

# Informe Laboratorio 3

## Sección 2

Tomás Díaz Calderón  
e-mail: tomas.diaz\_c@mail.udp.cl

Mayo de 2025

## Índice

<b>1. Descripción de actividades</b>	<b>2</b>
<b>2. Desarrollo de actividades según criterio de rúbrica</b>	<b>2</b>
2.1. Identifica el algoritmo de hash utilizado al momento de registrarse en el sitio	2
2.2. Identifica el algoritmo de hash utilizado al momento de iniciar sesión . . . . .	5
2.3. Genera el hash de la contraseña desde la consola del navegador . . . . .	6
2.4. Intercepta el tráfico login con BurpSuite . . . . .	8
2.5. Realiza el intento de login . . . . .	9
2.6. Identifica las políticas de privacidad o seguridad . . . . .	11
2.7. Comente 4 conclusiones sobre la seguridad del sitio escogido . . . . .	12

## 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 una contraseña incorrecta por el hash obtenido en el punto anterior.
- 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

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

Se comienza la actividad del laboratorio ingresando a la página <https://www.mmo-champion.com/content/>.



Figura 1: MMO-CHAMPION

Se selecciona la opción de registrarse y se llena el formulario, donde se ingresa un nombre de usuario "Shiren125", contraseña "contrasena123" y correo "tomas.dc125@gmail.com":

Register at MMO-Champion

Required Information

User Name:

Shiren125

✓

Username is valid and not in use.

Please enter the name by which you would like to log-in and be known on this site.

Password:

\*\*\*\*\*

Confirm Password:

\*\*\*\*\*

Please enter a password for your user account. Note that passwords are case-sensitive.

Email Address:

tomas.dc125@gmail.com

Confirm Email Address:

tomas.dc125@gmail.com

Please enter a valid email address for yourself.

Human Verification

✓ No soy un robot

reCAPTCHA

Privacidad - Términos

Figura 2: Relleno de formulario para registro en mmo-champion

Una vez hecho el registro, se selecciona la inspección de página de google chrome y se selecciona "Network", obteniendo lo siguiente:

## 2 DESARROLLO DE ACTIVIDADES SEGÚN CRITERIO DE RÚBRICA

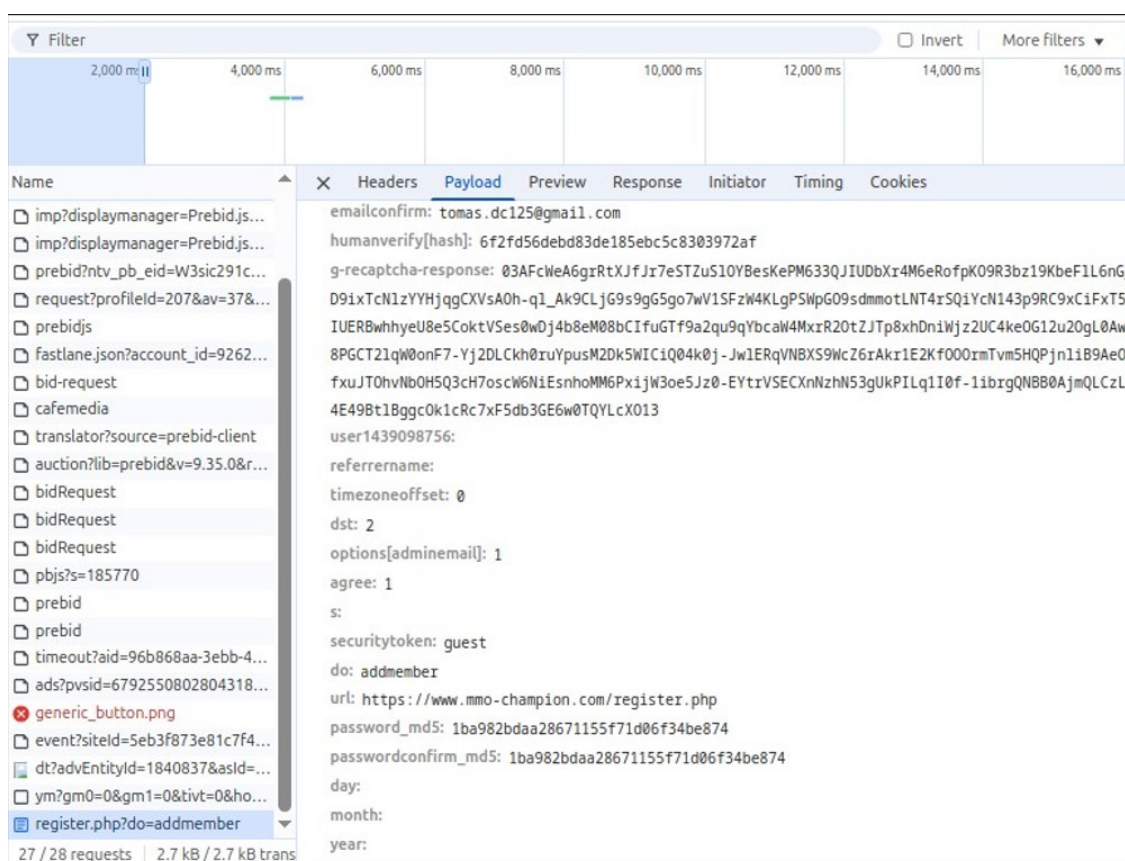


Figura 3: Inspección de página al registrarse

Se puede observar en la figura anterior que se tiene la petición de registro.php, la que al seleccionarla muestra una contraseña hashada con MD5 en la variable "password\_md5: 1ba982bdaa28671155f71d06f34be874". Para verificar que efectivamente se utilizó MD5 para hashear la contraseña, se ingresa a la página <https://www.md5hashgenerator.com/> y se ingresa la contraseña, obteniendo lo siguiente:

