

Informe Laboratorio 3

Sección 1

Alumno: Sebastian Silva
e-mail: sebastian.silva_b@mail.udp.cl

Octubre de 2024

Índice

| | |
|---|----------|
| 1. Descripción de actividades | 2 |
| 2. Desarrollo de actividades según criterio de rúbrica | 2 |
| 2.1. Identifica el algoritmo de hash utilizado al momento de registrarse en el sitio | 3 |
| 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 | 7 |
| 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 | 9 |
| 2.7. Demuestra 4 conclusiones sobre la seguridad | 11 |

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:

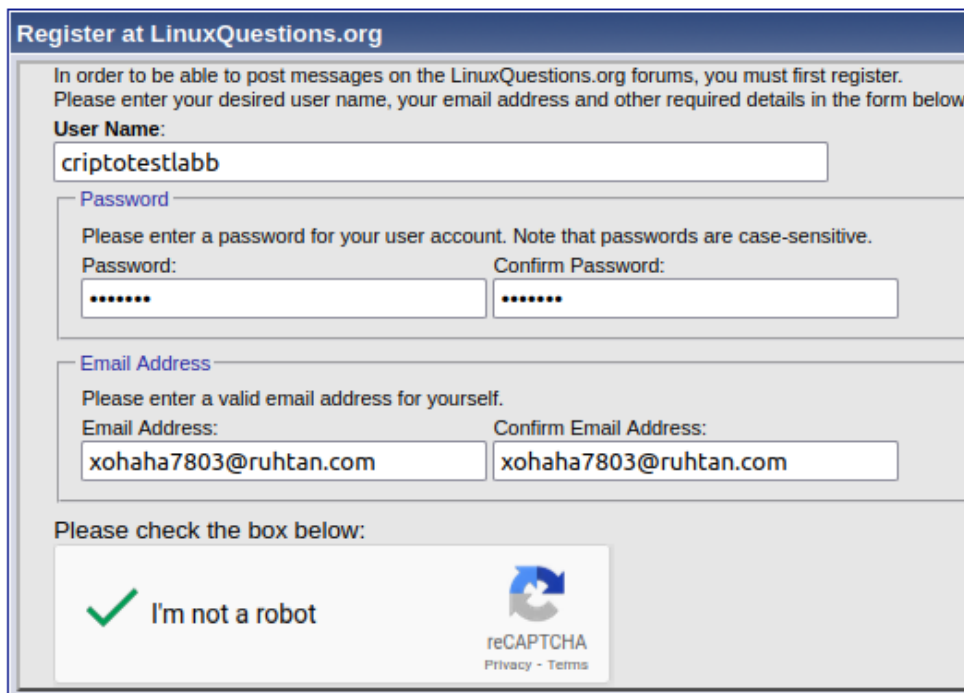
- Identificación del algoritmo de hash utilizado para las contraseñas al momento del registro en el sitio.
- Identificación del algoritmo de hash utilizado para las contraseñas al momento de iniciar sesión.
- Generación del hash de la contraseña desde la consola del navegador, partiendo de la contraseña 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

Para el desarrollo de este laboratorio se utilizara la pagina 'linuxquestion.org' donde se completara el registro y luego un inicio de sesion para revisar que algoritmo de hash esta utilizando. Cabe recalcar que se utilizaran herramientas adicionales para poder trabajar en esta experiencia, tales como 'hash analyzer' para verificar que algoritmo se esta empleando en la pagina a analizar y 'temp-mail.org' para generar mails temporales y no tener que usar el correo personal.

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

En primera instancia se realizara un registro en la pagina objetivo para luego utilizar la herramienta de inspeccionar elemento y poder identificar el algoritmo hash empleado en la pagina.



