

Tarea 1: Gestión de contraseñas

Sebastián Campos Vega

<https://github.com/ScamposV/Tarea1CSR-Gestion-de-contrasenas.git>

Criptografía y Seguridad en Redes

Escuela de Informática y Telecomunicaciones, Universidad Diego Portales

Profesor: Nicolas Boettcher

Profesor Auxiliar: Macarena Velásquez

01 de Abril 2021

1. Introducción

En el presente informe se auditará la implementación de los sistemas de creación, actualización, acceso, transmisión y de recuperación de contraseñas de dos sitios diferentes, uno de Chile y el otro de Francia, el cual será automatizado mediante Selenium en Python versión 3.9, el código contempla las siguientes automatizaciones: creación de cuenta, inicio de sesión, restablecimiento y modificación de contraseña.

Los sitios a utilizar son los siguientes:

- Chile: <https://www.fantasilandia.cl/>
- Francia: <https://www.probikeshop.fr/>

Cada sitio se someterá a distintas pruebas las que responderán las preguntas propuestas por el profesor, entre ellas están algunas como el largo mínimo y máximo que debe tener la contraseña, que tipo de información solicita la página para restablecer la contraseña, como se transmite la contraseña entre otras más.

2. Desarrollo

2.1. ¿Cuál es el largo mínimo y máximo de la contraseña a utilizar? ¿Cuál es la máxima base que permite utilizar el sitio?

2.1.1. Análisis para el sitio de Chile

Cuando se crea la cuenta no se menciona nunca un mínimo o un máximo de caracteres para la contraseña. Sin embargo, automatizando el proceso (ver imagen ??) de cambio de contraseña para establecer las restricciones para el sitio chileno, se concluye lo siguiente:

```
##### MODIFICACION DE CONTRASEÑA #####
#
time.sleep(20)
Cpass = driver.find_element_by_css_selector ("#main > div > div.row > div.col-md-3 > div > ul > li:nth-child(6) > a"
Cpass.click()
time.sleep(3)
Apass = driver.find_element_by_css_selector ("#passActual")
Apass.click()
Apass.send_keys("123456789123456789123456789123456789123456789123456789123456789")
Npass = driver.find_element_by_css_selector ("#passNueva")
Npass.click()
Npass.send_keys("1")
Rpass = driver.find_element_by_css_selector ("#passNuevaRe")
Rpass.click()
Rpass.send_keys("1")
save = driver.find_element_by_css_selector ("#btnCambiarPass")
save.click()
```

Figura 1: Código para cambio de contraseña en Python

Al cambiar la contraseña inicial por otra de un caracter, la página muestra el siguiente mensaje **”Clave Actualizada”** (ver imagen 2).



Figura 2: Respuesta de la página al cambio de contraseña.

Para saber el límite de caracteres que acepta el sitio, se realizan pruebas con contraseñas extensas, independiente de que tan extensa era la contraseña la página no arrojaba error. Por como respondía el sitio de acuerdo con el inicio de sesión, se concluye que el sistema truncaba en el máximo de caracteres permitido. Por lo tanto, para saber la extensión máxima de caracteres que admite el sistema, se fue reduciendo la contraseña de manera manual hasta que no permitiera acceder a la cuenta.

```
#Contraseña de 72 caracteres
Ipass.send_keys("123456789123456789123456789123456789123456789123456789123456789")
inicio sesion = driver.find_element_by_id("btnEnviarTop")
inicio sesion.click()
```

Figura 3: Ingreso cuenta 72 caracteres en contraseña

```
#Contraseña de 73 caracteres
Ipass.send_keys("1234567891234567891234567891234567891234567891234567891234567891")
inicio sesion = driver.find_element_by_id("btnEnviarTop")
inicio sesion.click()
```

Figura 4: Ingreso cuenta 73 caracteres en contraseña

Para ambas contraseñas anteriores se lograba ingresar al sistema sin inconvenientes, pero cuando se trunca la contraseña a 71 caracteres este nos arrojaba el siguiente mensaje:



Figura 5: Respuesta de la página al intentar acceder

Para determinar tipo de base que admite se realizan pruebas en donde se cambia la contraseña por caracteres especiales, una de las pruebas que se realizó fue la siguiente:

Se cambia la contraseña original por una serie de caracteres especiales los que son leídos por el sitio como se muestra en la imagen que sigue (ver imagen 6), también se realizaron pruebas con emojis, símbolos especiales tanto de la base ASCII como de Unicode, pero en todas la forma de lectura es la misma.

