CySec News

2020 ENERO

SEGURIDAD EN LAS API – Android

INTRODUCCIÓN

Desde su aparición hasta hoy gracias a las API (Application Programming Interface), las aplicaciones web y móviles se han expandido enormemente por uso, ya que gracias a las API es muy fácil acceder a los recursos que ofrece una aplicación en particular; utilizando el lenguaje de programación que se prefiera. Muchas compañías dejan a disposición sus API para que puedan ser consumidas dentro de una página web, o una aplicación como es el caso de Instagram, Spotify, Twitter y muchas otras, dicho de otra forma, las API son el intermediario que permiten que una aplicación extraiga información, de cierto tipo y lo use dentro de su programa.

Consumir estas APIs es bastante sencillo, lo que hay que tener en cuenta, es que haya un filtro que controle quienes acceden a nuestra API y si los mismos tienen el permiso, por ello vamos a añadir un tipo de permiso especial el Access token, el cual solo permitirá el ingreso a quienes realmente se les ha otorgado. El encargado de elaborar el Access token es desde el lado de servidor por ello, “La seguridad de las API necesita un entorno confiable con políticas la autenticación y autorización.” Red Hat.

DESARROLLO

Recordaremos que una API es interfaz de programación de aplicaciones que permite la comunicación entre aplicaciones separadas. Las API basada en REST (Representational State Transfer) es una arquitectura basada en el protocolo http REST.

REST utiliza métodos de estado GET con get solicitando recursos, POST para crear recursos, PUT editar recursos, DELETE para eliminar recursos y Patch para editar recursos concretos.

Hoy en día tenemos el gran reto de implementar nuestras API, en un servidor seguro, con un Access token, una firma digital, un cifrado y entre tantas cosas, debemos estar a la vanguardia para la protección de nuestra información, de la misma forma si estamos utilizando una API de terceros tenemos que estar seguros de que, por el canal que se ha otorgado el permiso nuestra información no esté siendo robada por intrusos.

¿Por qué es importante la seguridad de las API?

Las API nos ayudan a conectar servicios y transferir datos; una API robada o tomada sin el permiso correspondiente puede causar una serie vulneración de datos y exponerlo a extraños.

DEMOSTRACIÓN

Ejemplo de una API con token: Vamos a ponernos en el caso que tengamos nuestro dominio que sería: http://Mywebpage.com/

Por n razones no se ha configurado el protocolo seguro, pero aun así nuestro dominio funciona. Primero debemos asegurarnos de que nuestro dominio sea seguro:

https://Mywebpage.com/

Hemos conseguido que nuestro dominio sea seguro, seguidamente tenemos una API que me trae todos los movimientos de mi cliente #21:

https://Mywebpage.com/v1/api/api_cli_mov?id=21

Nuestro código Java, sería la siguiente forma:

```
@Override
public void onClick(View v) {

    new ConsultarDatos().execute("https://Mywebpage.com/v1/api/api_create?id="+etId.getText().toString());

}
```

Ilustración 1, Fuente Propia

Al ejecutar la línea de arriba nos desplegará los datos de mi cliente 21, lo que no hemos provisto es que estos datos están expuestos a que cualquier persona que obtenga la url pueda consultar por ello una mejor practica sería añadir un token

https://Mywebpage.com/v1/api/api_cli_mov?access-token=2b166b3d2b822d189299f63db6813792&id=21

Este es un modelo de arquitectura cliente servidor, a través de una API el cliente solicita información al servidor, proporcionando el Access token, el cual es su permiso es decir la llave para acceder a este file de archivos la API recibe dicha información y se lo presenta al servidor al validar que es conforme este le devuelve la información, y la comunicación va llevando esa dinámica.

Hay muchas formas de generar un Access token seguro y aleatorio, para este ejemplo hemos tomado uno de la documentación oficial de Android. Una función para obtener un Access token a través de un random y luego a este se le aplica un tipo de cifrado de MD5(Algoritmo de Resumen del Mensaje 5) para obtener al final un valor único.

```
    private function getUniqueAccessToken() {
        $resultado = md5(Yii::$app->security->generateRandomString() .
'_' . time());
        $identity = $this->findIdentityByAccessToken($resultado);
        if ($identity) {
            $resultado = $this->getUniqueAccessToken();
        }
        return $resultado;
    }
```

Ilustración 2, Fuente developer.android.com

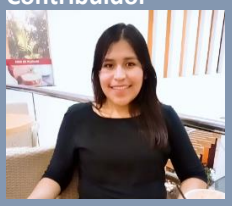
RECOMENDACIÓN

- Implementar un protocolo seguro en el sitio, donde se aloje las API.
- Usar Access tokens, ya que cuando el usuario se autentica de formar satisfactoria, puede acceder a la información que brinda la API hasta que su acceso dure o expire.
- Usar cifrados, el algoritmo HS es una de mis favoritas para app pequeñas, pero este será otro tema de discusión más adelante.
- Proteger la API, ya que es una puerta a nuestro servidor y ustedes deciden qué tipo de seguro quieren ponerle. Tal vez sea complicado darse cuenta de las vulnerabilidades, sobre todo cuando no hay errores, para ello mi consejo es que se pregunten que necesito.

FUENTE DE REFERENCIA

- https://developer.android.com/jetpack/docs/guide
- https://www.redhat.com/es/topics/security/api-security

Contribuidor



Elizabeth Quispe Esteban: Profesional informática, Analista y gestor de servicios de TI, gran apasionada de la tecnología, software y Java; ITIL y TOEFL certified. Actualmente desarrolladora de Aplicaciones Android. Contribuyente en causas humanistas.

LinkedIn: www.linkedin.com/in/elizabeth-quispe-esteban-99543074

Recursos LCW

LinkedIn	https://www.linkedin.com/company/cysecbywomen/
Facebook	https://www.facebook.com/CySecByWomen/
Twitter	@cysecbywomen