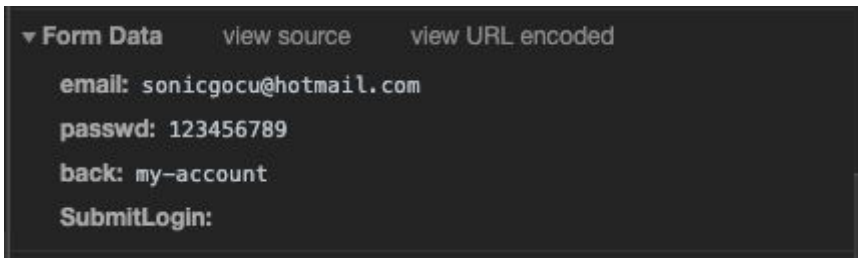
TAREA 1: Criptografía

José Proboste

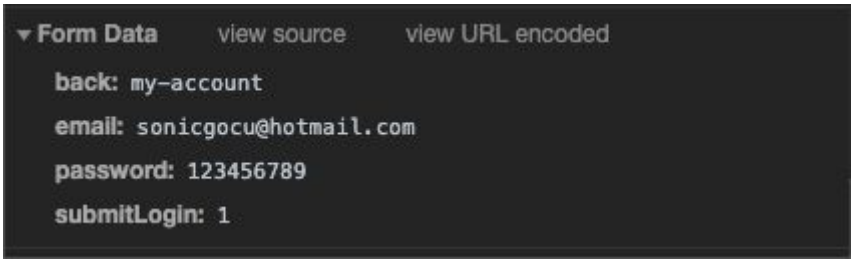
1) Arrow: Largo mínimo 5 (por código externo).
   Largo máximo 32 (por código externo).
   UNICODE, acepta todo tipo de caracteres, incluidos emojis y kanjis.
   Promovil: Largo mínimo 5 (por código externo).
   Largo máximo 72 (comprobado de forma manual).
   UNICODE, acepta todo tipo de caracteres, incluidos emojis y kanjis.

2) En ambas páginas, la contraseña es enviada por texto plano:

   Arrow:



   Promovil:



3) Arrow: email y passwd.
   Promovil: email y password.

4) Arrow: Primero se envía un correo con link para reestablecer la contraseña, al clickear el link, se procede a enviar un segundo correo con una contraseña temporal para poder realizar el cambio de la contraseña.

   Promovil: Se envía un correo con un link para reestablecer la contraseña.

5) Para ambos casos, en el correo enviado automáticamente, se envía el nombre registrado por el usuario.

6) La contraseña temporal de Arrow.cl corresponde a base64, ya que admite mayusculas [A-Z], minusculas [a-z], numeros [0,9] y [+,/].

7) En ninguno de los dos casos, la página recuerda contraseñas antiguas.

8) Ninguna de las 2 páginas tiene una medida de seguridad contra ataques por fuerza bruta, esto fue comprobado por código en Selenium.

9) En Arrow.cl, se expone que su información privada no podrá ser vista por terceros, pero como ya comprobé anteriormente, si se conoce el correo electrónico, se puede llegar al nombre.
En promovil.cl no se especifica sobre la seguridad de nuestros datos.

10) La automatización con Selenium podría evitarse generando contramedidas como detección de software externo, como lo hace Google con sus sitios webs.

11) Se debería utilizar un sistema, en el cual el usuario no pueda escribir erróneamente su contraseña más de 3 o 4 veces, con el fin de evitar ataques por fuerza bruta.

    No se debería exponer ningún dato ajeno a los ya proporcionados por el usuario, para así evitar la exposición de datos.

    No se debería enunciar la cantidad máxima de caracteres (como en el caso de Arrow.cl), ya que se acota el universo de contraseñas posibles.

    No enviar los datos al servidor en texto plano, ya que de esa manera cualquiera podría ver su contraseña, debería existir algún tipo de cifrado entre el cliente y el servidor.

12) Debería existir una mejor exposición de las políticas de seguridad (en el caso de promovil.cl), ya que no se especifica si nuestros datos están seguros o no.

    En general las páginas no son malas, ya que como tienen una cantidad limitada de caracteres posibles para la constraseña, se evita que se envíen contraseñas los suficientemente largas como para que colapse el servidor, aunque en el caso de promovil.cl, esta permite que se ingresen contraseñas gigantes, pero no permite el inicio de sesión.

    Ambas páginas decaen en el hecho de que no poseen contramedidas para ataques por fuerza bruta, esto debe ser mejorado.

Para el restablecimiento de contraseña, una buena opción sería una verificación de 2 pasos, con el fin de evitar que si una persona posee acceso a nuestro correo, pueda cambiar nuestra contraseña, con el fin de evitar que nuestro perfil se haga inaccesible.