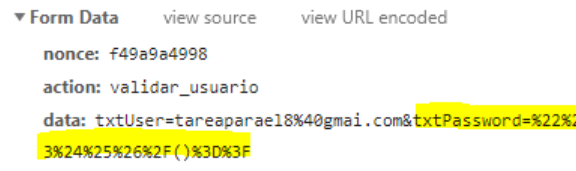


Figura 6: Admisión de base

En conclusión, las restricciones para el sitio chileno son las siguientes:

1. Password de 1 a 72 caracteres.
2. Base permitida por el sitio: Base64 + algunos caracteres como ().

2.1.2. Análisis para el sitio de Francia

Para la creación de cuenta en la plataforma francesa, se nos restringe la cantidad mínima de caracteres que debe llevar la contraseña (ver imagen 7), pero no nos indica la cantidad máxima de caracteres que admite, lo que será evaluado más adelante.

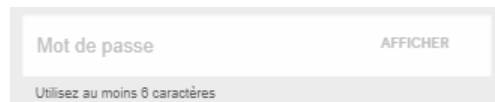


Figura 7: Respuesta de la página al cambio de contraseña

Al intentar cambiar la contraseña original por una contraseña de extensión menor a 6 caracteres, el sitio respondió de la siguiente manera:

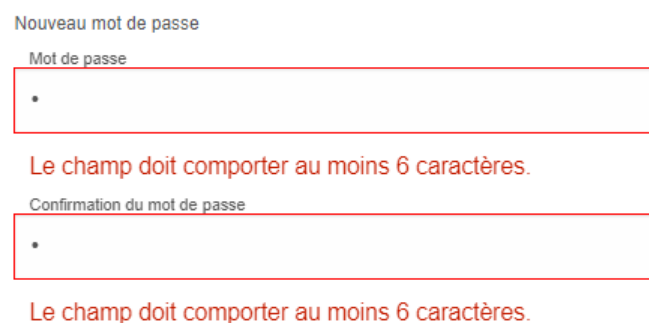


Figura 8: Respuesta de la página al cambio de contraseña

Para determinar la cantidad máxima de caracteres de la página, se procedió a analizar de forma similar a lo que se hizo en la página de Chile, no siendo una forma correcta al momento de determinar el largo, puesto que en el sitio Frances no truncaba la clave para ingresar al sitio. Si se quiere cambiar a una contraseña más larga que el permitido, el sitio responde *"Hubo un error al restablecer su contraseña, intente nuevamente"* (ver imagen 9).

VOTRE NOUVEAU MOT DE PASSE

Nouveau mot de passe

Mot de passe

.....

Confirmation du mot de passe

.....

Une erreur est survenue lors de la réinitialisation de votre mot de passe, merci de réessayer

SE CONNECTER

Figura 9: Respuesta de la página al cambio de contraseña

Cabe destacar que en la opción de cambio de contraseña de que nos brinda el perfil de usuario de la plataforma no indica ningún tipo de mensaje, pero cuando se reestablece la contraseña vía correo electrónico, se obtienen los mensajes anteriores (ver imágenes 8 - 9).

De forma manual se debió obtener la cantidad de caracteres permitidos por el sistema, el cual responde sin dejar entrar a la cuenta (ingresando una contraseña de 73 caracteres), previamente se cambió la contraseña a una de 150 por el método en donde no existen "restricciones".

Para determinar la base se ingresaron distintos tipos de caracteres especiales, logrando que símbolos Unicode, ASCII e incluso emojis sean admitidos por el sitio.