The image shows a web registration form for LinuxQuestions.org. The form is titled "Register at LinuxQuestions.org" and includes instructions: "In order to be able to post messages on the LinuxQuestions.org forums, you must first register. Please enter your desired user name, your email address and other required details in the form below." The form fields are as follows:

- User Name:** A text input field containing "criptotestlabbb".
- Password:** A section with two input fields. The first is labeled "Password:" and contains "*****". The second is labeled "Confirm Password:" and also contains "*****". A note above the fields states: "Please enter a password for your user account. Note that passwords are case-sensitive."
- Email Address:** A section with two input fields. The first is labeled "Email Address:" and contains "xohaha7803@ruhtan.com". The second is labeled "Confirm Email Address:" and also contains "xohaha7803@ruhtan.com". A note above the fields states: "Please enter a valid email address for yourself."
- reCAPTCHA:** A section with a checkbox labeled "I'm not a robot" and a reCAPTCHA logo. Below the checkbox is a green checkmark icon. The reCAPTCHA logo includes the text "reCAPTCHA" and "Privacy - Terms".

Figura 1: Visualización de registro

Posteriormente se utiliza la herramienta de inspeccionar elemento para verificar el algoritmo de hash que se esta empleando.

```
password_md5: "afdd0b4ad2ec172c586e2150770fbf9e"  
passwordconfirm_md5: "afdd0b4ad2ec172c586e2150770fbf9e"  
day: "0"  
month: "0"  
year: "0"  
username: "criptotestlabb"  
password: ""  
passwordconfirm: ""  
email: "xohaha7803@ruhtan.com"  
emailconfirm: "xohaha7803@ruhtan.com"
```

Figura 2: Visualización de algoritmo hash

Como se puede evidenciar en el recuadro azul, se tiene que la pagina utiliza un algoritmo de hash. Si bien, se puede ver visualmente que el codigo de la pagina utiliza MD5, se procedera a verificar el algoritmo con la herramienta hash analyzer.

Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

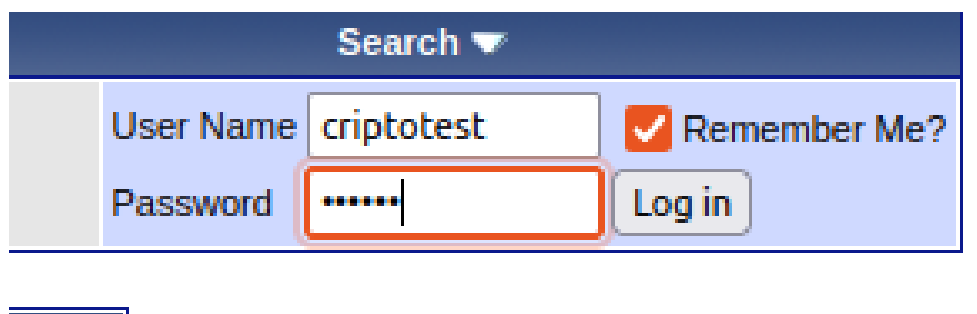
| | |
|--------------------------|----------------------------------|
| Hash: | afdd0b4ad2ec172c586e2150770fbf9e |
| Salt: | Not Found |
| Hash type: | MD5 or MD4 |
| Bit length: | 128 |
| Character length: | 32 |
| Character type: | hexidecimal |

Figura 3: Verificación del algoritmo hash del registro

Luego de utilizar la herramienta hash analyzer, se tiene que efectivamente la pagina objetivo utiliza MD5 o MD4 para cifrar sus contraseñas en el registro.

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

Para el siguiente punto, se realizara ahora un inicio de sesión, utilizando parametros aleatorios en los campos de usuario y contraseña a fin de identificar el algoritmo hash que se utiliza al momento de iniciar sesión.



The image shows a login form with a dark blue header containing a 'Search' button with a dropdown arrow. Below the header, there is a light blue box containing the login fields. The 'User Name' field contains the text 'criptotest'. The 'Password' field contains six dots, and it is highlighted with a red border. To the right of the password field is a 'Remember Me?' checkbox with a red checkmark. A 'Log in' button is located to the right of the password field.