## MD5 Hash Generator

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

contrasena123

Generate →

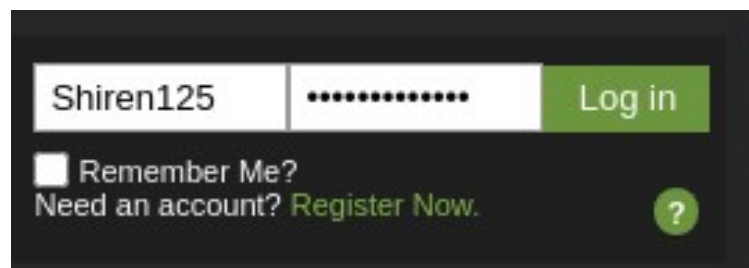
Your String	contrasena123	
MD5 Hash	1ba982bdaa28671155f71d06f34be874	<button>Copy</button>
SHA1 Hash	094e8e159db7824161b1e67ab209da503434c626	<button>Copy</button>

Figura 4: Transformación de contraseña usando MD5

Se puede observar que el hash generado con MD5 corresponde al de la variable de la Figura 3, por lo que se comprueba que se utilizó MD5 para hashear en su formulario de registro.

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

Se ingresan las credenciales "Shiren125" y "contrasena123":



Shiren125 | ..... | Log in

☐ Remember Me?

Need an account? [Register Now.](#) ?

Figura 5: Ingreso de credenciales correctas

Luego, se vuelve a inspeccionar la página:

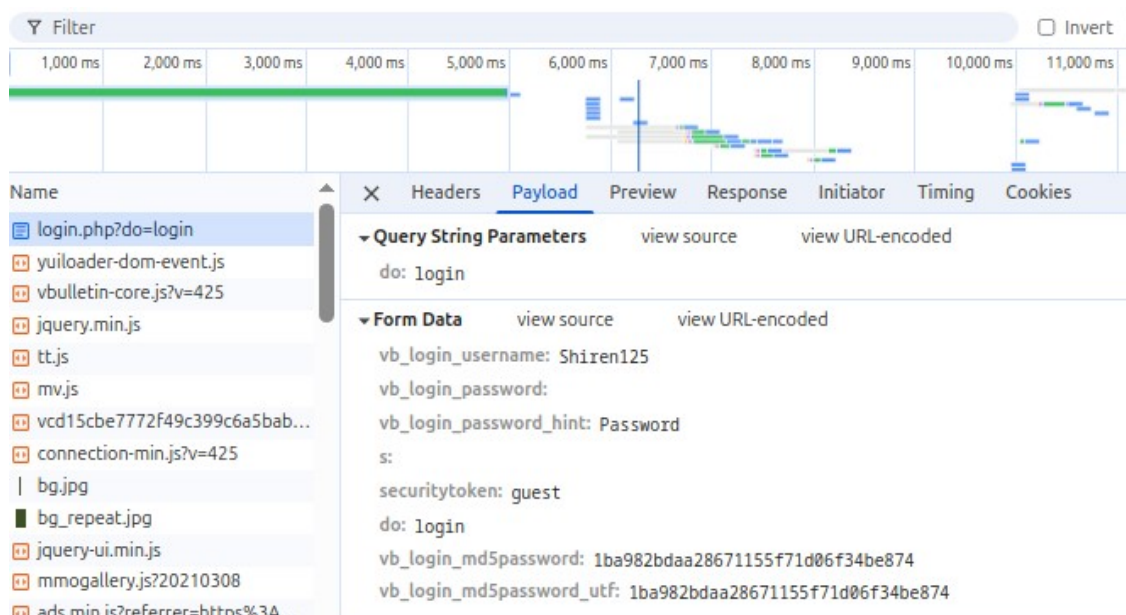


Figura 6: Inspección de página al realizar un login con credenciales correctas

Se puede observar que se tiene la petición login.php, la que al ser seleccionada muestra la información del usuario y la variable "vb\_login\_md5password: 1ba982bdaa28671155f71d06f34be874", la cual como se puede observar en la Figura 4 corresponde a "contrasena123", que es la contraseña correcta del usuario, lo que confirma la utilización de MD5 para el inicio de sesión.

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

En mmo-champion, sin iniciar sesión, se inspecciona la página y se va a "Sources", buscando así donde se encuentran las funciones respectivas del md5.



