## 1.1 Autores

Somos el grupo T4 formado por:

* Jonatan Viñuelas Caballero
* Ana Olmeda Fernández
* Miguel Domingo Calvo

## 1.2 Planificación

El enlace a nuestra planificación es el siguiente:

<https://app.ganttpro.com/shared/token/b8f0262e0ed911fce78cebe0d3971b1dd8bf59238feb055e046c3e0858c19d9a>

# **2. Descripción del tipo de tecnología**

En este trabajo vamos a centrarnos en Web testing tools: Security, ya que la seguridad es un tema importante, actual y de futuro.

Las herramientas de pruebas web se encargan de realizar pruebas software. Estas pruebas pueden ayudar a abordar problemas antes de que el sistema se revele al público. Se encargan de cuestiones tales como la seguridad de la aplicación web, la funcionalidad básica del sitio, su accesibilidad para los usuarios…

Las pruebas de seguridad Web nos dicen si los requisitos de las aplicaciones basadas en Web se cumplen cuando son sometidos a datos de entrada maliciosos.

Hemos elegido las siguientes herramientas para trabajar Netsparker y Nmap, ya que nos parecen las más interesantes.

* Netsparker: Es el único escáner de seguridad de aplicaciones web falso-positivo-libre. Simplemente apuntas a tu sitio web y se detectará automáticamente los defectos que podrían dejarte peligrosamente expuesto.

Fácil de usar, y utiliza la avanzada tecnología de escaneo de vulnerabilidades Prueba-base y se ha incorporado en las pruebas de penetración y herramientas de reporte. Hay opción Premium.

* Nmap: Es una herramienta de código abierto para la exploración de red y auditoría de seguridad. Fue diseñado para escanear rápidamente grandes redes, aunque funciona bien contra el anfitrión individuales.  Se utiliza comúnmente para las auditorías de seguridad, aunque a muchos sistemas y administradores de red les resulta útil para tareas de rutina, tales como inventario de la red, los horarios de actualización de servicio de gestión, monitoreo y anfitrión o un tiempo de servicio.