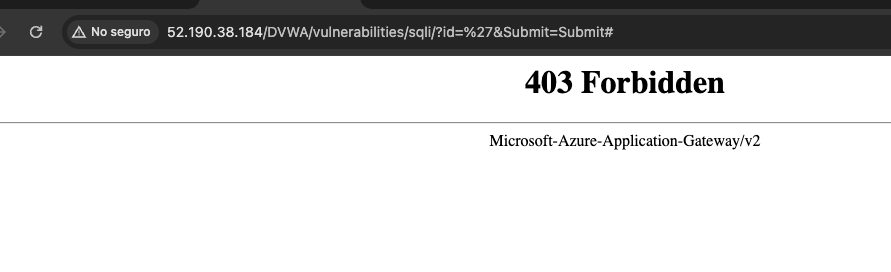
Without WAF, with ip: http://20.185.153.132/DVWA/vulnerabilities/sqli/



Now with WAF, with ip: <http://52.190.38.184/DVWA/vulnerabilities/sqli/>





We can verify that the WAF is working by conducting an attack.