■ ASCII

```
▼ Request Payload view source
▼ {_username: "tareaparael8@gmail.com", _password: "!\"#$%&('/%$#\""}
  _password: "!\"#$%&('/%$#\""
  _username: "tareaparael8@gmail.com"
```

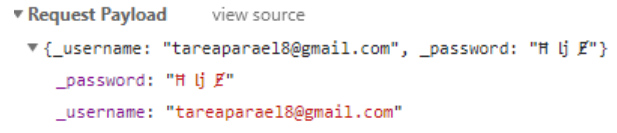
Figura 10: Lectura ASCII

■ Emoji

```
▼ Request Payload view source
▼ {_username: "tareaparael8@gmail.com", _password: "❤️"}
  _password: "❤️"
  _username: "tareaparael8@gmail.com"
```

Figura 11: Lectura emoji

- Unicode



```

▼ Request Payload view source
▼ {_username: "tareaparael18@gmail.com", _password: "H lj Ž"}
  _password: "H lj Ž"
  _username: "tareaparael18@gmail.com"

```

Figura 12: Lectura Unicode

Por lo tanto, las restricciones para el sitio francés son las siguientes:

1. Password de 1 a 72 caracteres.
2. Base permitida por el sitio: ASCII, Unicode y emoji.

2.2. ¿El largo mínimo/máximo está restringido desde el cliente?

Para ambos sitios el largo y mínimo de las contraseñas están establecidas por el sistema.

A continuación se adjuntan algunas imágenes según sitio.

2.2.1. Análisis para el sitio de Chile

- Limite de contraseña desactivado.

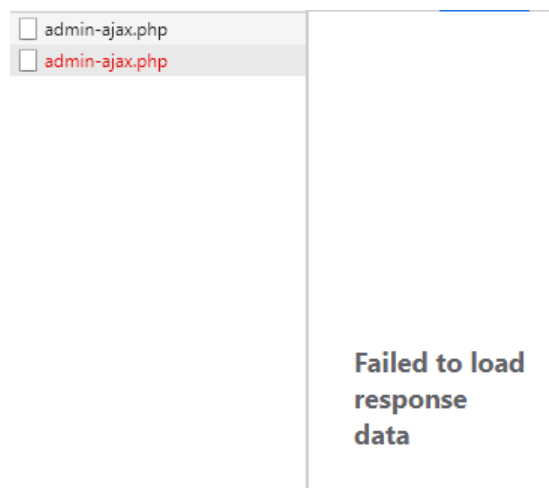
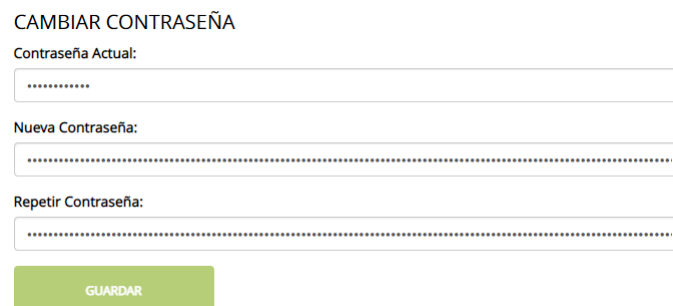


Figura 13: Bloqueo límite de contraseña

- El sitio quedo cargando por varios minutos sin completar el proceso.



CAMBIAR CONTRASEÑA

Contraseña Actual:

.....

Nueva Contraseña:

.....

Repetir Contraseña:

.....

GUARDAR

Figura 14: Respuesta del sitio

2.2.2. Análisis para el sitio de Francia

- Limite de contraseña desactivado.