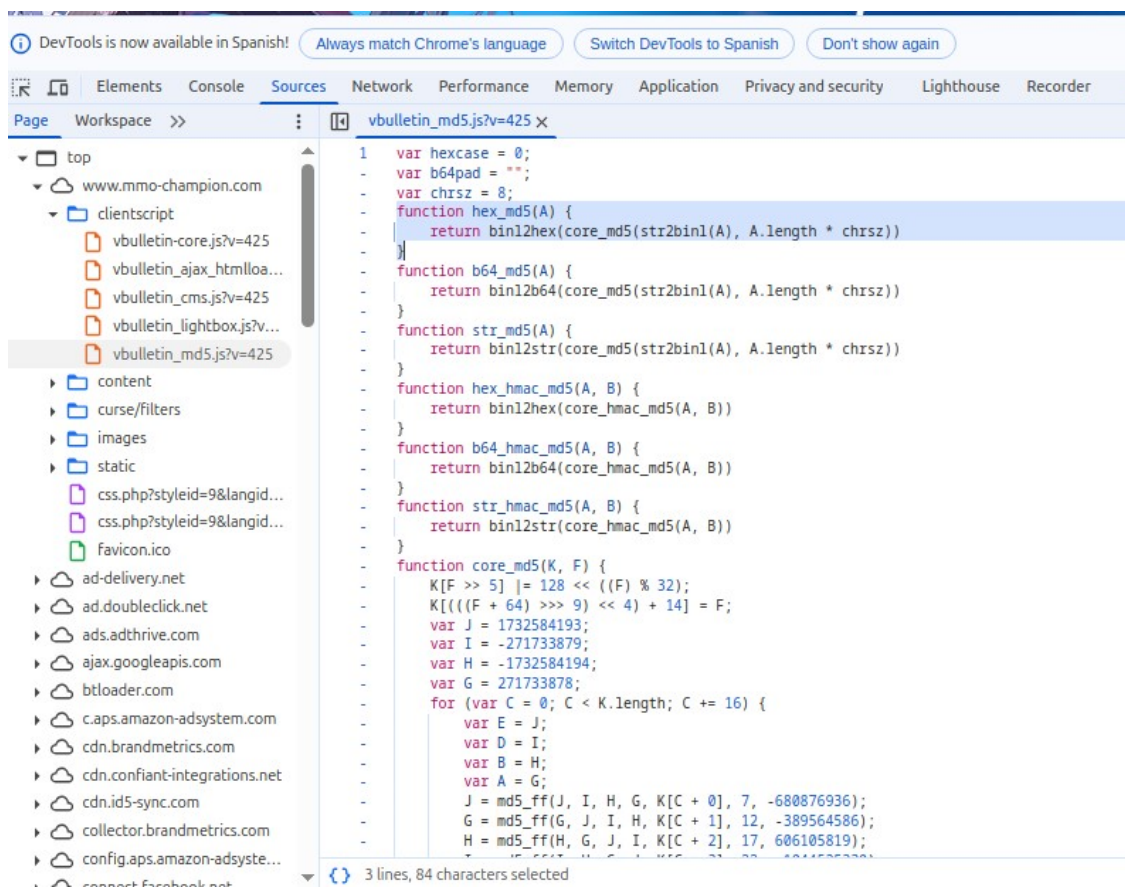


Figura 7: Funciones de MD5 al inspeccionar la página

Se puede observar que la función que transforma una cadena de caracteres utilizando MD5 es "hex\_md5(A)", por lo que en la consola se ingresa la función con la contraseña "contrasena123":

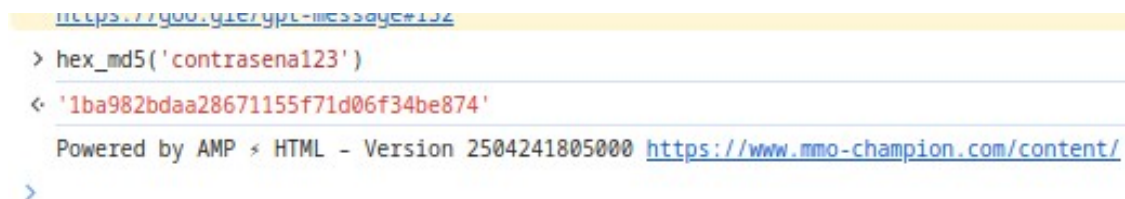


Figura 8: Uso de la función hex\_md5() en la consola

Se puede observar que la respuesta obtenida corresponde a la misma que en los casos anteriores.

