

UNIVERSIDAD DIEGO PORTALES

CRIPTOGRAFÍA & SEGURIDAD EN REDES

Tarea1: Gestión de contraseñas

Autores:

Marcos Fantóval

Profesor: Nicolás Boettcher Ayudante: Francisco Lara

2 de abril de 2021

Índice

1. Pagina chilena	2
1.1. ¿Cuál es el largo mínimo y máximo de la contraseña a utilizar? ¿Cuál es la máxima base que permite utilizar el sitio? LLL	2
1.2. ¿El largo mínimo/máximo está restringido desde el cliente?	3
1.3. ¿Existe comprobación de robustez de la password? LLL	3
1.4. ¿Se transmite la contraseña en texto plano? LLL	3
1.5. ¿En qué variable se transmite al server el user y password?	3
1.6. ¿Qué información se solicita para restablecer la contraseña? LLL . . .	4
1.7. ¿Cómo opera el servicio de reestablecer contraseña? LLL	4
1.8. ¿En el proceso de reseteo se expone información privada del usuario? LLL	6
1.9. ¿Qué patrón tiene la nueva contraseña al resetearla?	6
1.10. ¿El sitio recuerda contraseñas antiguas? LLL	6
1.11. ¿El sitio es susceptible a ataques por fuerza bruta? ¿Cómo lo evita? .	7
1.12. ¿Existe la opción de eliminar su cuenta? LLL	8
1.13. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio? LLL	8
2. Pagina europea	9
2.1. ¿Cuál es el largo mínimo y máximo de la contraseña a utilizar? ¿Cuál es la máxima base que permite utilizar el sitio?	9
2.2. ¿El largo mínimo/máximo está restringido desde el cliente?	10
2.3. ¿Existe comprobación de robustez de la password? LLL	10
2.4. ¿Se transmite la contraseña en texto plano?	10
2.5. ¿En qué variable se transmite al server el user y password?	10
2.6. ¿Qué información se solicita para restablecer la contraseña?	11
2.7. ¿Cómo opera el servicio de reestablecer contraseña?	11
2.8. ¿En el proceso de reseteo se expone información privada del usuario? .	12
2.9. ¿Qué patrón tiene la nueva contraseña al resetearla?	13
2.10. ¿El sitio recuerda contraseñas antiguas?	13
2.11. ¿El sitio es susceptible a ataques por fuerza bruta? ¿Cómo lo evita? .	13
2.12. ¿Existe la opción de eliminar su cuenta? En caso de ser así, ¿Queda algún indicio de la existencia de su cuenta?	14
2.13. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio?	15
3. LInk Guthub	15

1. Pagina chilena

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

Al crear el usuario en esta pagina se pudo ver que el largo mínimo de la contraseña debe de ser de 5 caracteres y un máximo de 64 caracteres. Además, las bases Emojis por lo que contiene o permite todas las otras bases mas pequeñas.

Contraseña debe tener un máximo de 64 caracteres

Regístrate y disfrutarás de una experiencia de compra más rápida

Completa el siguiente formulario

Nombre Oliver

Apellido Queen

RUT 20480198-3

Email criptotareas@gmail.com

Contraseña

Al registrarte, aceptas los [términos y condiciones](#) y la [política de privacidad](#) de acuerdo a la Ley N° 19.628.

Regístrame

Figura 1: Máxima cantidad de caracteres en la contraseña

Contraseña

La contraseña no es válida, recuerda, debe tener más de 5 caracteres

Al registrarte, aceptas los [términos y condiciones](#) y la [política de privacidad](#) de acuerdo a la Ley N° 19.628.

Regístrame

Figura 2: Mínima cantidad de caracteres en la contraseña

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

No ya que el largo mínimo/máximo está restringido desde el servidor.

1.3. ¿Existe comprobación de robustez de la password? LLL

Esta pagina no presenta comprobación de robustez de ningún tipo.

1.4. ¿Se transmite la contraseña en texto plano? LLL

Al crear la cuenta se hizo una captura de paquetes para revisar si los datos verificar como se envinaban los datos descubriendo que se envían por texto plano como se comprueba en la siguiente imagen.

