Trabajo en clase _1_ DE TECNOLOGÍAS DE SEGURIDAD

TEMA: Hash

Nombre: Ariel Suntasig

Carrera: Software

Grupo: GR1

Fecha: 02/01/2024

1. OBJETIVOS

- Explicar qué son las colisiones de hash y cómo se pueden interpretar.
- Indicar las limitaciones y riesgos de las colisiones de hash para la seguridad de los datos.

2. INFORME

Imágenes con MD5:

Una colisión, en el contexto de las funciones hash, se refiere a una situación en la que dos entradas diferentes producen el mismo valor hash de salida. Se considera una vulnerabilidad de seguridad porque puede dar lugar a varios ataques que comprometen la integridad y autenticidad de los datos.

Imagen 1:

Hash 1:

Tu hash generado

hex: 253dd04e87492e4fc3471de5e776bc3d

HEX: 253DD04E87492E4FC3471DE5E776BC3D

h:e:x: 25:3d:d0:4e:87:49:2e:4f:c3:47:1d:e5:e7:76:bc:3d

base64: JT3QTodJLk/DRx3l53a8PQ==

Imagen 2:

Hash 2:

Your generated hash

hex: 253dd04e87492e4fc3471de5e776bc3d

HEX: 253DD04E87492E4FC3471DE5E776BC3D

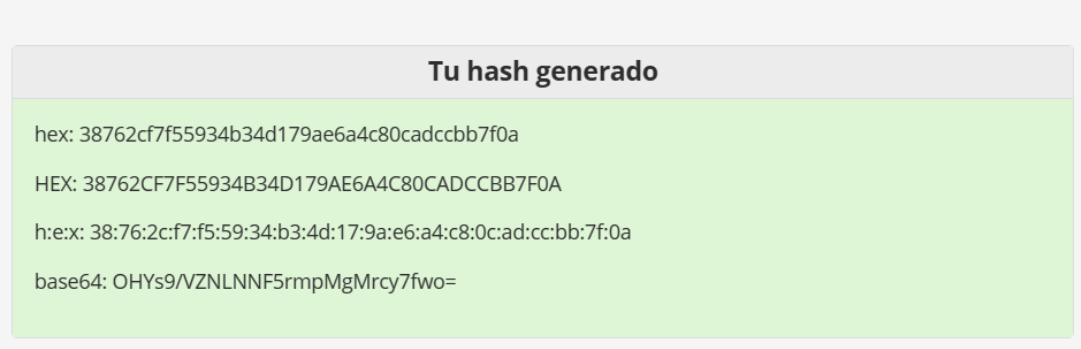
h:e:x: 25:3d:d0:4e:87:49:2e:4f:c3:47:1d:e5:e7:76:bc:3d

base64: JT3QTodJLk/DRx3l53a8PQ==

Donde los hashes entregados por la aplicación web son valores hexadecimales de 16 bytes que representan el mismo valor binario. El valor base64 es otra forma de codificar el valor binario en un formato de texto. El algoritmo de hash que se usó para generar estos valores es MD5, que es un algoritmo común que tiene una longitud de salida de 16 bytes.

Ahora lo probamos con los Documentos con Sha-1:

Hash 1 con pdf:



Hash 2 con pdf:

Donde Los hashes son valores hexadecimales de 20 bytes que representan el mismo valor binario. El valor base64 es otra forma de codificar el valor binario en un formato de texto. Se uso una herramienta en línea para obtener el hash. El algoritmo de hash que se usó para generar estos valores es SHA-1, que es un algoritmo que tiene una longitud de salida de 20 bytes.

¿Qué funciones tiene el PIN?

El PIN es una contraseña que protege el acceso y el uso del certificado digital en una firma electrónica. El certificado digital contiene la clave pública y la clave privada del usuario, que se usan para cifrar y descifrar los datos que se firman. El PIN se utiliza en la parte del proceso de firma digital donde se necesita confirmar la identidad y la autorización del firmante. Por ejemplo, cuando se quiere firmar un documento electrónico, se solicita el PIN para acceder al certificado digital que contiene las claves criptográficas que se usan para generar y verificar la firma.

3. CONCLUSIONES Y RECOMENDACIONES

- Las colisiones de hash ocurren cuando dos entradas diferentes producen el mismo valor hash de salida.
- Las colisiones de hash son una vulnerabilidad de seguridad que puede dar lugar a varios ataques que comprometen la integridad y autenticidad de los datos.
- Las funciones hash se usan para varios propósitos, como la verificación de la integridad de los datos, la generación de contraseñas, la firma digital y la criptografía.

4. BIBLIOGRAFÍA

[1] "Conversor online - convertir gratis vídeos, imágenes, audio y textos", online-convert.com. Consultado: el 2 de enero de 2024. [En línea]. Disponible en: https://www.online-convert.com/es/result

[2] "Conversor online - convertir gratis vídeos, imágenes, audio y textos", online-convert.com. Consultado: el 2 de enero de 2024. [En línea]. Disponible en: https://www.online-convert.com/es/result