## 2.4. Intercepta el tráfico login con BurpSuite

Se abre la aplicación Burpsuite instalada en el laboratorio anterior, se activa la intercepción y se realiza el login desde la página mmo-champion, obteniendo lo siguiente:

Burp

Project

Intruder

Repeater

View

Help

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Intercept

HTTP history

WebSockets history

Match and replace

Proxy settings

Intercept on

Forward

Drop

Request to https://www.mmo-champion.com:443 [104.26.9.132]

Time	Type	Direction	Method	URL
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=0000417-17ee1fad-6400-5330a-319015a1v=97bc.dm781p, pingTime: -4, time: 000950, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=4589a286-4a0d-1842-54a8-3856f5238deeTv=67Bc.dm782p, pingTime: -4, time: 361800, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2471736&askId=34c6da8-e402-dfb3-11af-55cd1e26d11c&tv=67Bc.dm781p, pingTime: -1, time: 808050, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2471736&askId=34c6da8-e402-dfb3-11af-55cd1e26d11c&tv=67Bc.dm781p, pingTime: -4, time: 808478, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=ac905ea0-cf22-a516-844e-d826f2cf9c48v=67Bc.dm783p, pingTime: -4, time: 242389, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=66866417-17ee-fad-6400-5330a-51790f5a&tv=67Bc.dm781W, pingTime: -1, time: 689900, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=cf3edac-33c6-33da-2762-9459dc4bb7fd&tv=67Bc.dm783p, pingTime: -4, time: 619182, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=854585&askId=cbcd5c9-5e78-8dd1-e726-b61ccb972596&tv=67Bc.dm783p, pingTime: -1, time: 259064, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=cf3edac-33c6-33da-2762-9459dc4bb7fd&tv=67Bc.dm782p, pingTime: -1, time: 619185, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=4589a286-4a0d-1842-54a8-3856f5238deeTv=67Bc.dm782H, pingTime: -1, time: 361816, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=854585&askId=cbcd5c9-5e78-8dd1-e726-b61ccb972596&tv=67Bc.dm783p, pingTime: -4, time: 259061, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=ac905ea0-cf22-a516-844e-d826f2cf9c48v=67Bc.dm783p, pingTime: -1, time: 242393, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=98fc9f3f-e582-fad4-1104-d3c5946322a&tv=67Bc.dm783p, pingTime: -4, time: 188683, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=98fc9f3f-e582-fad4-1104-d3c5946322a&tv=67Bc.dm783p, pingTime: -1, time: 188685, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=4ad1009d-4317-1359-6c17-9bb55b92a695&tv=67Bc.dm783p, pingTime: -4, time: 143237, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	GET	https://dt.adsafeprotected.com/d?advEntityId=2495028&askId=4ad1009d-4317-1359-6c17-9bb55b92a695&tv=67Bc.dm783p, pingTime: -1, time: 143240, type.u, clog: %5B%7Bpiv...
14:01:45.22	HTTP	→ Request	POST	https://www.mmo-champion.com/login.php?do=login
14:01:49.22	HTTP	→ Request	GET	https://analytics.google.com/g/collect?v=2&id=G-CGRBNJWMVH&utm=45je551h2v871017967za200b812220430&_p=1747936054636&gcd=1313313111&npa=0&dma=0&tag...
14:02:09.22	HTTP	→ Request	GET	https://aax.amazon-us-east-system.com/elt/bid?src=600&ch=https%3A%2F%2Fwww.mmo-champion.com%2FContent%2F&pid=HyErVSGazV1W0&cb=56&ws=1374&781v=24...
14:02:09.22	HTTP	→ Request	POST	https://pbs.raptive-eu.as.delivery/openb2/auction
14:02:10.22	HTTP	→ Request	POST	https://prebid.production.adthrive.com/openb2/auction
14:02:10.22	HTTP	→ Request	POST	https://exchange.postrelease.com/prebid?v=ntb_pb_eid=W3sic291cmNlloYzJpdGpVnVhNvbSlsrVpZHM0It7lmkloJnpUnYU5W0XdtMGH0tmxkaFzUsNZVtGtYOZM1RTVXIRa...
14:02:10.22	HTTP	→ Request	POST	https://gids-bidder.criteo.com/openb2_5_bps/auction/request?profileId=207&av=37&vv=9.35_0&cb=43231889410&isaval=1&bundle=8Vm_gv9klU4VElOXZ5Q7BPJUsaDNK...
14:02:10.22	HTTP	→ Request	GET	https://fastlane.rubiconproject.com/api/fastlane.json?account_id=9262&site_id=180726&zone_id=881416&size_id=2&alt_size_ids=1%2C243962C44%2C5592C2117%2C2218...

Figura 9: Intercepción de tráfico de login en burpsuite

Luego, se selecciona el paquete que contiene la información del login, el cual se puede observar en la figura anterior destacado:

**Request**

Pretty	Raw	Hex
1 POST /login.php?id=login HTTP/2		
2 Host: www.mmo-champion.com		
3 Cookie: gclid=GAL.2.296949007.1747862875; usprivacy=LYNY; lc2_fpi=c928e18e2dd--0j1ybtwxv8bsvsqz5szta8bwk4o; lc2_fpi_meta=w7B%22A%22%3A1747862877160%7D; lr_env_src_ats=false;		
4 panoramaId=expiry=1748467677882d; cc_uid=cc3984d92296f6bf59396539e314f73d; panoramaId=5b7596764f3382a2c5821d79dc25185ca92cb5633b1079322cc6b221e77dfdeb; scor_uid=8f5e88052da4123a4a5ef2b1773eccd; mmoc_lastvisit=1747867793; mmoc_lastactivity=0; li_dcde_cw=mmo-champion.com; lr_retry_request=true; ga=GA(2.1493106841.1747862875; AMZN-Token=v2FveLwXzkxBHJRSbjdhkeZpeTNzWvpIYKxOVMxOZHMLC29mSLQzak9wb1psbUNYLzVtZHXZUlo2MlVqYoDUYdmNMDOUZLUdkhRamZKvZYs25UafdtNjVDWKJMaTU4ULZYUMJpb3ldAfdtMWLTZvc5ZF2CFTRCUyoJtkE5WaEdvdUphLVH3CEpOTXZCUFUzlONJMVG6T2xld3dRTETvY2ozRTFYRhxZc0g2dzFFZDJNyUYNFJIIdLZNODJQWUDBPWRjdrgFiaX24DKc3KzkyS5nzcrOU8RKy9Z25svdaUrL3ZjeUX;; _ga_NCHWS789G=		
5 GS2.F.s1747936065q0sg0st1747936065js0j0sh0; connectid=7B%22muidd%22%3A%221dbEDT40twI7FUQu9vG92469oG6awvrztCjnIWrhVKD85zsD7n-C40e4c2fGHtzlTMWckXkofXUCiuEvEU_e0%22%2C22connectid%22%3A%221dbEDT40twI7FUQu9vG92469oG6awvrztCjnIWrhVKD85zsD7n-C40e4c2fGHtzlTMWckXkofXUCiuEvEU_e0%22%2C22connectid%22%3A%221dbEDT40twI7FUQu9vG92469oG6awvrztCjnIWrhVKD85zsD7n-C40e4c2fGHtzlTMWckXkofXUCiuEvEU_e0%22%2C22%3A86400000%2C22he%22%3A22030541ab26eca9da6e1755b2a259e22a1d578d92df438eb4e60201d01a296af%22%2C22ppuid%22%3A%228be1726-f0c2-4025-bb05-ccc29620d99c%22%2C22allastSynced%22%3A1747865867994%2C22allUsed%22%3A174793606908073; gads=ID=b44d990c54bf8ds; T=1747862884; RT=1747936725; S=ALNI_MybK04_R84m9zCDZJNDGT9I2C6Thgxg; _gqi=EO=00001d005346fbcc; T=1747862884; RT=1747936725; S=ALNI_MybK04_CXXOLCS=0207004K; _eoi=ID=6452990db4b828bc; T=1747862884; RT=1747936725; S=A-A-FjbpdpITFHxlFLQiw6q4dm; _ga_GCBRNJMMVH=GS2.L.s1747936061q0sg1st1747936904js1js0j0sh0sdengQTBNBerkt7b1L2GBoWhXNZTVLOrha		
6 Content-Length: 222		
7 Cache-Control: max-age=0		
8 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"		
9 Sec-Ch-Ua-Mobile: ?0		
10 Sec-Ch-Ua-Platform: "Linux"		
11 Accept-Language: es-ES;q=0.9		
12 Origin: https://www.mmo-champion.com		
13 Content-Type: application/x-www-form-urlencoded		
14 Upgrade-Insecure-Requests: 1		
15 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36		
16 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		
17 Sec-Patch-Site: same-origin		
18 Sec-Patch-Mode: navigate		
19 Sec-Patch-User: ?1		
20 Sec-Patch-Dest: document		
21 Referer: https://www.mmo-champion.com/content/		
22 Accept-Encoding: gzip, deflate, br		
23 Priority: u=0, i		
vb_login_mdpassword=Shiren125vb_login_password=6vb_login_password_hint>Password&s=&securitytoken=get&do=login&vb_login_mdpassword=1ba982bdaa28671155f71d06f34be874		

Figura 10: Información de login

En la línea 23 se pueden observar las credenciales con las que se inició sesión, donde se tiene



## 2 DESARROLLO DE ACTIVIDADES SEGÚN CRITERIO DE RÚBRICA

al usuario "Shiren125" y la contraseña hashheada con MD5 "1ba982bdaa28671155f71d06f34be874" la cual corresponde a la misma de los casos anteriores (ver Figura 4)

### 2.5. Realiza el intento de login

Se realiza un intento de login con las siguientes credenciales: "Shiren125" y "contrase-naincorrecta". Como se puede observar, la contraseña no es con la que se registró al usuario. Se captura este proceso con Burpsuite:

The screenshot shows the Burp Suite interface. At the top, there are buttons for 'Intercept on', 'Forward', and 'Drop'. Below this is a table of intercepted requests. The table has columns for Time, Type, Direction, Method, URL, and Status code. The requests are from 14:19:13 to 14:19:22. The last request is a POST to 'https://www.mmo-champion.com/login.php?do=login' with a status code of 200. Below the table, the 'Request' tab is selected, showing the raw HTTP request. The request is a POST to 'https://www.mmo-champion.com/login.php?do=login' with a body containing login credentials. The body is: 'vb\_login\_username=Shiren125&vb\_login\_password=7ab86fe270770f6baef6a22e1d4b0ffe&vb\_login\_md5password=7ab86fe270770f6baef6a22e1d4b0ffe&vb\_login\_md5password\_utf=7ab86fe270770f6baef6a22e1d4b0ffe'.

