

Tarea 1

Christian Muñoz
`christian.munoz1@mail.udp.cl`

Índice general

1. Introducción	2
2. New Game	3
2.1. Información Básica	3
2.2. Creación de la cuenta	4
2.2.1. Usuario y Correo	5
2.2.2. Clave	5
2.3. Envío de Datos	5
2.4. Modificar, Restablecer y Eliminar Datos	5
2.5. Información Almacenada	6
2.6. Políticas del Sitio	6
2.7. Fuerza Bruta	6
3. Versus Gamers	7
3.1. Información Básica	7
3.2. Creación de la cuenta	7
3.2.1. Usuario y Correo	7
3.2.2. Clave	7
3.3. Envío de Datos	8
3.4. Modificar, Restablecer y Eliminar Datos	9
3.5. Información Almacenada	10
3.6. Políticas del Sitio	10
3.7. Fuerza Bruta	10

1. Introducción

En el presente informe se auditarán 2 paginas web, una chilena y una europea, con el fin de analizar la seguridad que tienen sus cuentas, la factibilidad de realizar ataques de fuerza bruta, sus políticas de privacidad y seguridad. Se analizaran varios aspectos para finalmente lograr una comprensión del comportamiento real de las paginas versus sus políticas y la sensibilidad de la información que manejan.