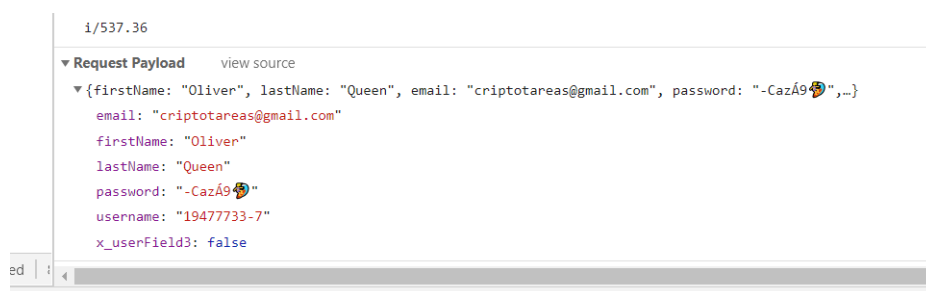


Figura 3: Datos enviados en texto plano

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

Como se observa en la imagen anterior, el user tiene nombre username (en este caso el rut), y la password con el nombre password. y la La variable utilizada para transmitir es un POST como se muestra a continuación:

Name	Method	Stat...	Type	Initiator	Size	Ti...	Waterfall
reset-password	POST	200	xhr	vendor_...	99...	60...	
cm?tid=10&ci=...	GET	(fail...		elumina...	0 B	1 ...	

Figura 4: Variable utilizada: POST

1.6. ¿Qué información se solicita para restablecer la contraseña? LLL

Para poder restablecer la contraseña sin iniciar sesión solo pide el RUT:

¿Olvidaste tu contraseña?

Ingresa tu RUT para buscar tu cuenta

RUT	19477733-7
Buscar cuenta	

Figura 5: Restablecer la contraseña

1.7. ¿Cómo opera el servicio de reestablecer contraseña? LLL

Una vez ingresado el RUT, el sistema muestra el correo asociado de forma parcial, avisando que se envió una contraseña temporal para cambiar la contraseña y acceder a la cuenta.

Luego, al correo asociado a la cuenta llega un mensaje con una contraseña temporal de 10 caracteres los cuales contienen números, letras minúsculas y mayúsculas y también símbolos.

Finalmente cuando se vuelve a ingresar a la pagina hay que ingresar la contraseña temporal y se cambia por una nueva contraseña. Como se muestra en las siguientes imágenes por orden. (Por otro lado no existe manera de cambiar la contraseña mientras se esta logueado.)



Figura 6: Notificación de correo electrónico

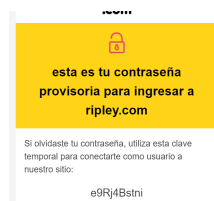


Figura 7: Contraseña temporal en el correo

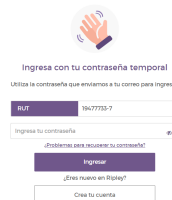


Figura 8: Validación por la contraseña temporal

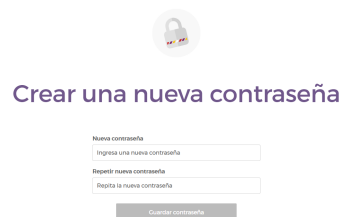


Figura 9: Nueva contraseña de usuario

1.8. ¿En el proceso de reseteo se expone información privada del usuario? LLL

En cierta medida si, ya que como se menciono anteriormente el sistema muestra el correo asociado de forma parcial.

1.9. ¿Qué patrón tiene la nueva contraseña al resetearla?

Utilizando la ego de automatización solicitada los resultados obtenidos son los siguientes:

h7NeypVHgV e9Rj4Bstni c8Rh9zfr83
s7IKA\$cydn r4UME5kCuy r6IRHsSU3X
y8M!PZrPuS d7F6E_XfTe z8KgchVn4G
m9SGNSvEMk

Figura 10: Contraseñas temporales

Como se puede observar, existen dos patrones que se cumplen en todas las contraseñas siendo el primero que todas tienen mayúsculas, minúsculas y al menos un número y el segundo patrón siendo este más exacto todavía es que todas parten con los tres mismos tipos de caracteres o sea cada contraseña parte con una minúscula luego un número y el tercer carácter una mayúscula. Aparte de lo anterior existen patrones parciales por decirlo de alguna manera ya que el 60 % de las claves contienen al menos dos números y también que 30 % de estas contiene un símbolo.

1.10. ¿El sitio recuerda contraseñas antiguas? LLL

El sitio no recuerda contraseñas antiguas ya que se puede volver a escribir la misma contraseña varias veces aunque se hubiese restablecido esa misma contraseña anteriormente.