Time	Type	Direction	Method	URL	Status code
14:19:13	HTTP	Request	POST	https://csi.gstatic.com/csi/v=2&s=ima&mc=4&puid=3-mazp4kx&c=7155586511215&slotid=3577793255607&fb=ima_html5-ima&sdv=h.3.695.1&mrd=8&aab=1&av=1&met.4...	
14:19:14	HTTP	Request	GET	https://logger.adthrive.com/event?siteid=5eb3f873e81c7f4e9287b57&siteName=MMO%20Champion&bucket=flex-23&branch=25b3ee4&deployment=2025-05-22-05%3Ape-7...	
14:19:14	HTTP	Request	GET	https://nrb.ybp.yahoo.com/vasterror/imp/qbfJdZzqCUL6D8KygDhUHS-2ucWp81yhcg3K05cfr3C5BFuFskPSPkOmtLUJgaMsrckxDYPPwif8K7U8_r725WpLyp6iLzdcnwRo...	
14:19:14	HTTP	Request	GET	https://edgecast-vod.yimg.com/brdsp/919d6f27-cab1-4bf8-b987-75a550dc645b/539ae518-d1d5-4060-8807-108756ab12a0%7C426x240x350x30%7C.mp4	
14:19:15	HTTP	Request	POST	https://csi.gstatic.com/csi/v=2&s=ima&mc=4&puid=3-mazp4kx&c=7155586511215&slotid=3577793255607&fb=ima_html5-ima&sdv=h.3.695.1&mrd=8&aab=1&av=1&ua_e=1...	
14:19:16	HTTP	Request	GET	https://logger.adthrive.com/event?siteid=5eb3f873e81c7f4e9287b57&siteName=MMO%20Champion&bucket=flex-23&branch=25b3ee4&deployment=2025-05-22-05%3Ape-7...	
14:19:16	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askid=390f7b65-9765-1cf0-8e1f-2bd71875ce21&tv=%7Bc:dmbxn9.pingTime:-4,time:146,type:m,im:%7Bsf:0%7D,env:%...	
14:19:16	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askid=390f7b65-9765-1cf0-8e1f-2bd71875ce21&tv=%7Bc:dmbxn9.pingTime:-2,time:155,type:a,im:%7Bpom:1,prf:%7Bbe...	
14:19:16	HTTP	Request	POST	https://nrb.ybp.yahoo.com/ym?gm0=0&gm1=0&ivt=0&hov=1&th=16&int=2&int=0&st=24421&foc=1&adt=24408&scr=2&ph=1&scd=0&svd=0&svu=0&scst=0&mivp=98.4...	
14:19:16	HTTP	Request	POST	https://nrb.ybp.yahoo.com/ym?gm0=0&gm1=0&ivt=0&hov=1&th=16&int=2&int=0&st=24421&foc=1&adt=24360&scr=2&ph=1&scd=0&svd=0&svu=0&scst=0&mivp=92.59...	
14:19:16	HTTP	Request	POST	https://www.mmo-champion.com/login.php?do=login	
14:19:16	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askid=390f7b65-9765-1cf0-8e1f-2bd71875ce21&tv=%7Bc:dmbxy,time:543,type:e,sca:%7Bbnq:b,ts:%7Bbs:2025-05-...	

**Request**

Pretty Raw Hex

```
ea450302-z10c-470e-at71-a901104a0a20; connectid=
%7B%22vuid%22%3A%22u1dBeDT40tw17fUQu9vG92469oG6awvrtCjnIWrhVKD85zSD7n-C40e4c2fGHTzLTmWckXofXUciuvEYU_e0%22%2C%22connectId%22%3A%22u1dBeDT40tw17fUQu9vG92469oG6awvrtCjnIWrhVKD85zSD7n-C40e4c2fGHTzLTmWckXofXUciuvEYU_e0%22%2C%22t1%22%3A86400000%2C%22%20305a41b26eca9da6c1755b2a259e22a1d578d92df438eb4e60201d01a296af%22%2C%22puid%22%3A%228bee1726-f0c2-4025-bb05-ccc29620d99c%22%2C%22astSynced%22%3A1747865867994%2C%22astUsed%793792562%2D%7D%7B%22ga_GCBRNJWMVH%22%3A%221s17479396061%2D%7D%7B%22s1747939489%7D%7B%22h0Ddenq0TBN8etk7b1l2G8oBwhXN2VLOyha
4 Content-Length: 268
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept-Language: es-ES,es;q=0.9
10 Origin: https://www.mmo-champion.com
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/135.0.0.0 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.mmo-champion.com/login.php?do=logout&logouthash=1747937905-7006933c8b535662f980a235090b43eeac8a511
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 vb_login_username=Shiren125&vb_login_password=7ab86fe270770f6baef6a22e1d4b0ffe&vb_login_md5password=7ab86fe270770f6baef6a22e1d4b0ffe&vb_login_md5password_utf=7ab86fe270770f6baef6a22e1d4b0ffe
```