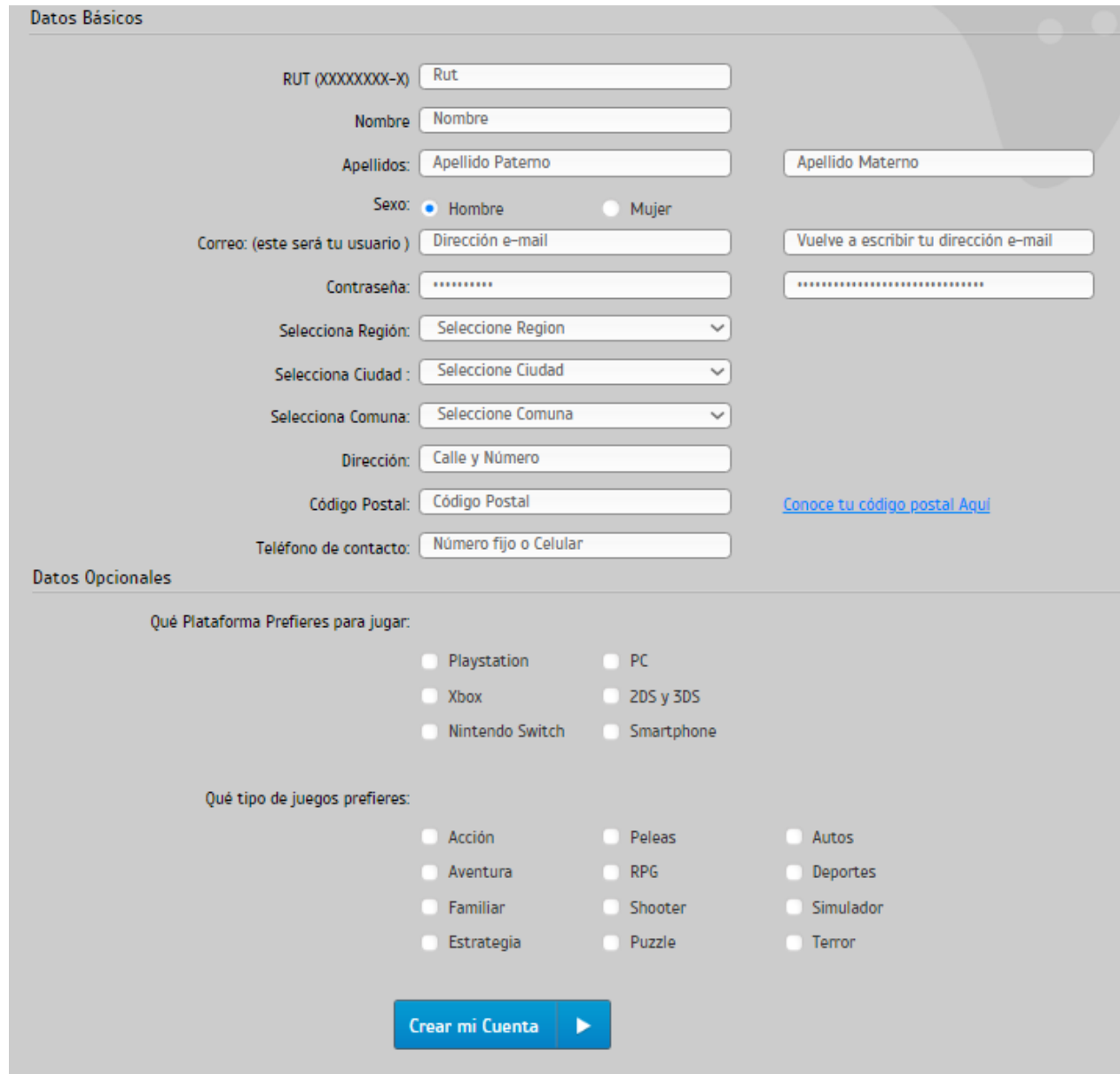
2. New Game

2.1. Información Básica

New Game es una tienda que realiza ventas de componentes electrónicos relacionados al mundo gamer de forma física y online mediante la pagina web que se auditara.

2.2. Creación de la cuenta

Crear una cuenta en esta pagina es un poco más lento que en sus pares dado que pide más datos de lo común con el fin de verificar de forma inmediata la mayor cantidad de datos posibles al momento de la creación de la cuenta y no al momento de la primera compra. Estos datos se pueden ver más en detalle en la siguiente imagen.



Datos Básicos

RUT (XXXXXXXX-X)

Nombre

Apellidos:

Sexo: ☒ Hombre ☐ Mujer

Correo: (este será tu usuario)

Contraseña:

Selecciona Región:

Selecciona Ciudad:

Selecciona Comuna:

Dirección:

Código Postal: [Conoce tu código postal Aquí](#)

Teléfono de contacto:

Datos Opcionales

Qué Plataforma Prefieres para jugar:

☐ Playstation ☐ PC

☐ Xbox ☐ ZDS y 3DS

☐ Nintendo Switch ☐ Smartphone

Qué tipo de juegos prefieres:

☐ Acción ☐ Peleas ☐ Autos

☐ Aventura ☐ RPG ☐ Deportes

☐ Familiar ☐ Shooter ☐ Simulador

☐ Estrategia ☐ Puzzle ☐ Terror

Figura 2.1: Formulario de registro.

2.2.1. Usuario y Correo

De los datos que pide, los únicos que realmente verifica son el RUT y la clave, todos los demás datos quedan a responsabilidad del usuario, con la salvedad de que al elegir región limita la selección de ciudades a esa región y lo mismo sucede entre ciudad y comuna. Se debe mencionar que el "usuario" de la página es el correo y no el nombre que se ingresa, en general no se ocupa ni muestra ninguno de los otros datos hasta el momento de verificar la compra y los datos del envío.

2.2.2. Clave

La clave se deja a libre elección del usuario, es decir, no realiza ninguna verificación de largo mínimo, robustez, etc. Aunque algo muy curioso es que en el código fuente se especifica un máximo de 40 caracteres, el cual no se informa en ningún momento al usuario y al momento de ingresar esta clave, ya sea al crear la cuenta o al modificar los datos, esta es admitida por la página pero al tratar de iniciar sesión esta no es válida, lo más probable es que el servidor o la base de datos corte la clave o tenga problemas al procesarla.



Figura 2.2: Único parámetro de la clave.

2.3. Envío de Datos

El envío de datos en todo momento se envía en texto plano por parte de la página, no se aprecia ningún tipo de ofuscación, hash, ni encriptado. Además el envío de datos se realiza mediante una petición GET.

