

# Informe Laboratorio 3

## Sección 1

Diego Martin Espinoza  
e-mail: [diego.martin@mail.udp.cl](mailto:diego.martin@mail.udp.cl)

Mayo de 2025

# Índice

<b>1. Descripción de actividades</b>	<b>3</b>
<b>2. Desarrollo de actividades según criterio de rúbrica</b>	<b>4</b>
2.1. Identifica el algoritmo de hash utilizado al momento de registrarse en el sitio	5
2.2. Identifica el algoritmo de hash utilizado al momento de iniciar sesión . . . .	8
2.3. Genera el hash de la contraseña desde la consola del navegador . . . . .	10
2.4. Intercepta el tráfico login con BurpSuite . . . . .	11
2.5. Realiza el intento de login por medio del hash . . . . .	13
2.6. Identifica las políticas de privacidad o seguridad . . . . .	17
2.7. Comente 4 conclusiones sobre la seguridad del sitio escogido . . . . .	18

## 1. Descripción de actividades

Su objetivo será auditar la implementación de algoritmos hash aplicados a contraseñas en páginas web desde el lado del cliente, así como evaluar la efectividad de estas medidas contra ataques de tipo Pass the Hash (PtH). Para llevar a cabo esta auditoría, deberá registrarse en un sitio web y crear una cuenta, ingresando una contraseña específica para realizar las pruebas.

Al concluir la tarea, es importante que modifique su contraseña por una diferente para garantizar su seguridad.

Dado que la cantidad de sitios chilenos que utilizan hash es limitada, se permite realizar esta tarea en cualquier sitio web a nivel mundial. En este sentido, realice las siguientes actividades:

- Identificación del algoritmo de hash utilizado para las contraseñas al momento del registro en el sitio.
- Identificación del algoritmo de hash utilizado para las contraseñas al momento de iniciar sesión.
- Generación del hash de la contraseña desde la consola del navegador, partiendo de la contraseña en texto plano.
- Interceptación del tráfico de login utilizando BurpSuite desde su equipo.
- Realización de un intento de login modificando la contraseña por una incorrecta haciendo uso del hash obtenido en el punto anterior. Puede interceptar el tráfico y modificar el hash por el correcto o hacer uso del servicio repeater de BurpSuite.
- Descripción de las políticas de privacidad o seguridad relacionadas con las contraseñas, incluyendo un enlace a las mismas.
- Cuatro conclusiones sobre la seguridad o vulnerabilidad de la implementación observada.

## 2. Desarrollo de actividades según criterio de rúbrica

Para el desarrollo de las actividades de este laboratorio se utilizara un correo electrónico temporal, y se desarrollarnán las actividades para la página <https://www.pardus.at/>.

Las credenciales utilizadas son:

- Correo electrónico: ***laboratorio3cys@mailinator.com***
- Contraseña: ***password123***

Para una comparación y verificación más fácil también se guardan los hash md5 del correo y la contraseña, calculados en la página <https://www.md5hashgenerator.com/>:

- Hash Correo: **c82d97e56122efc5916e42a59e0cb0d3**
- Hash Contraseña: **482c811da5d5b4bc6d497ffa98491e38**

### MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

laboratorio3cys@mailinator.com

Generate →

Your String	laboratorio3cys@mailinator.com
MD5 Hash	c82d97e56122efc5916e42a59e0cb0d3 <button>Copy</button>

Figura 1: Hash MD5 Correo.

## MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

password123

Generate →

Your String	password123
MD5 Hash	482c811da5d5b4bc6d497ffa98491e38 <button>Copy</button>

Figura 2: Hash MD5 Password.

### 2.1. Identifica el algoritmo de hash utilizado al momento de registrarse en el sitio

El registro de un nuevo usuario no utiliza un algoritmo de hash, si no que maneja la información en texto plano. Esto se puede ver inspeccionando el código de la página, y también interceptando, con BurpSuite, el tráfico generado al momento de registrarse.

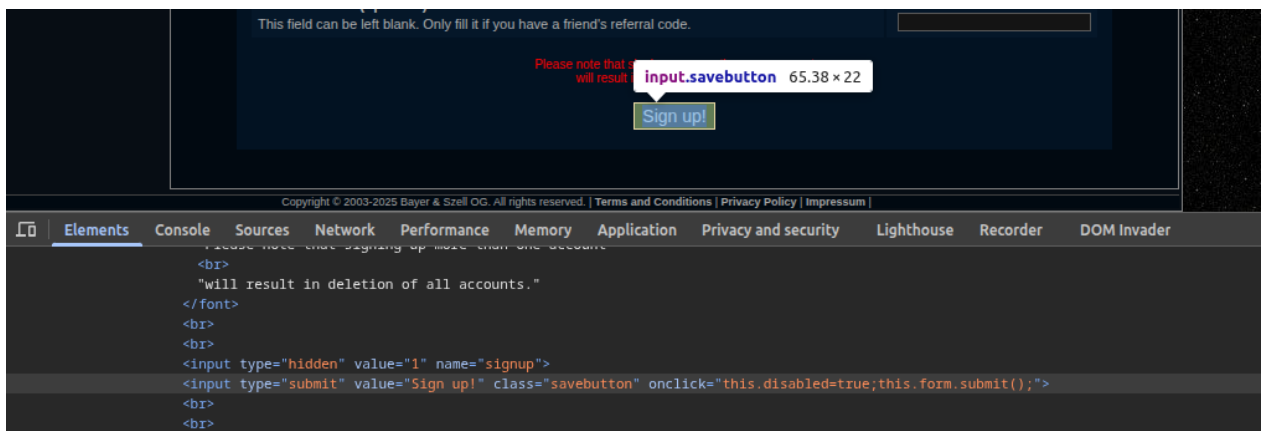


Figura 3: Inspección de elemento SignUp.