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

Al hacer el ataque por FB los primeros intentos muestra un mensaje que dice "usuario o contraseña incorrectos" luego del cuarto intento de ingreso, empieza a arrojar un mensaje que dice que "no se puede hacer login en estos momentos". Luego si se sigue un intentando otras 15 veces apox bloquea la cuenta, arrojando otro mensaje que que dice "prima el botón olvide la contraseña", para de restablecer la contraseña a través del correo. Se puede corroborar que es un bloqueo ya que aunque después se coloque la contraseña correcta no ingresa y continua el mensaje anterior.

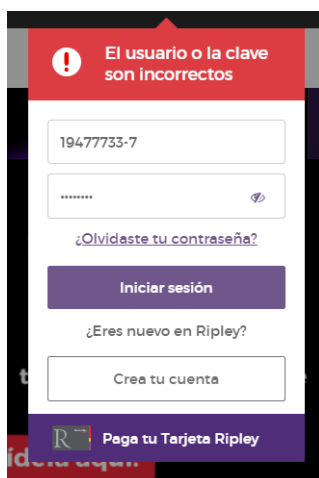


Figura 11: Nueva contraseña de usuario

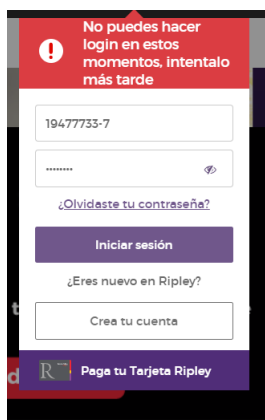


Figura 12: Nueva contraseña de usuario

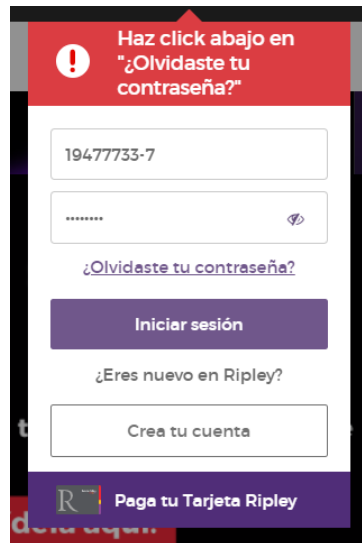


Figura 13: Nueva contraseña de usuario

1.12. ¿Existe la opción de eliminar su cuenta? LLL

El sitio no presenta la opción de eliminar la cuenta.

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

Teóricamente no porque el sitio afirma que la información de la cuenta no podrá ser leída ni capturada por terceros, siendo lo anterior falso ya que si se coloca el RUT de una persona en la parte de recuperación de contraseña puede saber si la persona tiene o no cuenta en la pagina y también muestra parcialmente el correo asociado al RUT. Además de demostrar que el envío de la contraseña no es seguro ya que se envía en texto plano.

2. Pagina europea

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

Al crear el usuario en esta pagina se pudo ver que el largo mínimo de la contraseña debe de ser de 5 caracteres y un máximo de 128 caracteres. Además, las bases Emojis por lo que contiene o permite todas las otras bases mas pequeñas.



Figura 14: Máxima y mínima cantidad de caracteres en la contraseña

Se puede apreciar que para crear la cuenta necesita una verificación por correo electrónico.



Figura 15: Verificación por correo electrónico

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

No ya que el largo mínimo/máximo está restringido desde el servidor.

2.3. ¿Existe comprobación de robustez de la password? LLL

Esta pagina no presenta comprobación de robustez de ningún tipo.

2.4. ¿Se transmite la contraseña en texto plano?

Al crear la cuenta se hizo una captura de paquetes para revisar si los datos verificar como se envinaban los datos descubriendo que se envían por texto plano como se comprueba en la siguiente imagen.

```
customerName: Barry Allen
email: criptotareas@gmail.com
password: -CazÁ9
passwordCheck: -CazÁ9
metadata1: ECdITeCs:jECDeL3gVj3wbVl
m1/Kbor5SmRF9RaatYL/Ps8aYYbWLnLxql
```

Figura 16: Datos enviados en texto pano

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

Como se observa en la imagen anterior, el user tiene nombre email (en este caso el correo), y la password con el nombre password. y la La variable utilizada para transmitir es un POST como se muestra a continuación:

<input type="checkbox"/>	request?arb=1e53ef66...	GET	200	docu...	/api/register	8.6 kB	737 ...			
<input type="checkbox"/>	register	POST	302	docu...	Other	1.5 kB	1.47 s			
<input type="checkbox"/>	pDxWAF1p880dzGB.w...	GET	200	font	images-eu...	(me...	0 ms			
<input type="checkbox"/>	KFPk-9iF4FgAqY-woff2	GET	200	font	images-eu...	(me...	0 ms			

Figura 17: Variable utilizada: POST

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

Para poder restablecer la contraseña sin iniciar sesión solo pide el user en este caso el email:



The screenshot shows the Amazon.es logo at the top. Below it, the heading "Ayuda de contraseña" is followed by the instruction: "Introduzca la dirección de correo electrónico o el número de teléfono móvil asociados con su cuenta de Amazon." There is a text input field labeled "E-mail o número de móvil" containing the email "criptotareas@gmail.com". Below the input field is a yellow button labeled "Continuar".

Figura 18: Confirmación de correo electrónico

2.7. ¿Cómo opera el servicio de reestablecer contraseña?

Una vez ingresado el email, el sistema muestra el correo asociado completo, avisando que se envió un código de verificación para cambiar la contraseña y acceder a la cuenta.

Luego, al correo asociado a la cuenta llega un código de 6 caracteres los cuales contienen solo números.

Finalmente cuando se vuelve a ingresar a la pagina hay que ingresar el código luego de verificarla cuenta se cambia la contraseña. Como se muestra en las siguientes imágenes por orden. (En este sitio si existe manera de cambiar la contraseña mientras se esta logueado.)



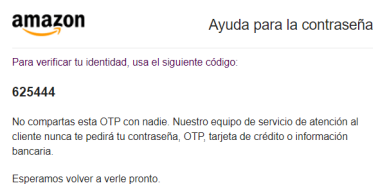
The screenshot shows the Amazon.es logo at the top. Below it, the heading "Verificación de inicio de sesión" is followed by the instruction: "Por la seguridad de tu cuenta, tenemos que verificar la titularidad de la misma. Hemos enviado un código a tu e-mail criptotareas@gmail.com. Introdúcelo a continuación." There is a text input field labeled "Escribir código". Below the input field is a yellow button labeled "Continuar". At the bottom, there are two links: "Volver a enviar código" and "Necesito más ayuda".

Figura 19: Variable utilizada: POST




The screenshot shows the Amazon.es interface for verifying an email address. At the top is the Amazon logo. The main heading is 'Verificar dirección de correo electrónico'. Below it, a message states: 'Para verificar tu email, te hemos enviado un código a criptotareas@gmail.com (Cambiar)'. There is a text input field labeled 'Escribir código'. Below the field is a yellow button labeled 'Cree tu cuenta de Amazon'. At the bottom, there is a link 'Volver a enviar código'.

Figura 20: Variable utilizada: POST



The screenshot shows the Amazon.es interface for password help. At the top is the Amazon logo and the heading 'Ayuda para la contraseña'. The text reads: 'Para verificar tu identidad, usa el siguiente código: 625444'. Below this, a warning states: 'No compartas esta OTP con nadie. Nuestro equipo de servicio de atención al cliente nunca te pedirá tu contraseña, OTP, tarjeta de crédito o información bancaria.' At the bottom, it says 'Esperamos volver a verte pronto.'

Figura 21: Variable utilizada: POST



The screenshot shows the Amazon.es interface for creating a password. At the top is the Amazon logo. The main heading is 'Crear contraseña'. Below it, a message states: 'Le pediremos esta contraseña siempre que inicie sesión.' There are two text input fields: 'Nueva contraseña' and 'Confirma tu contraseña'. Below the first field is a warning: 'La contraseña debe tener 6 caracteres como mínimo.' At the bottom is a yellow button labeled 'Guardar los cambios e iniciar sesión'.

Figura 22: Variable utilizada: POST

2.8. ¿En el proceso de reseteo se expone información privada del usuario?

Totalmente, ya que como se menciono anteriormente el sistema muestra el correo asociado completo aunque para que te manden el código de verificación se tiene que ingresar el correo por lo que al final te muestran algo que supuestamente ya conoces.

2.9. ¿Qué patrón tiene la nueva contraseña al resetearla?