Figura 11: Intento de inicio de sesión con credenciales incorrectas

Al seleccionar nuevamente el paquete con la información del login, como se puede observar en la línea 23, la contraseña hashheada corresponde a "7ab86fe270770f6baef6a22e1d4b0ffe". Se verifica que corresponda a la ingresada:

## MD5 Hash Generator

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

contrasenaincorrecta

Generate →

<b>Your String</b>	contrasenaincorrecta	
<b>MD5 Hash</b>	7ab86fe270770f6baef6a22e1d4b0ffe	Copy
<b>SHA1 Hash</b>	85e6b6db7fc58deff88888584fc4717602b89267	Copy

Figura 12: Comprobación de hash de contraseña incorrecta

La contraseña "7ab86fe270770f6baef6a22e1d4b0ffe" si corresponde a "contrasenaincorrecta".

Luego, se modifica el paquete de forma manual, ingresando "1ba982bdaa28671155f71d06f34be874" en los campos "vb\_login\_md5password" y "vb\_login\_md5password\_utf", que corresponden a la contraseña hasheada, y se selecciona Forward All.

## 2 DESARROLLO DE ACTIVIDADES SEGÚN CRITERIO DE RÚBRICA

The image shows a network traffic analysis tool interface. At the top, there are buttons for 'Intercept on', 'Forward', and 'Drop'. Below this is a table of network requests. The table has columns for Time, Type, Direction, Method, URL, and Status code. The requests are listed in chronological order, showing various HTTP methods like GET, POST, and GET. The last request in the list is a POST to 'https://www.mmo-champion.com/login.php?do=login' with a status code of 200. Below the table, there is a detailed view of the selected request, showing the raw data in hex and the pretty-printed version. The pretty-printed version shows the request headers and body, including the login credentials.

Time	Type	Direction	Method	URL	Status code
14:19:13.22	HTTP	Request	GET	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	200
14:19:13.22	HTTP	Request	POST	https://csi.gstatic.com/csi?v=2&s=ima&mc=4&puid=2-mazp400&c=7155586511215&slotid=3577793255607&fb=ima_html5-ima&sdv=h.3.695.1&mrdr=8&aab=1&iv=1&met.4...	200
14:19:14.22	HTTP	Request	GET	https://logger.adthrive.com/event?siteid=5eb3f873e81c7f4e9287fb57&siteName=MMO%20Champion&bucket=flex-23&branch=25b3ee4&deployment=2025-05-22-05%3Ape-7...	200
14:19:14.22	HTTP	Request	GET	https://nrb.ybp.yahoo.com/vasterror/imp/qbfDZzqCUL6D8tKyqDHUHS-2ucWp81yhcg3K05cfr3C5BfufSKPSPKoMTLJjgaMsrlckDYPPwif8K7U8_r725WpLvp6l1zdcnwRo...	200
14:19:14.22	HTTP	Request	GET	https://edgecast-vod.yimg.com/brdpsp919d6f27-cab1-4bf8-b967-75a550dc645b539ae518-d1d5-4060-8807-108756ab12a09c7C426x240x350x30%7C.mp4	200
14:19:15.22	HTTP	Request	POST	https://csi.gstatic.com/csi?v=2&s=ima&mc=4&puid=3-mazp4ky&c=7155586511215&slotid=3577793255607&fb=ima_html5-ima&sdv=h.3.695.1&mrdr=8&aab=1&iv=1&ua_e=1...	200
14:19:16.22	HTTP	Request	GET	https://logger.adthrive.com/event?siteid=5eb3f873e81c7f4e9287fb57&siteName=MMO%20Champion&bucket=flex-23&branch=25b3ee4&deployment=2025-05-22-05%3Ape-7...	200
14:19:16.22	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askd=3907b65-9765-1cf0-8e1f-2bd71875ce21&iv=%7Bc:dmbxnp.pingTime:-4,time:146,type:m,im:%7Bsf:0%7D,env:%...	200
14:19:16.22	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askd=3907b65-9765-1cf0-8e1f-2bd71875ce21&iv=%7Bc:dmbxnp.pingTime:-1,time:148,type:u,clog:%5B%7Bpv:0,vso:...	200
14:19:16.22	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askd=3907b65-9765-1cf0-8e1f-2bd71875ce21&iv=%7Bc:dmbxnp.pingTime:-2,time:155,type:a,im:%7Bpom:1,pr:%7Bbe:...	200
14:19:16.22	HTTP	Request	POST	https://nrb.ybp.yahoo.com/ym?gm0=0&gm1=0&iv=0&hov=1&th=16&int=2&intl=0&it=0&st=24421&foc=1&adi=24408&scr=2&ph=-1&scd=0&svd=0&svu=0&sct=0&mivp=98.4...	200
14:19:16.22	HTTP	Request	POST	https://nrb.ybp.yahoo.com/ym?gm0=0&gm1=0&iv=0&hov=2&th=0&int=2&intl=0&it=0&st=24362&foc=1&adi=24360&scr=2&ph=-1&scd=0&svd=0&svu=0&sct=0&mivp=92.59...	200
14:19:16.22	HTTP	Request	POST	https://www.mmo-champion.com/login.php?do=login	200
14:19:16.22	HTTP	Request	GET	https://dt.adsafeprotected.com/dt?advEntityId=854585&askd=3907b65-9765-1cf0-8e1f-2bd71875ce21&iv=%7Bc:dmbxnp.pingTime:543,type:e,sca:%7Bmq:b,tss:%7Bts:2025-05-...	200