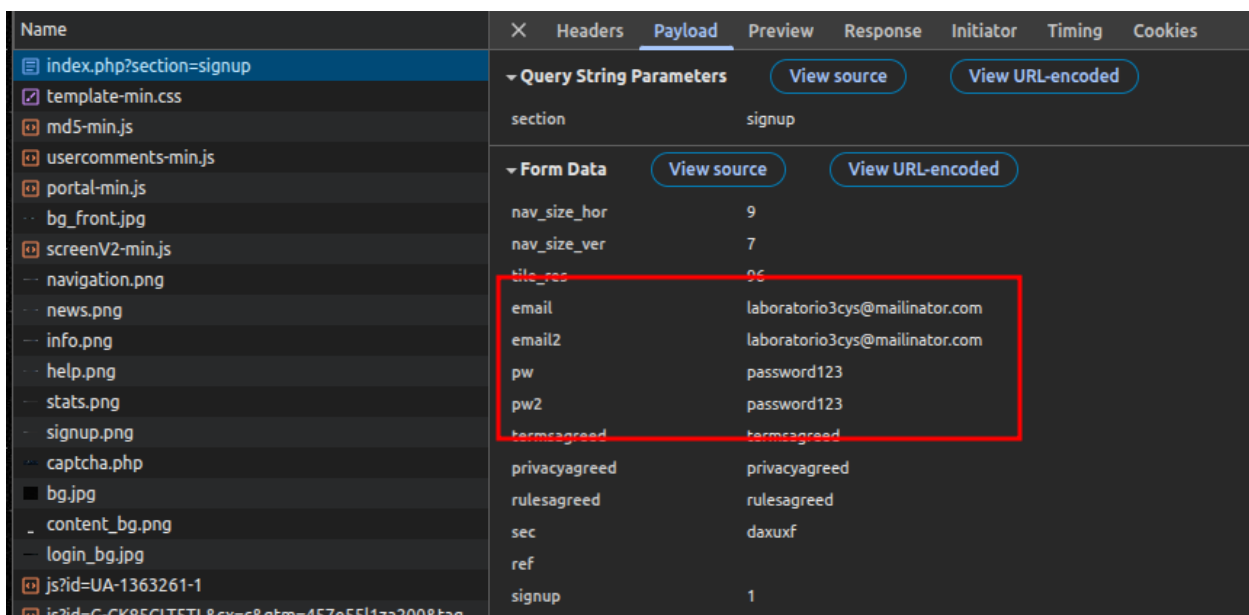


Figura 4: Request SignUp.

Y como se puede observar en el request generado por la página, se envía el correo y la contraseña en texto plano, por lo que no hay un Hash involucrado en el registro.

Se deja constancia de los siguientes pasos del registro.

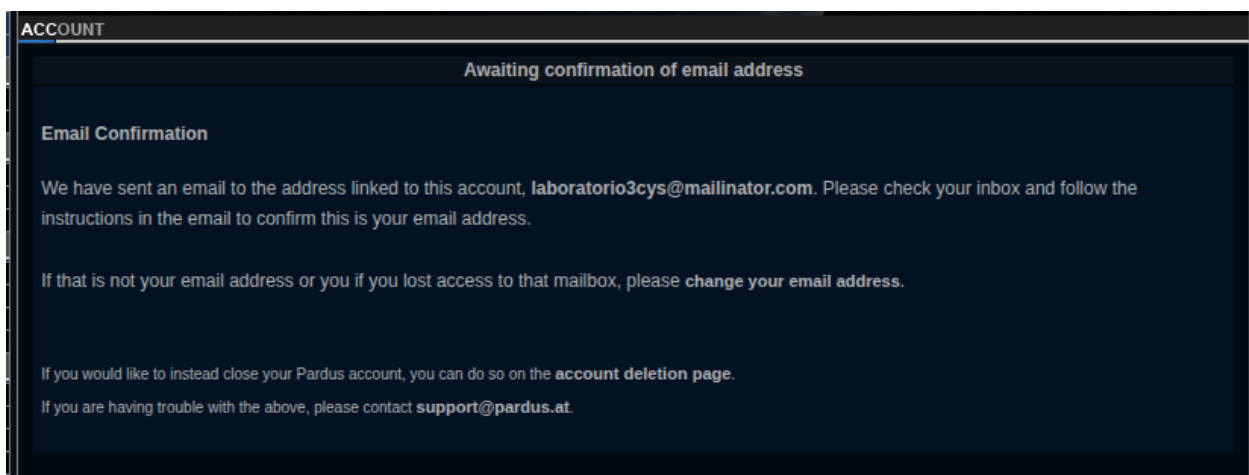


Figura 5: Registro 1.

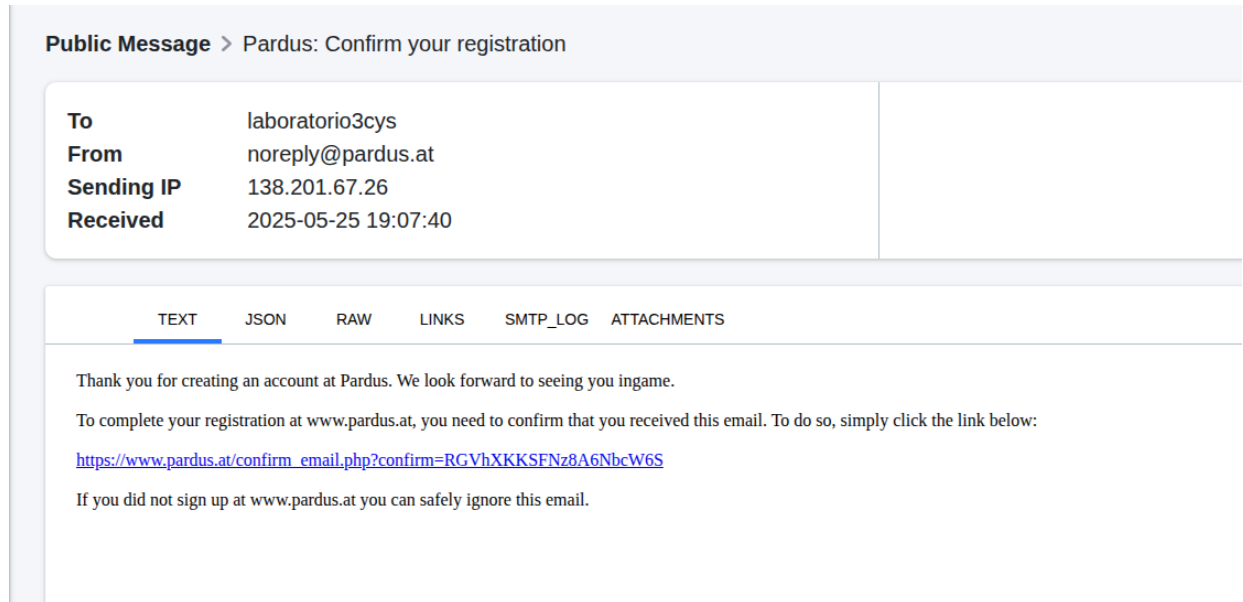


Figura 6: Registro 2.

The screenshot shows a web interface for creating a new character. At the top, a 'STATS' section displays: Online characters: 102, Active characters: 7,672, and Registered characters: 459,795. Below this is an 'ACCOUNT' section. The main area is titled 'New Character' and contains a confirmation message: 'Thank you for confirming your email address!'. The form is divided into three main sections: 'Character Name', 'Sex', and 'Universe'. The 'Character Name' section has a text input field and links for 'Naming Rules' and 'Why Naming Rules?'. The 'Sex' section has a dropdown menu currently set to '-- Please choose --'. The 'Universe' section includes a description of the game's universes and a key for population levels: green for 'sparsely populated (signup recommended)', blue for 'averagely populated', red for 'densely populated (signup not recommended)', orange for 'full (signup open to Premium Accounts only)', and yellow for 'premium (signup open to Premium Accounts only)'. To the right of the 'Universe' section is a table with three rows, each representing a universe: Artemis (green circle), Orion (blue circle), and Pegasus (yellow circle). Each row has a 'Please Choose' column with a radio button and a 'Name' column with the universe's name and icon. At the bottom of the form is a 'Create' button. The footer contains copyright information: 'Copyright © 2003-2025 Bayer & Szell OG. All rights reserved. | Terms and Conditions | Privacy Policy | Impressum |'.