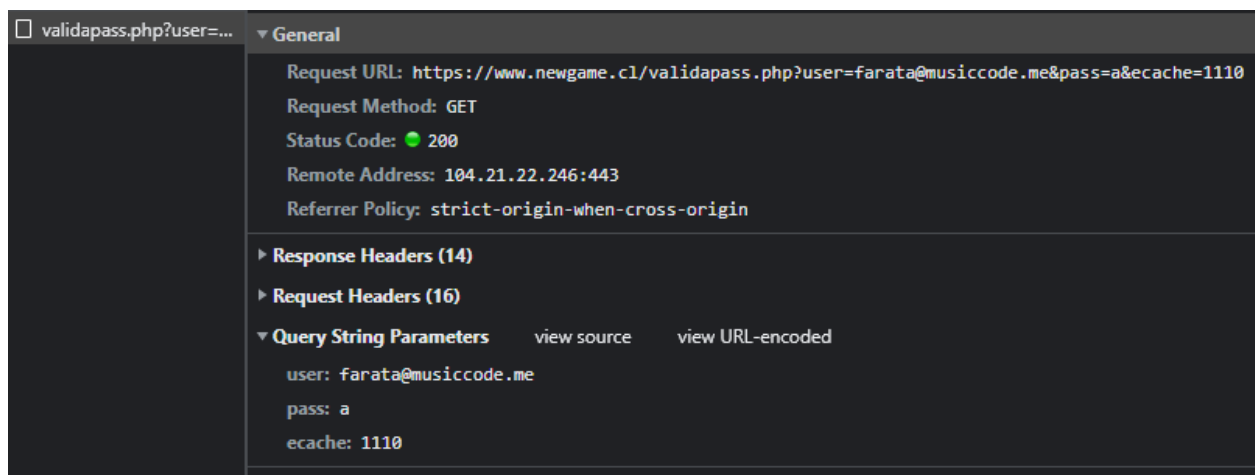


Figura 2.3: Petición de Inicio de Sesión.

2.4. Modificar, Restablecer y Eliminar Datos

La modificación no tiene mucha ciencia, es solamente llenar el mismo formulario de registro los nuevos datos en el campo correspondiente y listo.

A la hora de restablecer la contraseña, en el supuesto de que se olvidó, se solicita una dirección de correo cualquiera, y luego de verificar si corresponde a un usuario se procede a enviar un correo como el que se muestra a continuación.

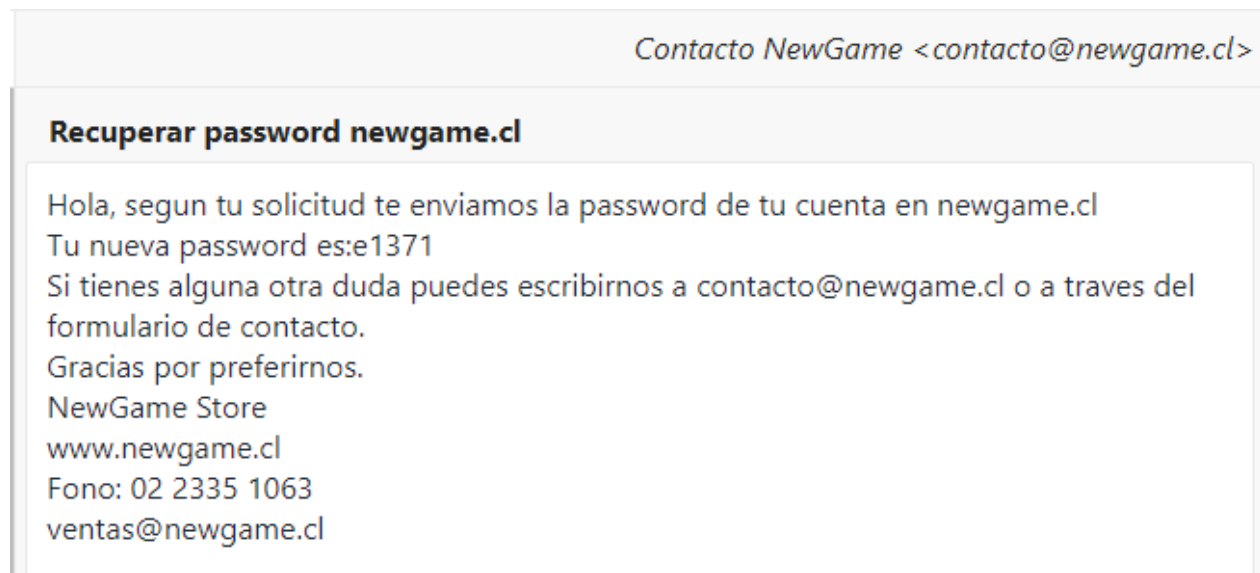


Figura 2.4: Correo con la nueva clave.