Figura 4: Visualización de inicio de sesión

Se utilizan los parametros 'criptotest' y '12345' para rellenar los campos de inicio de sesión. Posteriormente se usara la herramienta de inspeccionar elemento para obtener el algoritmo hash que se usa.

```
vb_login_username: "criptotest"  
cookieuser: "1"  
vb_login_password: ""  
s: ""  
securitytoken: "guest"  
do: "login"  
vb_login_md5password: "e10adc3949ba59abbe56e057f20f883e"  
vb_login_md5password_utf: "e10adc3949ba59abbe56e057f20f883e"
```

Figura 5: Visualización del algoritmo hash del inicio de sesión

Como se ve en el recuadro azul, se tiene que la pagina utiliza un algoritmo de hash. A pesar que se puede ver visualmente que el codigo de la pagina utiliza MD5, se procedera a verificar el algoritmo con la herramienta hash analyzer.

Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

| | |
|--------------------------|----------------------------------|
| Hash: | e10adc3949ba59abbe56e057f20f883e |
| Salt: | Not Found |
| Hash type: | MD5 or MD4 |
| Bit length: | 128 |
| Character length: | 32 |
| Character type: | hexidecimal |

Figura 6: Verificación del algoritmo hash del inicio de sesión

Luego de utilizar la herramienta hash analyzer, se tiene que efectivamente la pagina objetivo utiliza MD5 o MD4 para cifrar sus contraseñas en el incio de sesión.

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

Para generar la contraseña desde la consola del navegador se utilizara un script de modo que se pueda utilizar el algoritmo MD5 para generar el hash. A continuación se presenta el script utilizado junto con la contraseña cifrada.

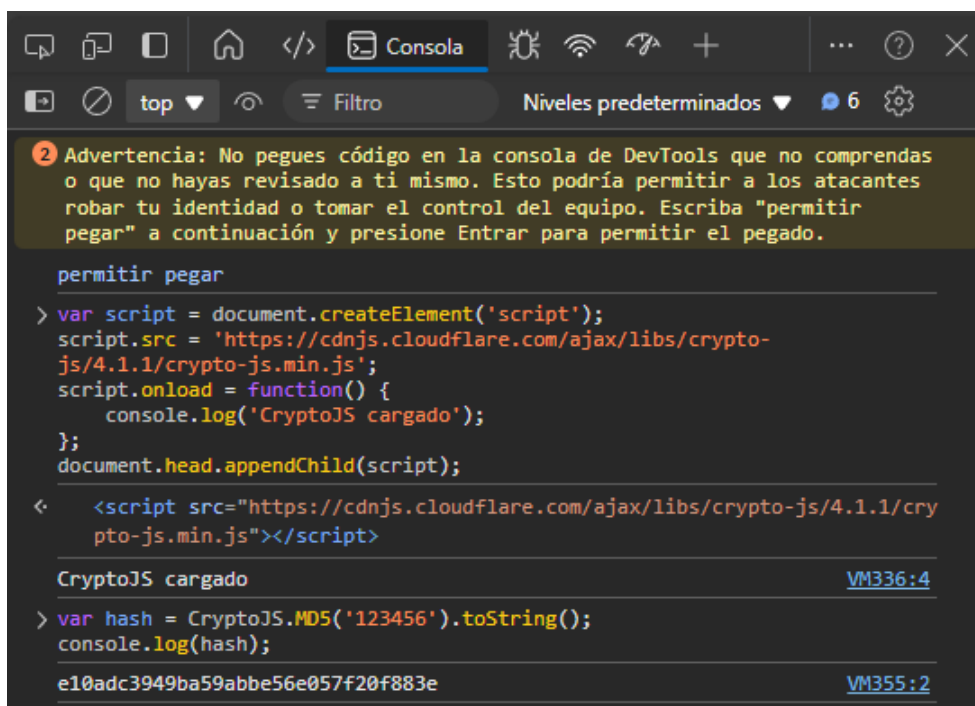


Figura 7: Utilización del script junto con hash obtenido

La primera parte del código consiste en cargar dinámicamente la biblioteca CryptoJS para luego calcular y mostrar el hash MD5 de la cadena '123456'.