Please Choose	Name
<input type="radio"/>	Artemis
<input type="radio"/>	Orion
<input type="radio"/>	Pegasus

Figura 7: Registro 3.

## 2.2. Identifica el algoritmo de hash utilizado al momento de iniciar sesión

Para poder identificar el algoritmo de Hash, se ingresa a la página de Login y luego desde el botón de login se inspecciona elemento para ver el código de la página. Luego desde el botón de login se puede ver lo que este hace, y que funciones llama, en este caso llama la función MD5.



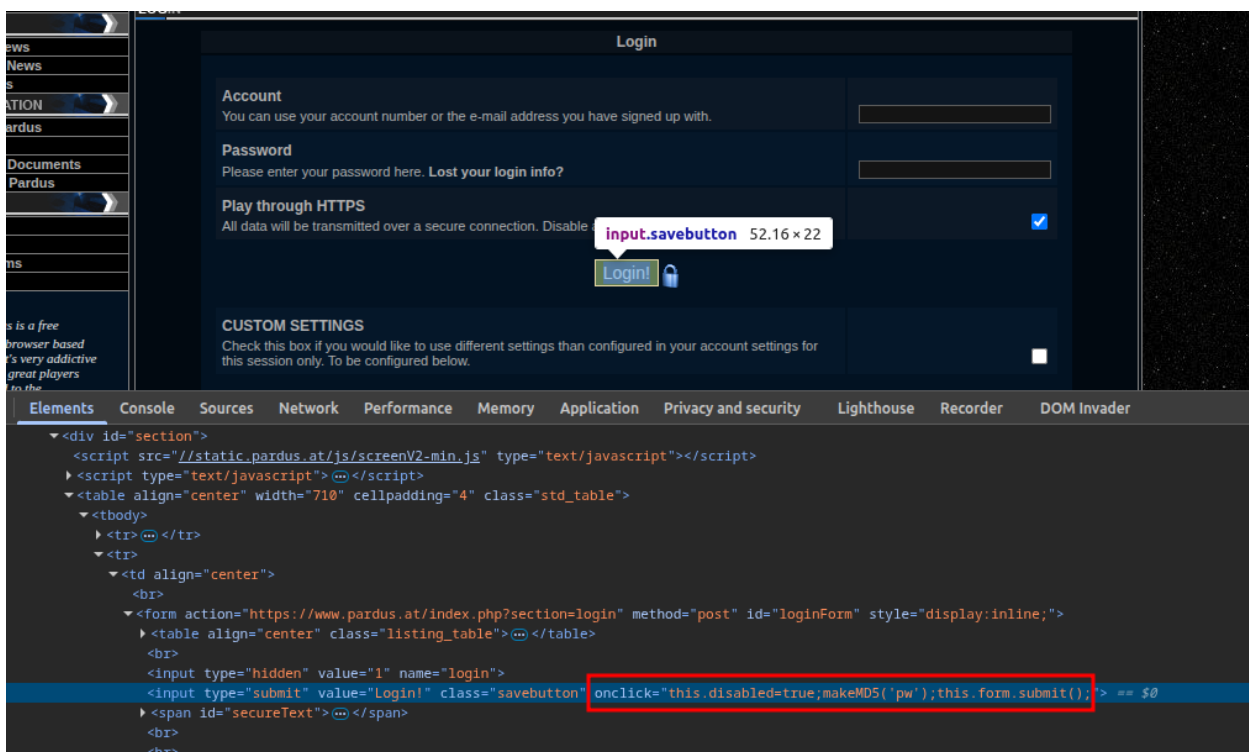


Figura 8: Inspección de elemento Login

Luego observando el payload del paquete enviado, se puede comparar con el Hash del calculador de Hash obtenido al inicio y estos coinciden.

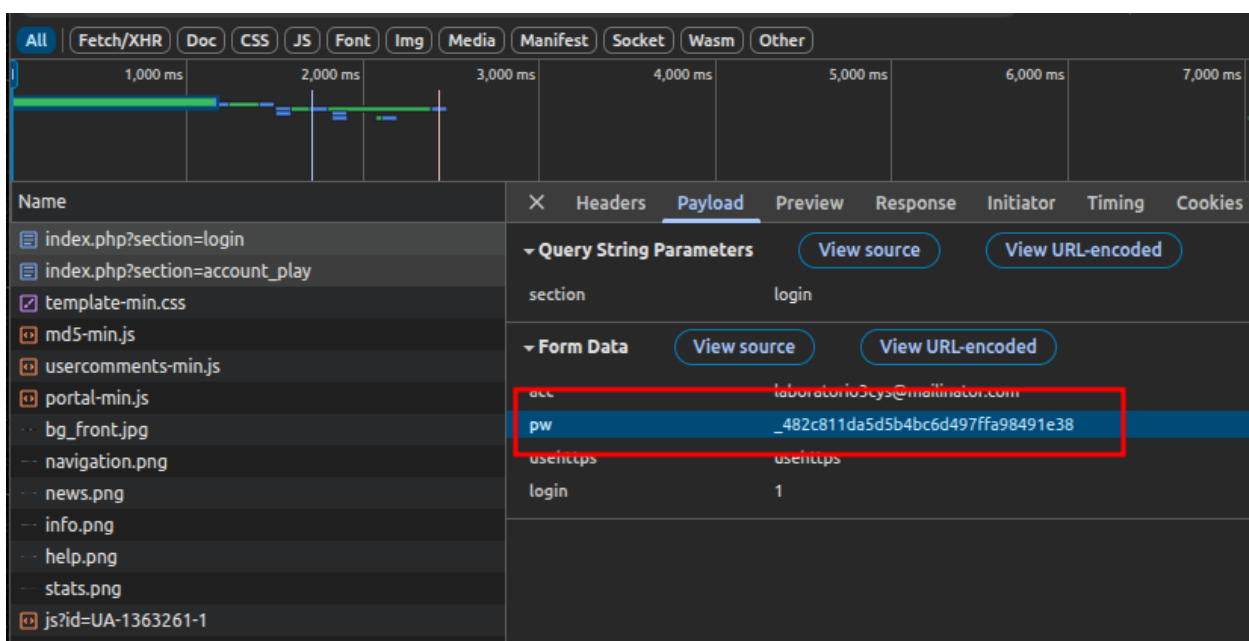


Figura 9: Hash Login.

### 2.3. Genera el hash de la contraseña desde la consola del navegador

Como fue mencionado antes, el usuario y la contraseña utilizados fueron para este caso, *laboratorio3cys@mailinator.com* y *password123*. Utilizando un calculador de Hash MD5 para la contraseña se obtiene *482c811da5d5b4bc6d497ffa98491e38*.

