Informe Laboratorio 3

Sección 3

Sergio Soto Cuevas
e-mail: sergio.soto1@mail.udp.cl

Octubre de 2025

Índice

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 comenzar se selecciono la pagina Free-Hack[1].

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

Primero nos registramos en la web, se utilizo el usuario siu7, y la contraseña siucr7.

[1]Free-Hack. Disponible en `https://free-hack.com`.

Figura 1: Registro Network

Se observa en la figura 1, obtenida desde el análisis de Network, donde se encuentra la solicitud para registrar al usuario, se destaca que el campo password anuncia estar usando md5.

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

De misma forma se realiza un intento de inicio de sesión incorrecto, y se observa el Network en la figura 2.

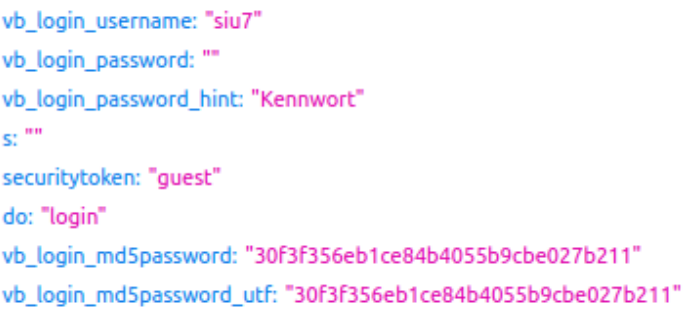

Figura 2: Login Incorrecto

Se observa que de nuevo se encuentra la contraseña en lo que parece ser md5, por ello se lleva a un analizador de hash.

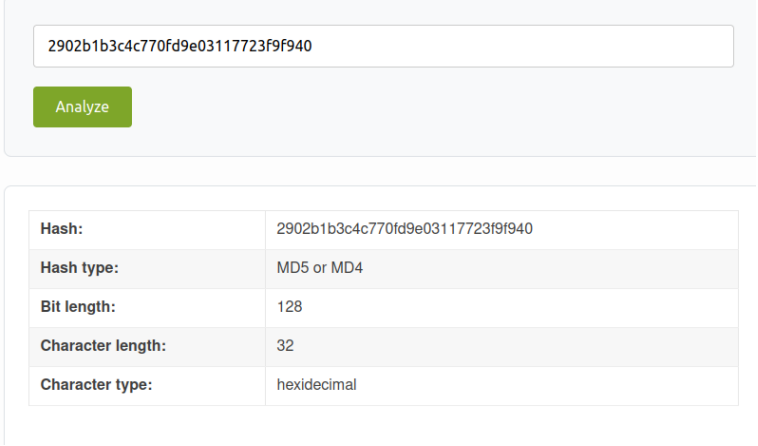

Figura 3: Hash Analyzer

Por ultimo en la figura 3 se determina que corresponde efectivamente a md5.

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

Ahora desde la consola del navegador, se utiliza hex_md5 y se genera el hash de la contraseña correcta en md5.

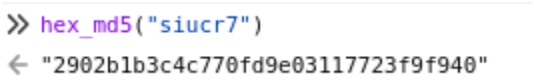

Figura 4: Hash consola

2.4. Intercepta el tráfico login con BurpSuite

A continuación desde burpsuite, se entra a la web desde la pestaña proxy y se intercepta un intento de sesión incorrecto.

Figura 5: Interceptar trafico

En la figura 5 se observa el formulario del login, donde se encuentra el usuario, y el hash de la contraseña incorrecta, se destaca que existe un token el cual no cambia con valor guest (previo al login correcto), y que se envía la contraseña en MD5, y en UTF-8.

2.5. Realiza el intento de login por medio del hash

Por ultimo, en la figura 6 se modifica los campos correspondientes con la contraseña incorrecta cambiándolos por el hash devuelto por la consola para intentar un inicio de sesión, y se realiza forward hasta realizar concretar el login.

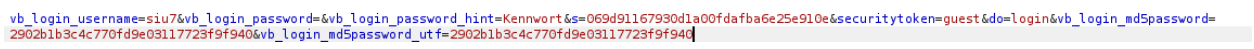

Figura 6: Modificar Trafico

Finalmente, en la figura 7 se observa el correcto inicio de sesión a través de cambiar el hash al interceptar.

Figura 7: Login

2.6. Identifica las políticas de privacidad o seguridad

Sobre las políticas de privacidad o seguridad en Chile.

Según la Ley 19.628 sobre protección de datos personales[2], que está vigente, pero será reformada y mayormente reemplazada por la Ley 21.719 cuando ésta ultima entre en vigencia

- Artículo 1° – Principio general de protección

  Aquí dice que cualquier institución o persona que maneje datos personales debe respetar la privacidad del titular, esto incluye proteger contraseñas que permitan acceder a esos datos.

- Artículo 7° – Deber de secreto

  En este articulo se menciona que toda persona o entidad que maneje datos personales como contraseñas tiene deber legal de confidencialidad.

- Artículos 4°, 5° y 6° – Uso legítimo, transmisión y eliminación

  Por ultimo aquí se menciona que cualquier sistema que use contraseñas o guarde información de acceso debe hacerlo con consentimiento, propósito claro y trazabilidad.Además, si los datos como contraseñas antiguas ya no son necesarios, deben eliminarse o anonimizar.

Ley 21.719[3], esta ley entra en vigencia el 1 de diciembre de 2026.

- Artículo 12 – Medidas de seguridad

  Aquí se habla de proteger la contraseñas y credenciales de acceso mediante cifrado o hashing robusto, control de acceso, autenticación multifactor, auditorías de seguridad.

2.7. Comente 4 conclusiones sobre la seguridad del sitio escogido

- Para comenzar se observa que el https, figura 7 sale tachado, esto significa que la conexión no garantiza privacidad ni autenticidad total, y que los datos como contraseñas podrían ser leídos y modificados por terceros.

- Por otro lado tenemos que se usa MD5 el cual esta obsoleto y vulnerable a ataques de fuerza bruta, se puede romper en fácilmente. Por tanto, no debe emplearse para almacenar ni transmitir contraseñas.

- De la misma forma el hash en MD5 no incluye un salt por ejemplo, haciéndolo aun mas vulnerable, buscando el hash en bases publicas o utilizando rainbow tables.

[2]Ley 19.628. Disponible en `https://www.bcn.cl/leychile/navegar?idNorma=141599`

[3]Ley 21.719. Disponible en `https://www.bcn.cl/leychile/navegar?idNorma=1209272`

- Por ultimo, se observa también que en consola al momento de ingresar al sitio la variable se llama MD5, delatándose aun mas el hash. Cabe destacar que hashear en el cliente tiene sentido por ejemplo con un protocolo challenge-response donde el servidor envía un nonce y el cliente demuestra conocimiento de la contraseña sin enviarla, evitando así el replay.

Referencias

[1] Sergio Soto. *Laboratorios Criptografía.* `https://github.com/SergioSoto1/LaboratoriosCriptografia`