Todos los correos tienen la misma estructura, lo único que cambia es la clave la cual en todos los correos posee un largo de 5 caracteres y su base es [a-z0-9].

La eliminación de cuentas no esta implementada por lo que la cuenta fake que se a creado posee un RUT, generado por una pagina web la cual fue dada de baja, probablemente pertenezca a una persona real, a la cual le causara problemas si algún día le interesa crearse una cuenta.

2.5. Información Almacenada

El sitio no almacena datos antiguos, todo se sobrescribe una vez se modifica.

2.6. Políticas del Sitio

Este sitio no posee ningún tipo de políticas, al menos no se muestran a simple vista en su pagina web. Lo cual es un problema ético dado que el usuario desconoce de que forma se van a manejar sus datos y que se va a hacer con ellos. Así mismo, el usuario no esta en la obligación de suministrar datos reales a excepción del destino de envío de las compras. Por lo tanto aquellos que no posean un segundo apellido, por ejemplo, no deben preocuparse por eso y pueden directamente rellenar con cualquier carácter que estimen conveniente.

2.7. Fuerza Bruta

A simple vista no pareciera ser factible realizar ataques de fuerza bruta dado que el sitio acepta todo lo que se le ingresa en el campo de la contraseña, pero, dado que el sitio mismo informa cuando se tiene un correo de un usuario existente se puede solicitar restablecer la contraseña de ese correo y seria solo cuestión de un par de horas, en el peor caso posible, acceder a la cuenta, dada la base de la clave restablecida.

3. Versus Gamers

3.1. Información Básica

Versus Gamers es una tienda que realiza ventas de componentes electrónicos dedicados al mundo gamer amateur y profesional de forma online mediante la pagina web que se auditará.

3.2. Creación de la cuenta

Crear una cuenta en esta pagina es más simple y fácil que en el sitio anterior, dado que solo pide lo más básico y fundamental como se ve en la siguiente imagen.

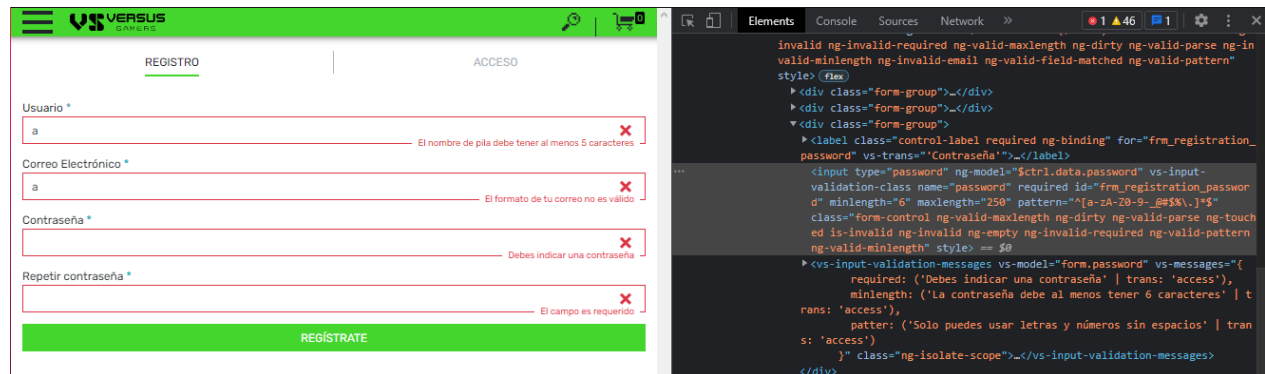


Figura 3.1: Formulario de registro.

3.2.1. Usuario y Correo

Este sitio funciona tanto con el correo o con el nombre de usuario a la hora de validar el inicio de sesión y a diferencia de New Game, que funciona en base al correo, este sitio se refiere al usuario con el "nombre" que el define. Estos datos están sujetos solo a la validación del correo mediante un link que se envía al mismo.

3.2.2. Clave

Como se puede ver en la figura 3.1, la clave debe tener entre 6 y 250 caracteres, los cuales deben pertenecer a la base `^[a-zA-Z0-9-@#$%&.]*$`. Estas restricciones no se pueden quitar en el cliente.