Para generar el Hash MD5 de la contraseña através de la consola, primero se debe buscar si es que la función existe en el código de la página.

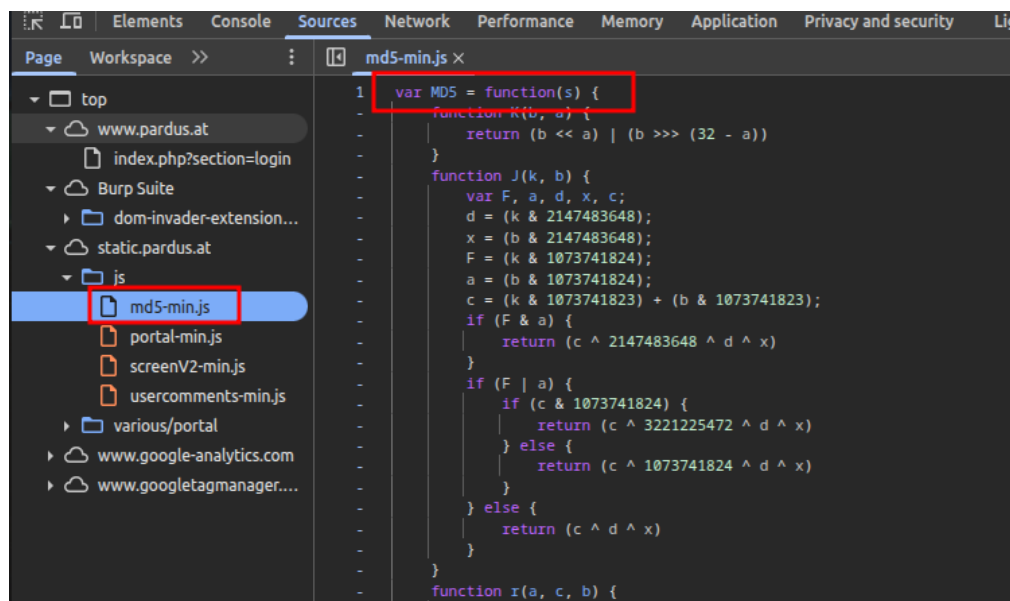


Figura 10: Función Hash MD5 en el js.

Luego se ejecuta el comando desde para hacer el hash MD5 desde la consola, con la contraseña *password123*:

```
MD5("password123")
```

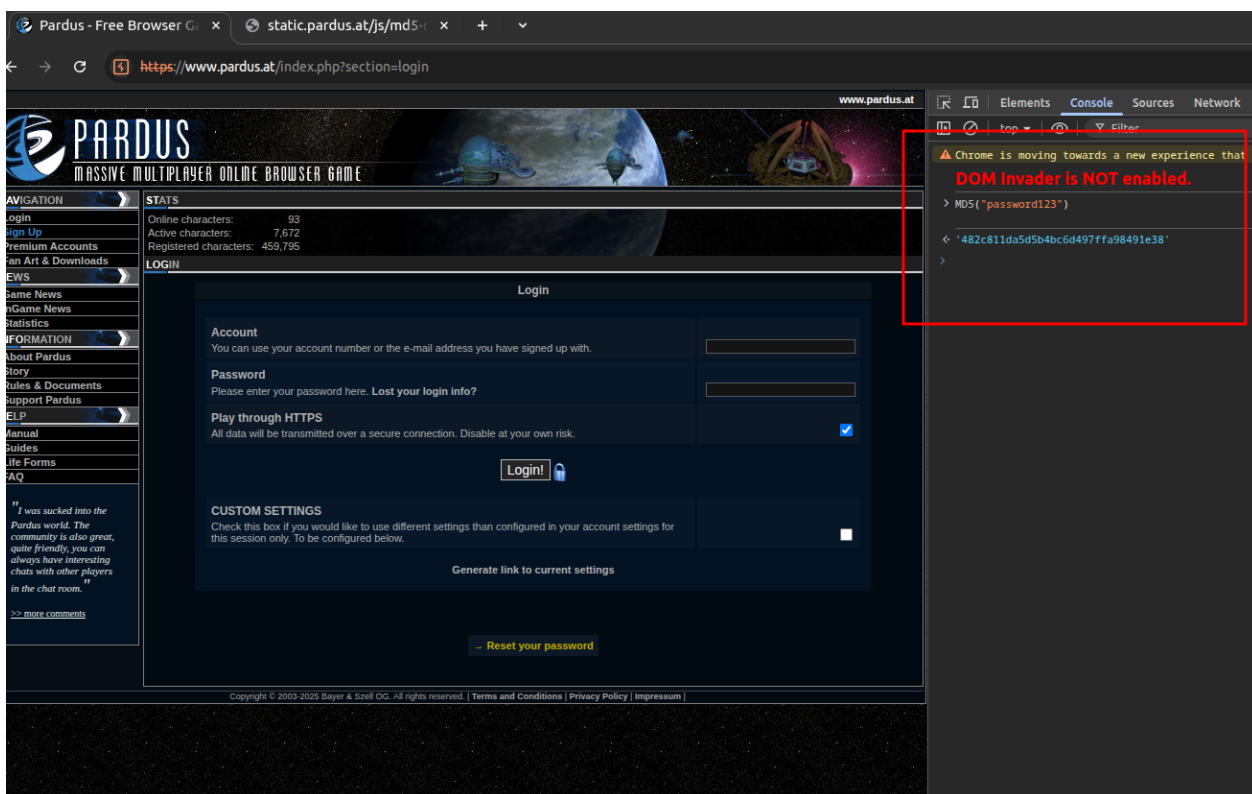


Figura 11: Hash de la contraseña desde la consola.

Una vez obtenido el hash de la contraseña desde la consola, se compara con la contraseña obtenida desde el calculador de hash, y se ve que ambas coinciden, por lo que el hash hecho desde la consola es correcto.

## 2.4. Intercepta el tráfico login con BurpSuite

Para interceptar el tráfico del login con BurpSuite se debe abrir la página web del login desde el navegador de BurpSuite y se comienza a interceptar el tráfico. En la página web se ingresa el correo registrado (*laboratorio3cys@mailinator.com*), y una contraseña incorrecta cualquiera, en este caso se utilizó *password*.