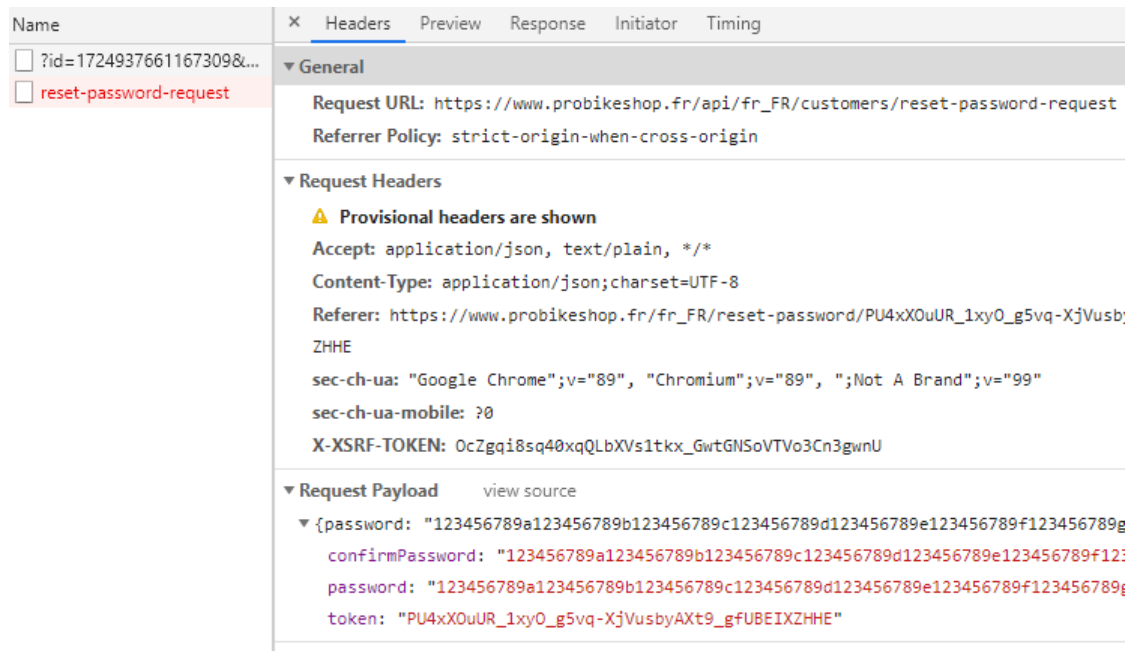


Figura 15: Bloqueo límite de contraseña

- Respuesta para el máximo de caracteres

Nouveau mot de passe

Mot de passe

Confirmation du mot de passe

Une erreur est survenue lors de la réinitialisation de votre mot de passe, merci de réessayer

SE CONNECTER

Figura 16: Respuesta del sitio

NOWE MOT DE PASSE

Nouveau mot de passe

Mot de passe

•


Le champ doit comporter au moins 6 caractères.

Confirmation du mot de passe

•

Le champ doit comporter au moins 6 caractères.

[SE CONNECTER](#)




PRIX LE MOINS CHER GARANTI

Vous trouvez moins cher ailleurs ? Nous vous remboursons la différence !



TOUS LES PRODUITS EN STOCK

60 000 références sont en stock



BESOIN D'UN CONSEIL ?

Nos experts à votre écoute gratuitement

A PROPOS DE PROBIKE

Qui sommes-nous ?

Notre gamme de vélos

#iamProbiaker

Communauté

Nos engagements

Recrutement

Probikeshop+

Store

The screenshot shows the Chrome DevTools Network tab with the 'Headers' sub-tab selected. The request is blocked, as indicated by the red 'X' icon in the status bar. The 'Request URL' is visible, showing a Facebook API endpoint for resetting a password. The status bar at the bottom shows '0 blocked' requests.

Figura 17: Respuesta del sitio

2.3. ¿Existe comprobación de robustez de la pass al momento de registrarse?

No existe comprobación de robustez para ninguno de los dos sitios en cuestión.

2.4. ¿Se transmite la contraseña en texto plano?

Ambas plataformas transmiten tanto el usuario como la contraseña en texto plano, a continuación se adjuntan las imágenes correspondientes según sitio.

2.4.1. Análisis para el sitio de Chile

▼ **Form Data** [view source](#) [view URL encoded](#)

nonce: f49a9a4998

action: validar_usuario

data: txtUser=tareaparael18%40gmail.com&txtPassword=TRANSMITIDOENEXTOPLANO

Figura 18: Texto plano sitio chileno

2.4.2. Análisis para el sitio de Francia



```
▼ Request Payload view source
{
  "_username": "tareaparael18@gmail.com",
  "_password": "TRANSMITIDOENTEXTOPLANO"
}
```

Figura 19: Texto plano sitio francés

2.5. ¿En qué variable se transmite al server el user y password?

2.5.1. Análisis para el sitio de Chile

Para este caso los datos de usuario y contraseña son transmitidos por la misma variable **"data"** (ver imagen 18).