3.3. Envío de Datos

El envío de datos en todo momento se envía en texto plano por parte de la pagina, no se aprecia ningún tipo de ofuscación, hash, ni encriptado. Además el envío de datos se realiza mediante una petición POST.

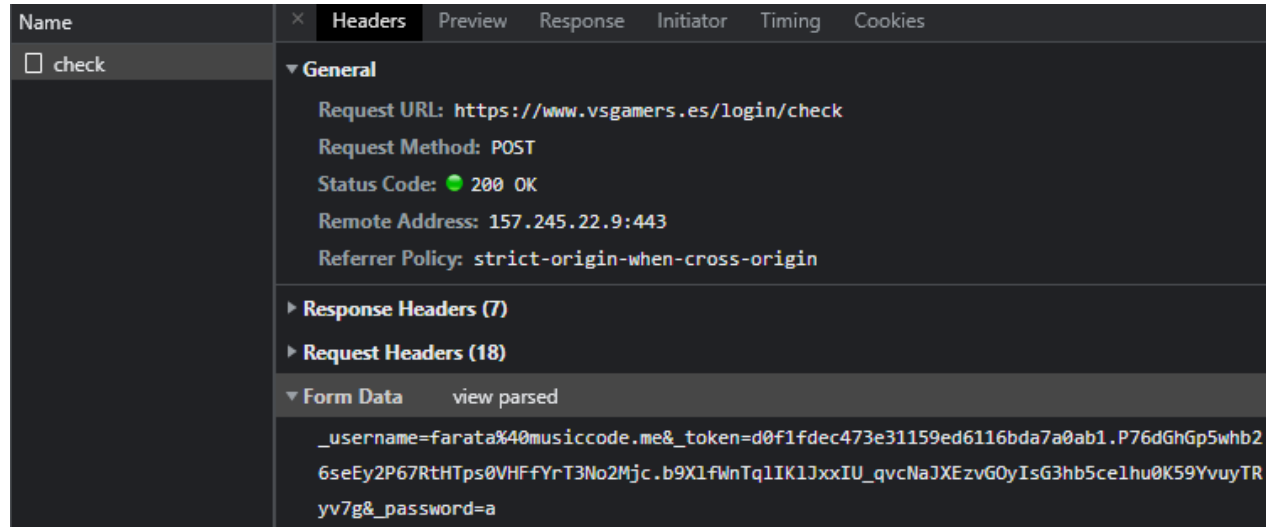


Figura 3.2: Petición de Inicio de Sesión.

3.4. Modificar, Restablecer y Eliminar Datos

Ala hora de modificar los datos se presentan los mismos campos que en el registro, pero además se dan las opción de agregar direcciones, datos de envío y puntos de recogida. Como curiosidad, a la hora de cambiar de contraseña no se realiza ninguna verificación sobre la nueva clave.

A la hora de restablecer la contraseña, en el supuesto de que se olvido, se solicita una dirección de correo cualquiera, y luego de verificar si corresponde a un usuario se procede a enviar un correo como el que se muestra a continuación.