**PARDUS**  
MASSIVE MULTIPLAYER ONLINE BROWSER GAME

**NAVIGATION**

- Login
- Sign Up
- Premium Accounts
- Fan Art & Downloads

**NEWS**

- Game News
- InGame News
- Statistics

**INFORMATION**

- About Pardus
- Story
- Rules & Documents
- Support Pardus

**HELP**

- Manual
- Guides
- Life Forms
- FAQ

*"I've played Runescape, Pardus, Travian, and Tibia. Only Pardus has kept my attention."*  
[>> more comments](#)

**STATS**

- Online characters: 103
- Active characters: 7,672
- Registered characters: 459,795

**LOGIN**

**Account**  
You can use your account number or the e-mail address you have signed up with.

**Password**  
Please enter your password here. [Lost your login info?](#)

**Play through HTTPS**  
All data will be transmitted over a secure connection. Disable at your own risk. ☒

**Login!**

**CUSTOM SETTINGS**  
Check this box if you would like to use different settings than configured in your account settings for this session only. To be configured below. ☐

[Generate link to current settings](#)

[Reset your password](#)

Copyright © 2003-2025 Bayer & Szell OG. All rights reserved. | [Terms and Conditions](#) | [Privacy Policy](#) | [Impressum](#)

Figura 12: Login.

Time	Type	Direction	Method	URL
19:38:50 25 May 20...	HTTP	→ Request	POST	https://www.pardus.at/index.php?section=login

Request	
Pretty	Raw
<pre> 1 POST /index.php?section=login HTTP/2 2 Host: www.pardus.at 3 Cookie: gid=GA1.2.1679391004.1748210834; captcha_id=3621982; _ga_CK85CLT5TL=GS2.1.s1748210833\$o1\$g1\$t1748216223\$j0\$10\$h0; _ga=GA1.2.584790842.1748210834 4 Content-Length: 99 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://www.pardus.at 11 Content-Type: application/x-www-form-urlencoded 12 Upgrade-Insecure-Requests: 1 13 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://www.pardus.at/index.php?section=login 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 acc=laboratorio3cys%40mailinator.com&amp;pw=_1a36591bceec49c832079e270d7e8b736usehttps=usehttps&amp;login=1 </pre>	

Figura 13: Obtención Login en BurpSuite.

## 2.5. Realiza el intento de login por medio del hash

Una vez interceptado el tráfico del login incorrecto, se envía al intruder para hacer un Pass The Hash con disintos Hashes y contraseñas.

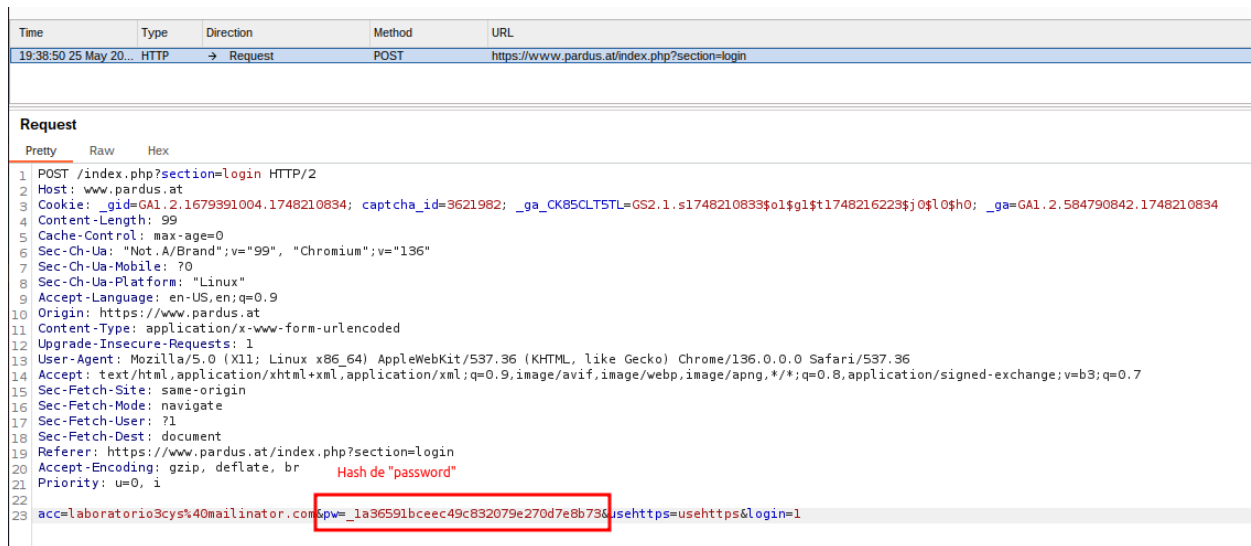


Figura 14: Login Request BurpSuite.

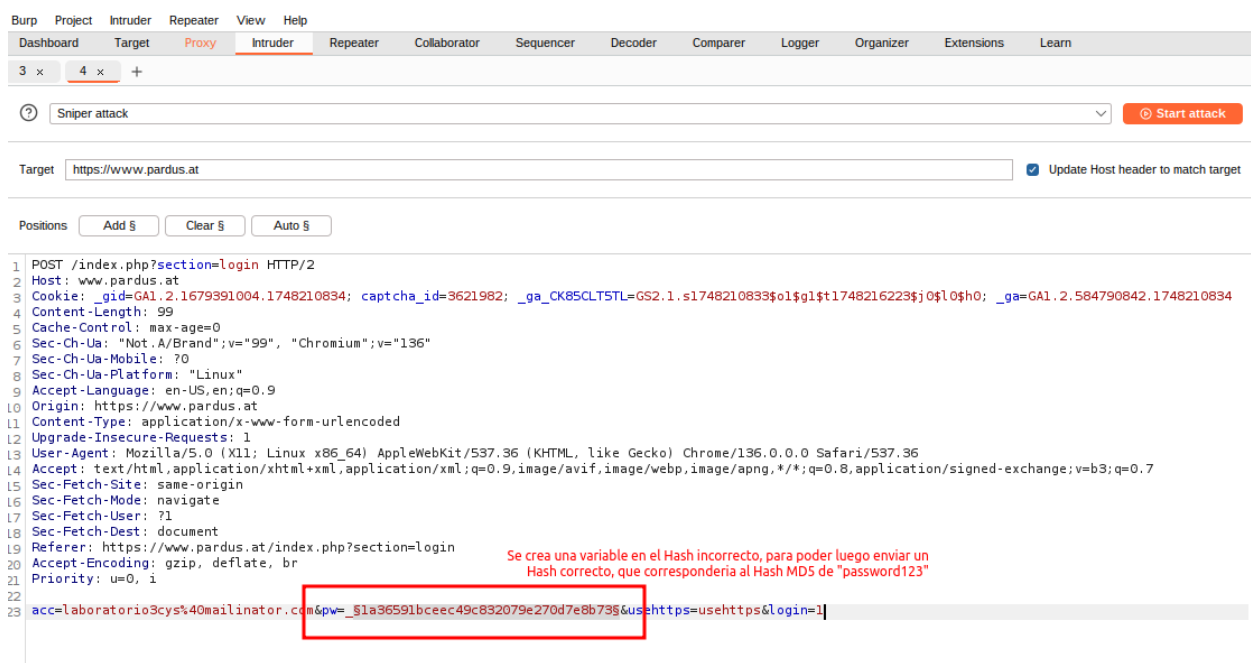
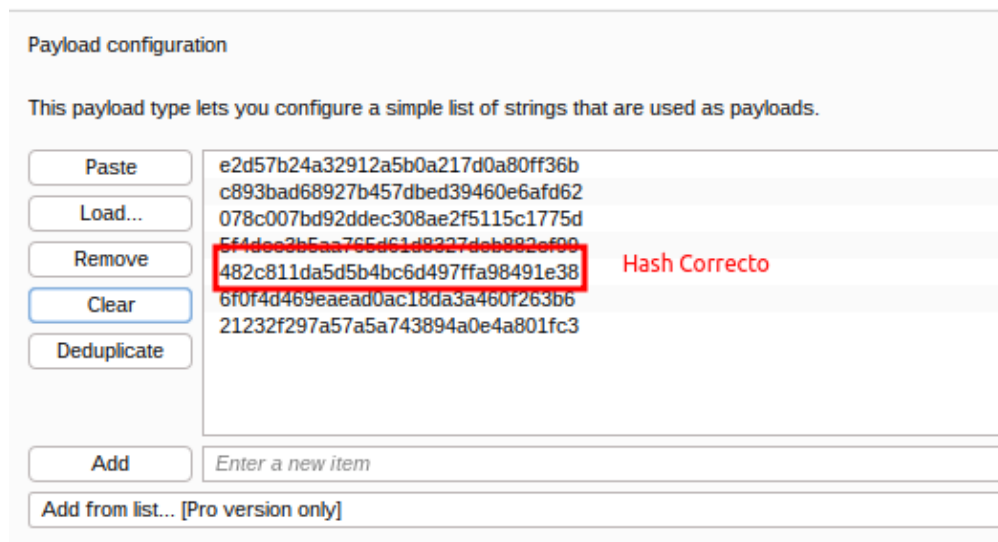