2.5.2. Análisis para el sitio de Francia

Para la página francesa el sitio transmite el usuario como **"_username"** y la contraseña como **"_password"** (ver imagen 19).

2.6. ¿Qué información se solicita para restablecer la contraseña?

Para ambos sitios la forma de reestablecer la contraseña es la misma, mediante el correo electrónico. A continuación, se adjuntan las imágenes correspondientes a cada página web.

2.6.1. Análisis para el sitio de Chile



Recuperar Contraseña ✕

Ingresa tu dirección de correo electrónico, te enviaremos un email con los pasos que debes seguir para recuperar tu contraseña.

Email:

RECUPERAR CONTRASEÑA

Figura 20: Recuperar contraseña

2.6.2. Análisis para el sitio de Francia

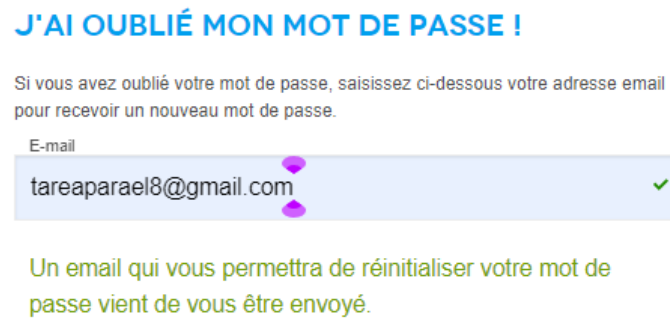


Figura 21: Recuperar contraseña

2.7. ¿Cómo opera el servicio de reestablecer contraseña?

En ambos sitios el modo de operar es el mismo, el sistema envía un correo con el enlace correspondiente para reiniciar la contraseña antigua por una nueva. A continuación, se adjuntan las imágenes correspondientes por cada sitio.

2.7.1. Análisis para el sitio de Chile

- Correo



Figura 22: Correo

- Restablecer contraseña

The image shows a web page with a blue header and a white form area. The header says "ESTÁS EN: FANTASILANDIA > RECUPERA TU CONTRASEÑA". Below the header, it says "Nueva Contraseña". Then there are two input fields: "Nueva Contraseña:" and "Repetir Contraseña:". At the bottom, there is a red button labeled "GUARDAR".

Figura 23: Página chilena

2.7.2. Análisis para el sitio de Francia

- Correo

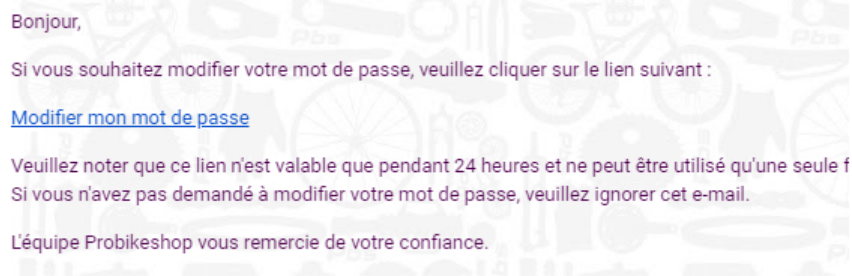


Figura 24: Correo

- Restablecer contraseña

VOTRE NOUVEAU MOT DE PASSE

Nouveau mot de passe

SE CONNECTER

Figura 25: Pagina francesa

2.8. ¿En el proceso de reseteo se expone información privada del usuario? ¿La información expuesta está completa o de forma parcial (n***@gmail.com)?

En ninguno de los dos sitios se exponen datos, los correos son generados de manera automática por el sistema.

2.8.1. Análisis para el sitio de Chile



Figura 26: Correo

2.8.2. Análisis para el sitio de Francia

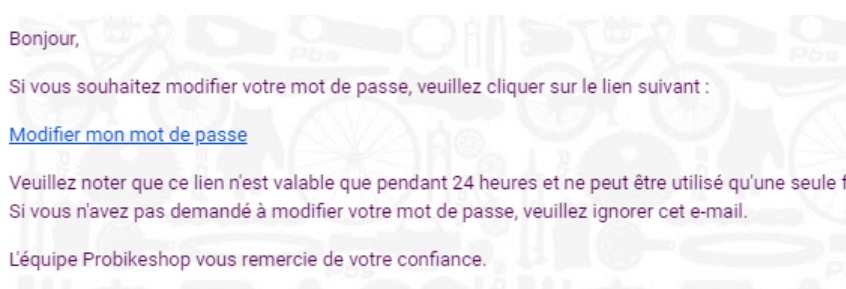


Figura 27: Correo

2.9. ¿El sitio recuerda contraseñas antiguas? ¿Cuántas? ¿Es posible eliminar esas passwords de la memoria del servidor (se pueden sobrescribir)?