2.4. Intercepta el tráfico login con BurpSuite

Para este punto se pide interceptar el tráfico con BurpSuite, de este modo al interceptar el login se obtiene lo siguiente:

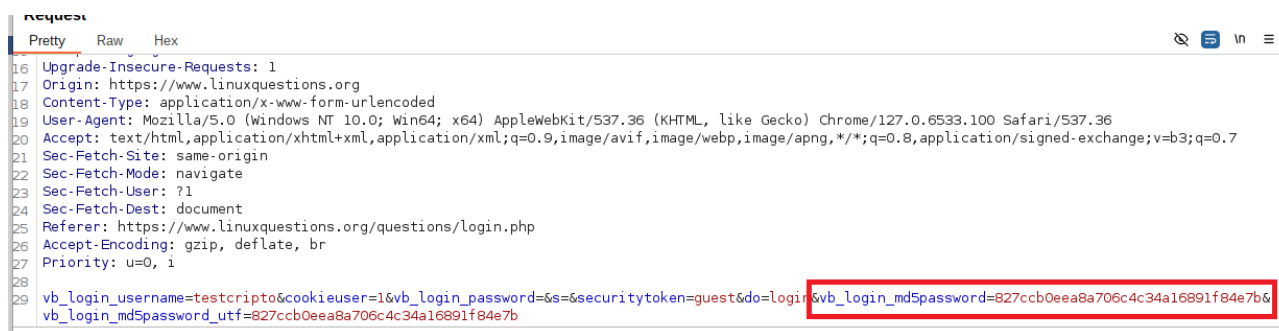


Figura 8: Tráfico interceptado con BurpSuite

En este caso se tiene un login incorrecto, sin embargo se le aplicó el algoritmo de hash a la contraseña, tal como se aprecia en el recuadro rojo.

2.5. Realiza el intento de login

Ahora para realizar el intento de login, se va a utilizar la contraseña correcta 'Aa12345' luego de aplicar el algoritmo de hash modificando los parametros en los campos de 'vb_login_md5password' (campo remarcado en rojo en la figura anterior) mientras se esta interceptando el tráfico. De esta forma se tiene lo siguiente:



Figura 9: Tráfico interceptado con BurpSuite con la contraseña correcta

Ahora que se tiene la contraseña, y a su vez, el hash correcto, se realiza un forward para mandar los datos a la pagina. Al ser los campos correctos, la pagina tomara como un inicio de sesión exitoso evidenciandose a continuación:

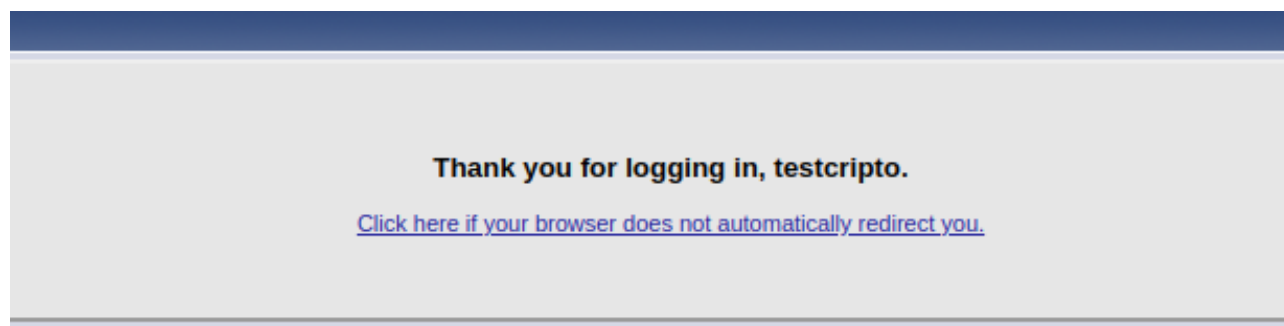


Figura 10: Inicio de sesión exitoso

Cabe recalcar que se tuvo que utilizar credenciales distintas a la que se mostraron en el registro, ya que existieron ciertas complicaciones a la hora de realizar esta experiencia.