Figura 15: LoginIntruder.

Desde el intruder, se define como variable el Hash, para poder configurarlo como un

payload, y así hacer un Pass The Hash con distintos hashes. Los distintos hashes se ingresan a la lista, para luego ejecutar el ataque.



**Payload configuration**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	e2d57b24a32912a5b0a217d0a80ff36b
Load...	c893bad68927b457dbed39460e6afd62
Remove	078c007bd92ddec308ae2f5115c1775d
Clear	5f4dec3b5aa765d61d8227deb882ef90
Deduplicate	482c811da5d5b4bc6d497ffa98491e38 <b>Hash Correcto</b>
	6f0f4d469eaead0ac18da3a460f263b6
	21232f297a57a5a743894a0e4a801fc3

**Add** Enter a new item

**Add from list...** [Pro version only]

Figura 16: Payload ataque PTH.

Para poder ver cuales resultados son los correctos y cuales incorrectos se utiliza la configuración de *Grep - Extract*.

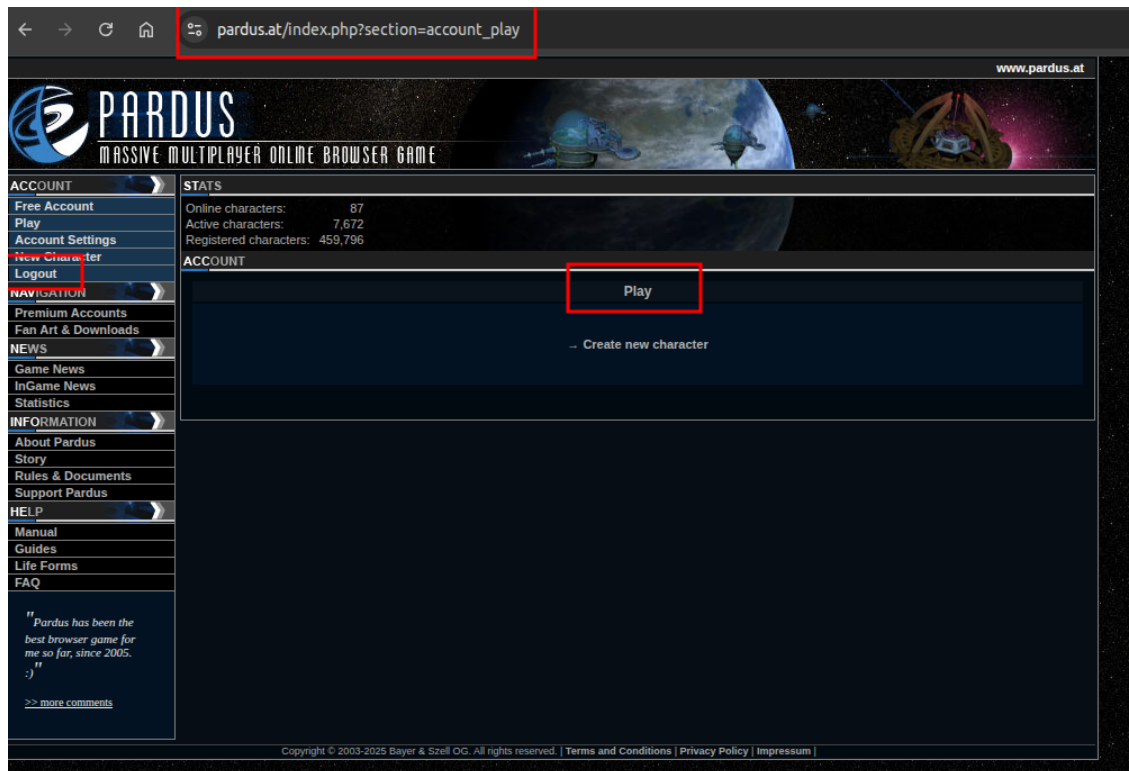


Figura 17: Login Correcto.