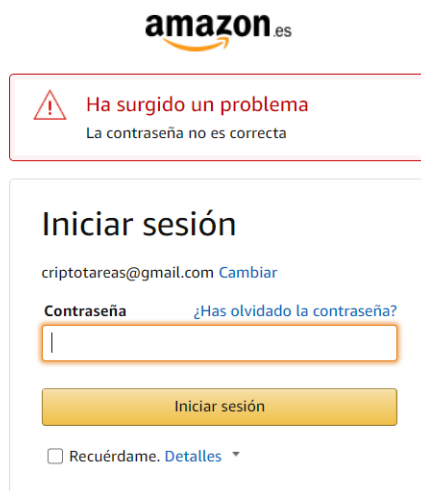
El código enviado al correo sigue un patrón estricto de 6 caracteres donde todos ellos son números.

2.10. ¿El sitio recuerda contraseñas antiguas?

El sitio no recuerda contraseñas antiguas ya que se puede volver a escribir la misma contraseña varias veces aunque se hubiese restablecido esa misma contraseña anteriormente.

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

Al hacer el ataque por FB los primeros intentos muestra un mensaje que dice "La contraseña no es correcta" luego del décimo intento de ingreso ocurre una de dos cosas. La primera te redirige automáticamente a la parte para restablecer la contraseña a través del correo y la segunda te pide hacer una verificación de si eres humano diciéndote que escribas la siguiente palabra. Pudo llegar a esta conclusión variando el tiempo de interacción con la pagina de 1 a 10 segundos. Se puede corroborar que esta vez no bloquea la cuenta ya que si después se coloca la contraseña correcta ingresa de manera normal.



The image shows the Amazon.es login interface. At the top is the Amazon logo. Below it is a red-bordered box with a warning icon and the text: "Ha surgido un problema" and "La contraseña no es correcta". Below this is the "Iniciar sesión" (Sign in) section. It displays the email "criptotareas@gmail.com" with a "Cambiar" (Change) link. There is a label "Contraseña" (Password) and a link "¿Has olvidado la contraseña?" (Forgot your password?). A password input field is shown with a single character. Below the input field is a yellow "Iniciar sesión" button. At the bottom, there is a checkbox for "Recuérdame" (Remember me) and a "Detalles" (Details) link.

Figura 23: Primeros fallos de contraseña



amazon.es

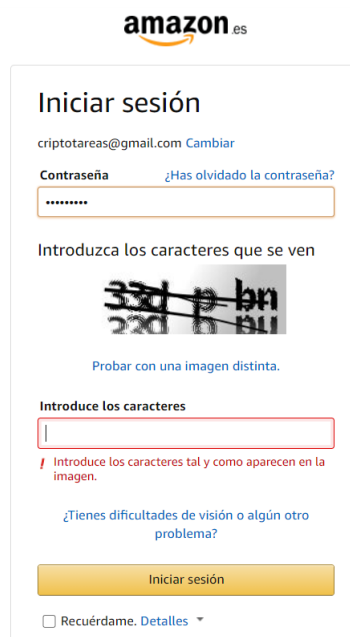
Ayuda de contraseña

Introduzca la dirección de correo electrónico o el número de teléfono móvil asociados con su cuenta de Amazon.

E-mail o número de móvil

Continuar

Figura 24: Después de 10 fallos a 10 seg cada fallo




amazon.es

Iniciar sesión

criptotareas@gmail.com [Cambiar](#)

Contraseña [¿Has olvidado la contraseña?](#)

Introduzca los caracteres que se ven



[Probar con una imagen distinta.](#)

Introduce los caracteres

! Introduce los caracteres tal y como aparecen en la imagen.

[¿Tienes dificultades de visión o algún otro problema?](#)

Iniciar sesión

☐ Recuérdame. [Detalles](#) ▾

Figura 25: Después de 10 fallos a 1 seg cada fallo

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

El sitio si presenta la opción de eliminar la cuenta y no deja rastro de la cuenta ya que se puede volver a crear la cuenta con el mismo correo que se uzo anteriormente y la misma contraseña también.

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

Teóricamente no porque al ingresar a la parte de las políticas de seguridad específicamente a la sección de Amazon y mis datos el sitio no muestra ninguna de información al respecto de hecho no muestra nada de nada por lo que se podría afirmar que no tiene políticas de seguridad cibernética. Además de demostrar que el envío de la contraseña no es seguro ya que se envía en texto plano.

3. LInk Guthub