2.6. Identifica las políticas de privacidad o seguridad

Las políticas de privacidad y seguridad se identifican a continuación:

By jeremy at 2018-05-25 16:53

Privacy Policy

LinuxQuestions.org does not sell members' personal information.

We collect the following personal information: email address, username, password, and IP address. We use this information to operate, maintain, and improve the site.

We will only use this information for the purposes for which we collected or received it.

Advertising

This site displays 3rd party ads. We do not share any information with any 3rd party directly.

External Links

This site contains links to other sites. We are not responsible for the privacy practices or the content of such Web sites.

Public Forums

This site makes chat rooms, forums, message boards, and/or news groups available to its users. Please remember that any information that is disclosed in these areas becomes public information and you should exercise caution when deciding to disclose your personal information.

Security

This site has security measures in place to protect the loss, misuse, and alteration of the information under our control.

Third Party Tools

We may use third party tools to improve the performance and features of our Website. These third party tools are designed to collect only non-personal information about your use of our Website. However, you understand that such tools are created and managed by parties outside our control. As such, we are not responsible for what information is actually captured by such third parties or how such third parties use and protect that information.

Figura 11: Políticas de privacidad y seguridad

En este caso, la política de LinuxQuestions.org establece que no venden la información personal de sus miembros, pero recopilan datos como el correo electrónico, nombre de usuario, contraseña y dirección IP con el propósito de operar, mantener y mejorar el sitio.

También menciona que el sitio contiene enlaces a otras páginas web, pero no asume responsabilidad por las prácticas de privacidad o el contenido de esos sitios externos. Los foros del sitio permiten la divulgación de información personal, por lo que los usuarios deben tener cuidado al compartir datos.

Por la parte de la seguridad, se ha implementado medidas para proteger la información contra la pérdida, uso indebido y alteración. Además, la página puede utilizar herramientas de terceros para mejorar las funcionalidades del sitio, pero no se hace responsable de cómo se utilicen esos datos.

2.7. Demuestra 4 conclusiones sobre la seguridad

En base a la experiencia realizada se puede concluir lo siguiente:

- Se usan algoritmos de hash débiles: El sitio utilizado usa MD5 o MD4 para cifrar las contraseñas. Dichos algoritmos son considerados inseguros para la protección de contraseñas debido a su vulnerabilidad a ataques de colisión. De este modo lo mejor que se puede hacer es implementar algoritmos más robustos como SHA-256.
- Se tiene exposición potencial en foros públicos: En base que el sitio permite a los usuarios compartir información en los foros, cualquier dato personal divulgado se convierte en información pública, presentando de este modo un riesgo para la privacidad de los usuarios si no tienen cuidado al compartir sus datos.
- Tiene dependencia de herramientas de terceros: La página utiliza herramientas de terceros para mejorar el rendimiento y las funciones del sitio web, implicando de este modo la recopilación de información por parte de estas herramientas. Si bien la política de privacidad aclara que no se responsabilizan de cómo estas herramientas manejan los datos, sigue representando un riesgo potencial para la seguridad de la información.
- Existen medidas de seguridad básicas implementadas: El sitio tiene implementado medidas para proteger la información contra pérdida, uso indebido y alteración. A pesar de esto se podrían utilizar técnicas más avanzadas como la autenticación multifactor, ayudando a mejorar la protección de la información.