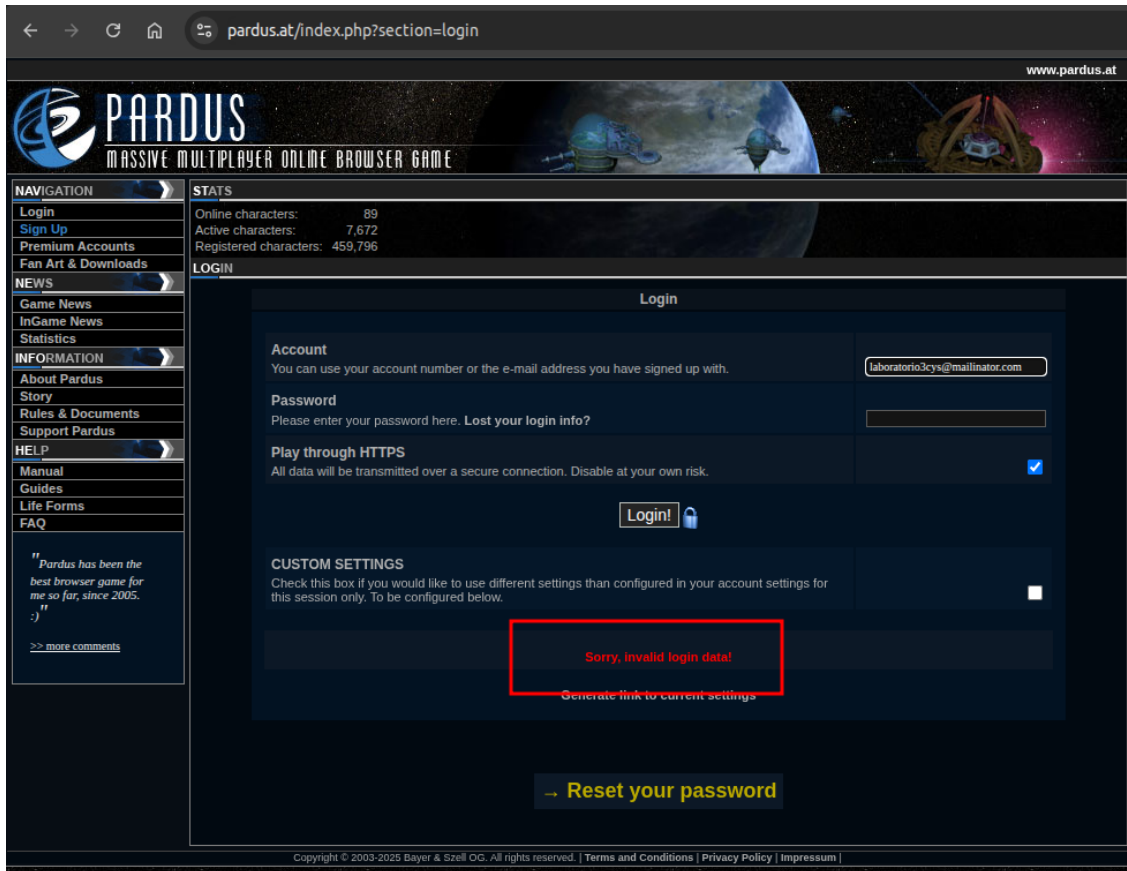


Figura 18: Login Incorrecto.

Finalmente se ejecuta el ataque, y se observan los resultados, siendo 1 resultado correcto y todos los otros incorrectos.

2. Intruder attack of https://www.pardus.at

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Requ...	Payload	Statu...	Re...	...	Length	"red"><b>	-8859-1\r\n	Comr
0		200	274	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	
1	e2d57b24a32912a5b0a217d...	200	313	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	
2	c893bad68927b457dbed394...	200	307	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	
3	078c007bd92dddec308ae2f5...	200	279	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	
4	5f4dccc3b5aa765d61d8327d...	200	287	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	
5	482c811da5d5b4bc6d497ff...	302	320	...	3469	Location: https://www.pardus.at/index.php?section=account_play		
6	6f0f4d469eaeadd0ac18da3a...	200	283	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	
7	21232f297a57a5a743894a0...	200	279	...	17381	Sorry, invalid login data!	Pragma: no-cacheCache-Control: no-store, no-cache, must-revalidate...	

Figura 19: Resultado PTH.

El resultado correcto corresponde al hash `482c811da5d5b4bc6d497ffa98491e38`, de la con-



traseña ingresada en el registro *password123*.

## 2.6. Identifica las políticas de privacidad o seguridad

Las políticas de privacidad y términos del servicio están en los siguientes links:

- <https://www.pardus.at/index.php?section=termsandconditions>
- <https://www.pardus.at/index.php?section=privacypolicy>

Dentro de los términos y condiciones del servicio se habla sobre contraseñas sólo en la sección de *Security*.

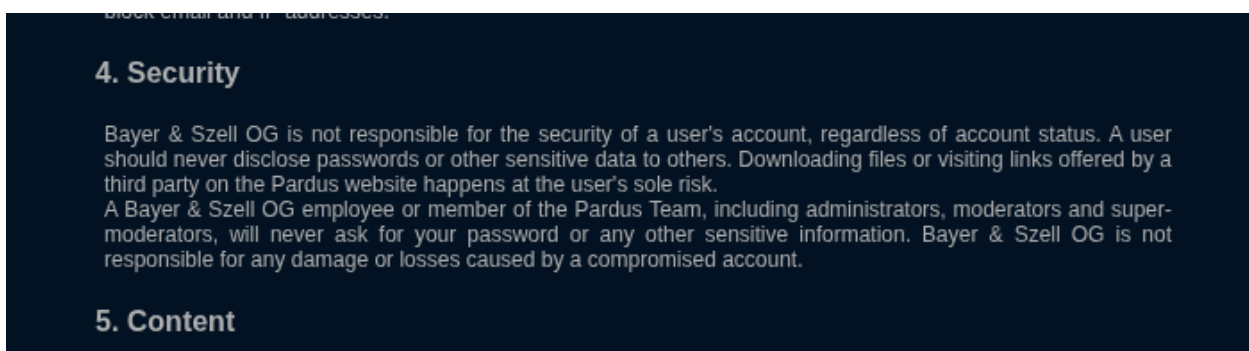


Figura 20: Sección de Seguridad en Términos y Condiciones.

En esta sección se mencionan las contraseñas, pero no se menciona ni habla de ningún tipo de seguridad o protocolo con el que se tratan las contraseñas. Se aborda la responsabilidad del usuario al manejar su información personal (contraseña, usuario, mail, etc.), y de la exención de responsabilidades de parte de la página en caso de cuentas comprometidas.

Luego en las políticas de privacidad se habla en 2 secciones sobre contraseñas.

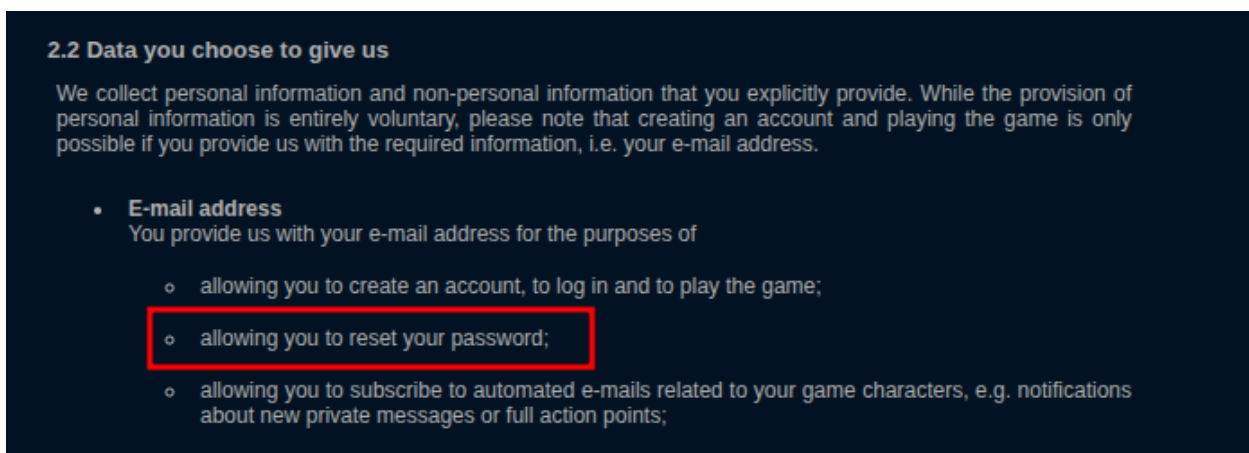


Figura 21: Uso de correo electrónico.