**Request**

Pretty Raw Hex

Content-Length: 268  
Cache-Control: max-age=0  
Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"  
Sec-Ch-Ua-Mobile: ?0  
Sec-Ch-Ua-Platform: "Linux"  
Accept-Language: es-ES;eq=0.9  
Origin: https://www.mmo-champion.com  
Content-Type: application/x-www-form-urlencoded  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36  
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  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: navigate  
Sec-Fetch-User: ?1  
Referer: https://www.mmo-champion.com/login.php?do=logout&logouthash=1747937905-7006933cb8b535662f980a235090b43eeac8a511  
Accept-Encoding: gzip, deflate, br  
Priority: u=0, i

vb\_login\_username=Shiren125&vb\_login\_password=&vb\_login\_password\_hint=Password&s=&securitytoken=1747937919-049a6b36f560dd53ed36fe946d49324d3bb71607&do=login&vb\_login\_md5password=1ba982bdaa28671155f71d06f34be874&vb\_login\_md5password\_utf=1ba982bdaa28671155f71d06f34be874

Figura 13: Cambio de contraseña en el paquete

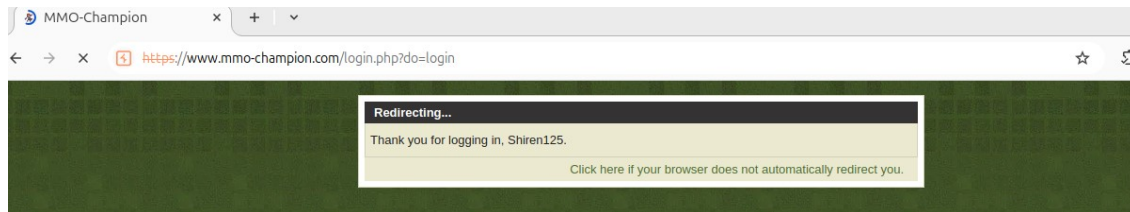


Figura 14: Inicio de sesión exitoso

Se puede observar que el inicio de sesión se realizó exitosamente.

### 2.6. Identifica las políticas de privacidad o seguridad

Las políticas de privacidad se encuentran en el final de la página de mmo-champion, como se puede observar a continuación:



Figura 15: Políticas de Privacidad en MMO-CHAMPION

Al seleccionar "Privacy Policy" se redirige a la siguiente dirección: <https://www.magicfind.us/privacy/>. Las políticas de privacidad y seguridad están descritas por Magic Find, donde se dice que la información recopilada tienen 2 categorías: La provista de manera voluntaria, que corresponde a la información que brinda el usuario, y la automática, que corresponde a la información enviada por los dispositivos al acceder a los servicios.

En cuanto a la seguridad de los datos, se dice que protegen los datos mediante medios comercialmente aceptables para prevenir su pérdida y robo, pero advierte que no garantiza el 100 % de su protección y que es responsabilidad del usuario la complejidad y robustez de la contraseña. No se dice de manera explícita cómo protegen los datos, es decir, no mencionan el uso de ningún tipo de hash por ejemplo.

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

- **Uso de MD5:** El hash MD5 es un método que actualmente se encuentra obsoleto, debido a su vulnerabilidad a ataques de fuerza bruta. Como se pudo observar a lo largo del laboratorio, es simple observar el parámetro de la contraseña en variables que explicitan el uso de MD5, lo cual se puede interceptar con Burpsuite y modificar el parámetro.
- **Falta de ofuscación en el mensaje:** Al inspeccionar la página luego de iniciar sesión, se puede observar con facilidad la variable donde se almacenan las contraseñas hasheadas. Al ingresar esta contraseña en un generador de hash MD5 online se obtiene exactamente el mismo valor. Añadir Salt o Pepper en el mensaje y hashear luego

aumenta la ofuscación de la contraseña, lo cual dificulta los ataques de fuerza bruta y evita que distintos usuarios con las mismas contraseñas tengan el mismo hash.

- **Vulnerabilidad a Pass the Hash:** Con el uso de Burpsuite, se pudo observar que el tráfico se puede interceptar fácilmente y hacer uso de los hashes para el ingreso sin necesidad de descifrar la contraseña.
- **Ausencia de verificación de 2 pasos:** A la hora de registrarse en la página, como medida extra de seguridad se tiene el uso de captcha. Luego de llenar el formulario, se envía un correo para completar la activación de la cuenta. Sin embargo, a la hora de iniciar sesión, no se tiene ningún tipo de paso extra para ingresar, solo se requiere usuario y contraseña. Añadir una verificación de 2 pasos, como ingresar un código enviado por SMS o correo, agregaría una capa extra de seguridad y evitaría ataques de fuerza bruta.