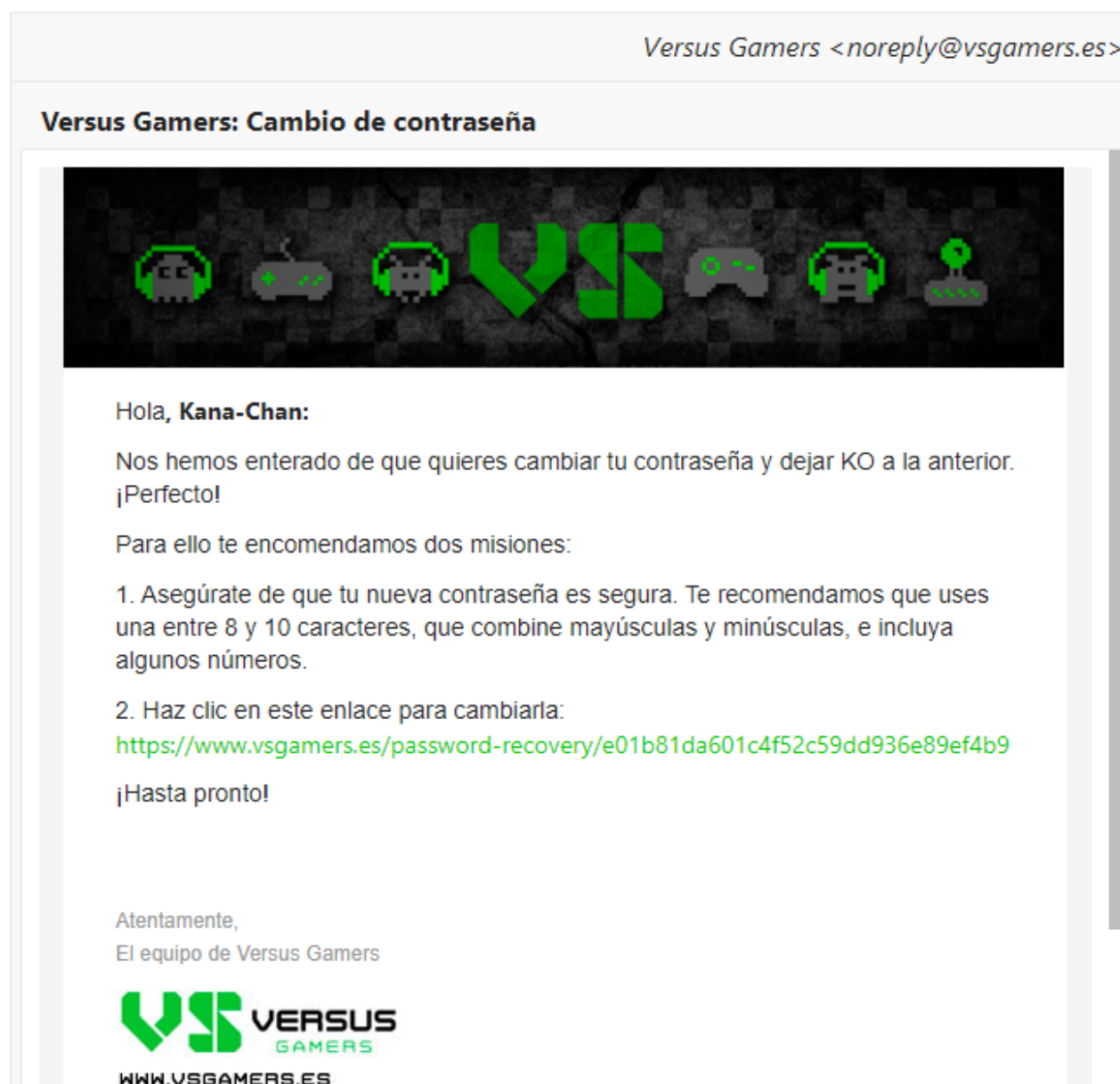


Figura 3.3: Correo con el enlace para cambiar la clave.

La ultima parte del enlace esta compuesta por un string con base [a-z0-9] de largo variable, el cual puede llegar a superar los 30 caracteres.

La eliminación de cuentas no esta implementada, pero al no pedir ningún dato que deba ser 100 % veridico, por ejemplo el RUT, no existe ningún problema con crear infinitas cuentas fake.

3.5. Información Almacenada

El sitio no almacena datos antiguos, todo se sobrescribe una vez se modifica.

3.6. Políticas del Sitio

Este sitio si informa sobre sus políticas de privacidad, en la cual, a grandes rasgos, informa sobre el tratamiento de los datos suministrados y quienes pueden acceder a ellos, además informa que asume todos los datos proporcionados como verídicos, por lo que no se hace responsable en caso de, por ejemplo, una dirección de envío que no existe o no es la correcta.

Se debe mencionar que aclaran que los datos del usuario solo serán utilizados con su consentimiento explícito y cuando el usuario decida retirar su consentimiento sus datos serán eliminados de los sistemas correspondiente a la brevedad anulando cualquier acción en curso, mientras no exista un impedimento de fuerza mayor como una acción judicial.

3.7. Fuerza Bruta

Dado que se aplican restricciones a la clave cuando se crea una cuenta es posible lanzar un ataque con fuerza bruta en búsqueda de claves con pocos caracteres, más de 6, lo cual ya depende del usuario. El truco de restablecer la contraseña no es útil para este fin dado que lograr completar correctamente una url que puede llegar a tener más de 30 caracteres es menos probable que encontrar un usuario con una clave menor a 20 caracteres.