Ninguno de los dos sitios guarda información sobre las contraseñas anteriores, incluso se puede "cambiar" la contraseña por la misma.

2.10. ¿El sitio es susceptible a ataques por fuerza bruta? ¿Cómo lo evita?

Los sitios son susceptibles a un ataque por fuerza bruta, ambos fueron capaces de tolerar 100 accesos, algunos correctos y otros erróneos, sin mayor dificultad.

2.11. ¿Existe la opción de eliminar su cuenta? En caso de ser así, ¿Queda algún indicio de la existencia de su cuenta?

Ninguna de las dos páginas permiten eliminar el usuario, salvo que en el sitio chileno se puede sobrescribir la cuenta.

Se asocia el Rut a un correo, cada vez que se crea una cuenta con el mismo Rut, pero diferentes correos, el ultimo es el que se conserva como un usuario "habilitado", mientras que el correo anterior queda a la deriva en alguna parte del sistema sin poder acceder a la sesión. Se intento reestablecer la contraseña con el correo antiguo, resultando de manera "exitosa" logrando entrar al sitio, pero cuando se ingresa de la manera habitual, muestra un mensaje de error. La solución a esto, como ya se dijo, fue crear otra cuenta con un correo nuevo para poder acceder sin problemas.

2.12. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio?

2.12.1. Análisis para el sitio de Chile

- "Derechos reservados, registro de los usuarios, claves y su uso diligente", párrafo 2: se menciona que el usuario seleccionara su nombre de usuario libremente, pero de la forma en que se registra en ningún momento se puede escoger el nombre de usuario y si se editan los datos, tampoco se tiene la opción de utilizar un usuario distinto.
- Fuera de lo anterior, la política de privacidad de la empresa es bastante severa al momento de la difamación de los datos ya ingresados al sistema. Sin embargo, no se hacen responsables de garantizar seguridad de la información entregada a través de la página web o móvil por algún tipo de vulneración.

2.12.2. Análisis para el sitio de Francia

- La plataforma se basa en la ley "Informatique et Libertés" del 6 de enero de 1978 y el Reglamento Europeo de Protección de Datos del 27 de abril de 2016.

3. Conclusión

Ambas plataformas son similares en varias cosas, salvo en el último punto tratado en el informe, en donde la página europea tiene una ley clara y definida que le da seguridad al usuario, mientras que en la página chilena solo se menciona la ley sin citar por cual se rige.

En los sitios tratados en el presente, no se hacen cargo de la robustez de la contraseña de sus usuarios, siendo vulnerables por ataques de fuerza bruta. La página francesa es un poco más estricta que la página chilena obligando al usuario a introducir mínimo 6 caracteres. Esto se puede solucionar mínimamente con un mensaje sugiriendo utilizar mayúsculas, minúsculas, números y símbolos (para quien lo permita).

El análisis de páginas de diferentes partes del mundo ayuda a entender la situación actual de Chile en cuanto a la seguridad informática y a la privacidad de los datos. Hay mucho que trabajar y mucho que auditar.

4. Bibliografía

- **Baiju Muthukadan**, s.f., "*Selenium with Python*", en <https://selenium-python.readthedocs.io/>. Recuperado en 23 de marzo 2021.
- **Probikeshop**, 2021, "*CONDITIONS GÉNÉRALES DE VENTE*", en <https://www.probikeshop.fr/static/conditions-generales-de-vente-probikeshop.html>. Recuperado en 28 de marzo 2021.
- **Sociedad Comercial Itahue Ltda.**, s.f., "*Términos y Condiciones*", en <https://www.fantasilandia.cl/terminos-y-condiciones/>. Recuperado en 01 de abril 2021.