NOMBRE: Felipe Carlos Jiménez Ortega SECCIÓN: 1

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía y Seguridad Computacional — 1' 2021

# Tarea 3 – Respuesta Pregunta 1

1. En el caso de la autentificación de algún sitio web como Facebook.com, Youtube.com, etc. que solicitan el correo y la contraseña, uno al momento de ingresar dichos datos, entrega los datos al servidor de dichos sitios web, lo que nos deja vulnerable ya que se confía que quién administra el servidor que guarda las autentificaciones de los usuarios lo haga de manera segura y que no realizará alguna acción maliciosa como puede ser utilizar contraseña y correo para hacerse pasar por uno, o incluso si es que el usuario ocupa la misma contraseña en otros sitios, lograr hacer un cruce de datos de autentificación entre dichos sitios y así obtener la clave para ambos sitios, lo que es una clara deficiencia de seguridad. En cuanto a la autorización de algún procedimiento bancario por ejemplo, lo que ocurre es que el sitio web genera un Token para dicha sesión y cada vez que el usuario anteriormente *logeado* desea realizar alguna acción, el navegador de este debe enviar su *request* con el Token enviado, el cual por cierto es guardado en el navegador a través de las Cookies. Supongamos que una persona desea comprar por MercadoLibre y al momento de realizar la transferencia esta ingresa a su banco y con su autentificación realiza la transferencia correspondiente. El problema que hay aquí, es que cuando se llega al momento de pago de la compra, MercadoLibre debe realizar una *request* al Banco diciendo que es tal usuario el que desea realizar la transferencia, pero el problema está en que debe mandar el usuario su Token para que el banco identifique que es dicho usuario el que desea realizar la transferencia, pero es en este momento cuando se manda el Token guardado en las Cookies del navegador que perfectamente algún código malicioso de Javascript de parte de Mercado Libre puede hacerse pasar por el usuario y realizar una transferencia bancaria al hacer un cross-site request.

2.