UNIVERSIDAD DE CASTILLA - LA MANCHA

Computadores
avanzados

ESCUELA SUPERIOR DE INFORMÁTICA

Práctica 2. API Restful

Autores:

Silvestre SANCHEZ-BERMEJO SANCHEZ

Profesor:

Cleto Martín

14 de noviembre de
2021

Instalación

Instalación de dependencias

En primer lugar, instalamos las dependencias, con

pip install -r requirements.txt

Resolver host

Después, debemos modificar el archivo **/etc/hosts** añadiendo a la dirección ip 127.0.0.1 la resolución myserver.local

En mi caso, queda de la siguiente manera:

127.0.0.1 localhost myserver.local

Esto significa que tanto "localhost" como "myserver.local" son equivalentes a 127.0.0.1

Instalar certificados HTTPS

A continuación, deberemos instalar los certificados, ya que es un servidor HTTPS.

Debemos copiar el archivo **cert.pem** a los siguientes directorios:

sudo cp cert.pem /usr/local/share/ca-certificates/cert.crt

sudo cp cert.pem /etc/ssl/certs/cert.crt

Y después, actualizar los certificados:

sudo update-ca-certificates

Debemos comprar que la salida del update indique que hay un certificado nuevo añadido, en caso contrario, deberemos hacer un fresh

sudo update-ca-certificates -f

Ejecución

Para ejecutarlo, simplemente lanzaremos el archivo de Python

./APIrest

Explicación del proyecto

Las principales medidas de seguridad que se han aplicado en este proyecto se han basado en la longitud y características de la contraseña, la cual debe tener un mínimo de 8 caracteres, incluyendo minúsculas, mayúsculas y números.

Dichas contraseñas se guardan en un archivo shadow, hasheadas junto con un salt, con sha256

También se restringe el uso de caracteres especiales para evitar la inyección de datos, tanto en el login y registro, como en la creación de archivos.

La extensión de los archivos al hacer un POST debe ser .json obligatoriamente, para evitar la subida de scripts.

Tampoco se puede acceder a otras rutas del sistema, por la manera en la que está hecho el código, y por las restricciones de caracteres.

Para asegurar la disponibilidad, implementaría un contador de peticiones por usuario y por espacio de tiempo. Esto quiere decir, que un usuario no pueda hacer mas de x peticiones por minuto, para, por ejemplo, evitar ataques DDOS o sobrecargas del sistema.

Si esto ocurriera, se limitarían las peticiones de dicho cliente; esto podría hacerse utilizando una “black list” en la que hubiera un listado de IP’s sospechosas.

También, limitaría el tamaño aceptable de payloads enviados por el cliente.

Por otro lado, limitaría el espacio disponible para cada usuario, en función de los requisitos del sistema.

Por ejemplo, si es un sistema local con poca capacidad de memoria, limitaría el espacio para cada usuario a 50GB. Para que de esta manera no ocupara espacio que podría estar disponible a otros usuarios.