Aquí se refiere a que el sistema puede utilizar la dirección de correo electrónico para recuperar la contraseña en caso de solicitarlo.

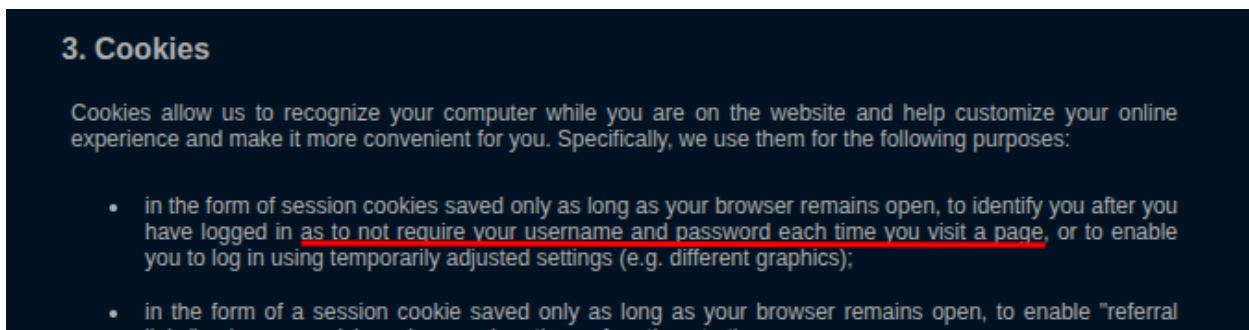


Figura 22: Uso de Cookies.

El uso de cookies para mantener la sesión iniciada, para que no sea necesario estar introduciendo la contraseña en reiteradas ocasiones.

### 2.7. Comente 4 conclusiones sobre la seguridad del sitio escogido

- Como se puede observar por lo hecho durante el laboratorio, este sitio web no cifra ni protege las credenciales al momento de hacer un registro del usuario, estas viajan en texto plano, lo que significa que es muy susceptible a que se filtre esta información y es algo que no debería pasar.
- En el caso del login, solo se cifra la contraseña mediante un hash MD5 y el correo se envía en texto plano. Si bien esto es un paso más seguro por sobre el registro, sigue quedando la información expuesta. Por ejemplo, buscando un sitio web que haga MD5 en reversa, e ingresando el hash se puede obtener la contraseña sin mayor esfuerzo.

<https://md5.gromweb.com/>

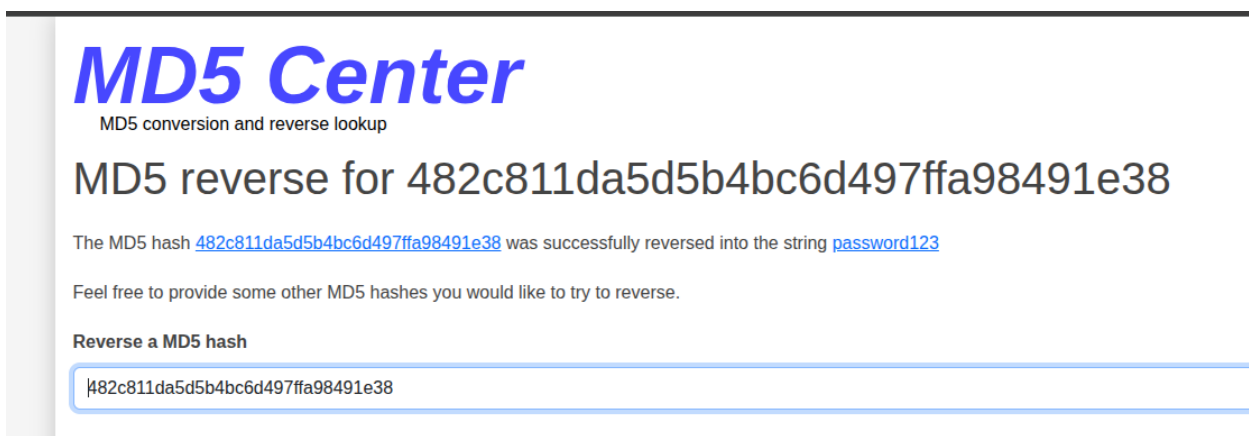


Figura 23: Búsqueda reversa de MD5.

- En el paso del ataque haciendo el Pass the Hash, el sitio web limita el número de intentos de login fallidos que se pueden hacer, y en caso de que sean muchos bloquea la IP para los intentos siguientes por un tiempo de 10 minutos. Esta medida de un timeout es bastante efectiva para evitar ataques de fuerza bruta.

3. Intruder attack of https://www.pardus.at

Attack Save

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Requ...	Payload	Status code	Respons...	Error	Timeout	Length	"red"><b>	-8859-1i/r/n	Comme
0		200	306			17381	Sorry, invalid login data!		
1	e2d57b24a32912a5b0a217d...	200	300			17381	Sorry, invalid login data!		Pragma: no-cacheCac...
2	c893bad68927b457dbed394...	200	275			17381	Sorry, invalid login data!		Pragma: no-cacheCac...
3	078c007bd92ddc308ae2f5...	200	302			17381	Sorry, invalid login data!		Pragma: no-cacheCac...
4	5f4dcc3b5aa765d61d8327d...	200	224			17446	Sorry, too many invalid login attempts! Your IP has been temporarily banned for 10 minutes.		Pragma: no-cacheCac...
5	482c811da5d5b4bc6d497ff...	200	293			17446	Sorry, too many invalid login attempts! Your IP has been temporarily banned for 10 minutes.		Pragma: no-cacheCac...
6	6f0f4d469eaead0ac18da3a...	200	248			17446	Sorry, too many invalid login attempts! Your IP has been temporarily banned for 10 minutes.		Pragma: no-cacheCac...
7	21232f297a57a5a743894a0...	200	260			17446	Sorry, too many invalid login attempts! Your IP has been temporarily banned for 10 minutes.		Pragma: no-cacheCac...

Figura 24: Timeout.

- Las posibles mejoras en términos de seguridad que podría aplicar el sitio web sería:
  1. Cifrar las credenciales al momento de la creación o registro de un nuevo usuario.
  2. Con una función agregar un *salt* de manera que sea más difícil obtener un hash haciendo una búsqueda en reversa.
  3. De la misma manera, agregar un *pepper* a las credenciales de manera que sean aún más seguras.
  4. Definir requerimientos de bases mas complejas para las contraseñas, de manera que dificulte la obtención de estas.