

Gestión de la Información en la Web

Curso 2016-17

Práctica Autenticación delegada

Fecha de entrega: miércoles 25 de enero de 2017, 13:55h

Entrega de la práctica

La entrega de la práctica se realizará a través del Campus Virtual de la asignatura mediante un fichero **grupoXX.zip** donde **XX** es el número de grupo. Este ZIP constará de un fichero **autenticacion_delegada.py** con el código del servidor web, cuyo esqueleto se puede descargar del Campus Virtual. Además del servidor web, el fichero ZIP contendrá las vistas/plantillas necesarias para mostrar los datos adecuadamente (si las habéis utilizado).

Lenguaje de programación

Python 2.7 o 3.5.

Declaración de autoría e integridad

Todos los ficheros entregados contendrán una cabecera en la que se indique la asignatura, la práctica, el grupo y los autores. Esta cabecera también contendrá la siguiente declaración de integridad:

(Nombres completos de los autores) declaramos que esta solución es fruto exclusivamente de nuestro trabajo personal. No hemos sido ayudados por ninguna otra persona ni hemos obtenido la solución de fuentes externas, y tampoco hemos compartido nuestra solución con nadie. Declaramos además que no hemos realizado de manera deshonesto ninguna otra actividad que pueda mejorar nuestros resultados ni perjudicar los resultados de los demás.

No se corregirá ningún fichero que no venga acompañado de dicha cabecera.

Autenticación delegada utilizando Google

En esta práctica vamos a utilizar el API de Google para autenticar usuarios. Únicamente vamos a implementar una prueba de concepto, por lo que los pasos a seguir serán:

1. Darse de alta en la Consola de Desarrolladores de Google y crear los credenciales de la aplicación web (<https://console.developers.google.com>).
2. A la hora de autenticar un usuario, redirigirlo a Google con los parámetros adecuados.
3. Recibir la petición del usuario, obtener el código generado por Google y canjearlo por un `id_token`.
4. Extraer el e-mail del usuario del `id_token` y devolver una página de bienvenida.

Aunque existen distintas librerías con funciones que facilitan la autenticación delegada con distintas redes sociales, el objetivo de esta práctica es realizar todo el proceso de manera *manual*, sin utilizar APIs ni funciones externas sino realizando las peticiones HTTP adecuadas.

Seguiremos el esqueleto que podéis descargar del Campus Virtual, llamado `autenticacion_delegada_skel.py`. Este fichero contiene un servidor web que responde a peticiones **GET** en dos rutas:

- `/login_google`
Genera una página HTML con un enlace o un botón que redirige al usuario a la página de autenticación delegada de Google. Esta petición debe contener las credenciales necesarias de nuestra aplicación web.
- `/token`
Recibe la petición del usuario redirigida desde Google con el código temporal que deberemos canjear por un `id_token`. Por tanto, en las credenciales de nuestra aplicación deberemos configurar el `redirect_uri` a `http://localhost:8080/token` tal y como aparece en el esqueleto. El `id_token` que obtendremos será un JWT con la información del usuario, del que extraeremos la dirección de e-mail¹. Finalmente se generará una página HTML de bienvenida con el mensaje **Bienvenido** `<e-mail>`.

Para conseguir la máxima puntuación en esta práctica es necesario utilizar tokens *anti-CSRF* para distinguir entre peticiones legítimas y maliciosas (consultad la documentación de Google para OpenID Connect en <https://developers.google.com/identity/protocols/OpenIDConnect>.)

¹Para descifrar el JWT recomiendo conectar con el servicio `tokeninfo` de Google. Más información en <https://developers.google.com/identity/protocols/OpenIDConnect#validatinganidtoken>.