

Desencriptación de contraseñas

Contenido

Prueba 1.....	2
Solución.....	3
Prueba 2.....	4
Solución.....	5
Prueba 3.....	7
Solución.....	8

Prueba 1

Se nos indican 3 contraseñas con las siguientes condiciones:

1. Deben tener como mínimo 8 caracteres.
2. Deben tener al menos un carácter de cada uno de los siguientes tres grupos:
 - a. Letras (mayúsculas y minúsculas): A, B, ... a, b...
 - b. Caracteres numéricos: 0, 1, 2,...,9
 - c. Símbolos: ! @ # \$ % & * ^ () - = { } [] \ : ; < > ? , . /

No existe mecanismo alguno que controle el cumplimiento de estas condiciones.

Me dan el nombre de usuario y la contraseña cifrada con un algoritmo de hashing.

Nombre del usuario	Username	Contraseña
Gonzalo García Panete	gogapanet	f63487f19ed4f53a5e60db806e477217c5ce51ce
Sergio Serote Minerva	sesemin	b1b3773a05c0ed0176787a4f1574ff0075f7521e
Marta Hidalgo Perez	marhidper	35a9c2444ec63ee39f3b214edb9011f32e624a28

El primer usuario “Ha decidido poner una contraseña contenida en la RAE”.

El segundo “Ha buscado en Google contraseñas más comunes”

El último ha dicho que “tiene puesta una contraseña jugando con algunas de las letras de su nombre y apellidos con un número al final”.

Solución

La primera contraseña la he sacado usando tabla arcoíris, ya que el enunciado dice que la contraseña está en la RAE, en específico he usado la página:

<https://crackstation.net/> y era repleto.

La página también provee información sobre su método de encriptación, sha1, el cual hoy en día no se considera seguro por su alta probabilidad de colisión.

La segunda he vuelto a usar la misma web, ya que es una contraseña común, y es qwerty.

Al igual que la anterior también es sha1.

La tercera al no estar contenida en ningún sitio he usado la fuerza bruta, he usado la página <https://hashes.com/en/decrypt/hash> y ha salido aaeiao5.

Otra vez SHA1, nada recomendable a no ser que la información a guardar sea irrelevante.

La primera no tiene 8 caracteres tampoco no tiene mayúsculas, caracteres numéricos ni símbolos.

La segunda no cumple ninguna de las condiciones propuestas.

La tercera tiene menos de 8 caracteres, y no tiene ni símbolos ni mayúsculas.

En conclusión ninguno de los 3 usuarios cumple las condiciones.

Prueba 2

Nos dan las mismas condiciones que antes.

Nombre	Username	Contraseña ^[1]	Salt	Comentarios de los empleados
Nathan Anderson Reese	natanres	6wH3Kcx+lkcmvmaQ/1jxcn9lWnROKVRdT0q8bgJt230=	12	“...Yo he usado una palabra rarísima, además es una palabra en inglés”
Elijah Parker Rodriguez	elijahparrod	07xatxNgb9iNdV8d9Qj57tiLL4M2Ilf4Yq2PLw+bLNo=	23	“ ... Yo no me he complicado, he usado una contraseña común pero le he añadido al final un punto y dos números”
Lily Bennett Mitchell	libenmitch	xenxjtkvuWoG2m3KHUHsR9pfmYxoFn3vntEcPdFriR0=	94	“... Pues mi contraseña es una combinación con la fecha de mi cumpleaños”

-Codificación Base64

ESTA INFORMACIÓN PODIA NO SER VERDAD

Cual o cuales de los usuarios no cumple las condiciones?

Solución

Para esto usare Hashcat 6.2.6 instalado en <https://hashcat.net/hashcat/>, ya que uso Windows lo instalo en 7z binario.

Los resultados obtenidos son:

Primero paso los hash de base64 a hexadecimal, el número de dígitos era de 64, por lo que dedujimos que usaba SHA-256 ya que $64 \times 4 = 256$, por ello uso el modo -m 1410 en hashcat.

Para la primera contraseña usamos un ataque por diccionario usando el diccionario rockyou:

```
hashcat -m 1410 -a 0  
eb01f729cc7e224726be6690ff58f1727f655a744e29545d4f4abc6e026ddb7d:12C:\User  
s\julio\Desktop\Diccionarios_hashcat\rockyou.txt
```

(:12 indica el salt)

La contraseña obtenida es: satisfaction12, que quitándole el salt es satisfaction. Por lo que podemos observar que incumple las políticas de seguridad 2.a, ya que no tiene letras en mayúsculas, la 2.b y la 2.c ya que tampoco tiene caracteres numéricos ni símbolos.

Le recomendaría al usuario alternar entre mayúsculas y minúsculas e incluir numeros y símbolos para fortalecer la seguridad de la contraseña, también sería recomendable no usar una palabra comprendida en el diccionario de la lengua más hablada.

Para la segunda contraseña genere un fichero con un script de Python que contenía todas las posibles combinaciones de 2 números precedidos de un .
(.0099) lo combinamos con el diccionario anterior y le añadimos el salt (:23).

```
hashcat-6.2.6>hashcat -m 1410 -a 1  
d3bc5ab713606fd88d755f1df508f9eed88b2f83369657f862ad8f2f0f9b2cda:23  
C:\Users\julio\Desktop\Diccionarios_hashcat\rockyou.txt  
C:\Users\julio\Desktop\Diccionarios_hashcat\0099.txt
```

Hallamos la contraseña: password.5223

A primera vista vemos que únicamente incumple la política de seguridad 2.a, ya que no tiene letras en mayúsculas pero si numeros y símbolos.

Le recomendaría al usuario alternar entre mayúsculas y minúsculas para fortalecer la seguridad de la contraseña, también sería recomendable no usar una palabra tan común siendo la traducción de la palabra contraseña en inglés.

Con la tercera contraseña aplico el diccionario rockyou y al tratarse de una combinación de numeros (aunque correspondía a una fecha de nacimiento) estaba contenido en dicho diccionario por lo que añadiéndole el salt (:94).

```
hashcat -m 1410 -a 0  
c5e9f18ed92fb96a06da6dca1d41ec47da5f998c68167def9ed11c3dd16b891d:94  
C:\Users\julio\Desktop\Diccionarios_hashcat\rockyou.txt
```

La contraseña es: 14111993

Podemos observar que incumple las políticas de seguridad 2.a, ya que no tiene letras, ni en mayúsculas ni minúsculas y la 2.c ya que tampoco tiene símbolos.

Le recomendaría al usuario incluir mayúsculas y minúsculas e incluir símbolos para fortalecer la seguridad de la contraseña.

Prueba 3

Buscar en internet una aplicación para ser utilizada por los usuarios desde un ordenador o un móvil, y que les permita obtener contraseñas seguras (el tamaño debe ser a elección del usuario) a partir de palabras que el usuario recuerde fácilmente.

Solución

He encontrado dos páginas distintas que me parecen interesantes comentar:

La primera con la que creo que más claramente se cumple la consulta del cliente:

<https://www.lastpass.com/es/features/password-generator>

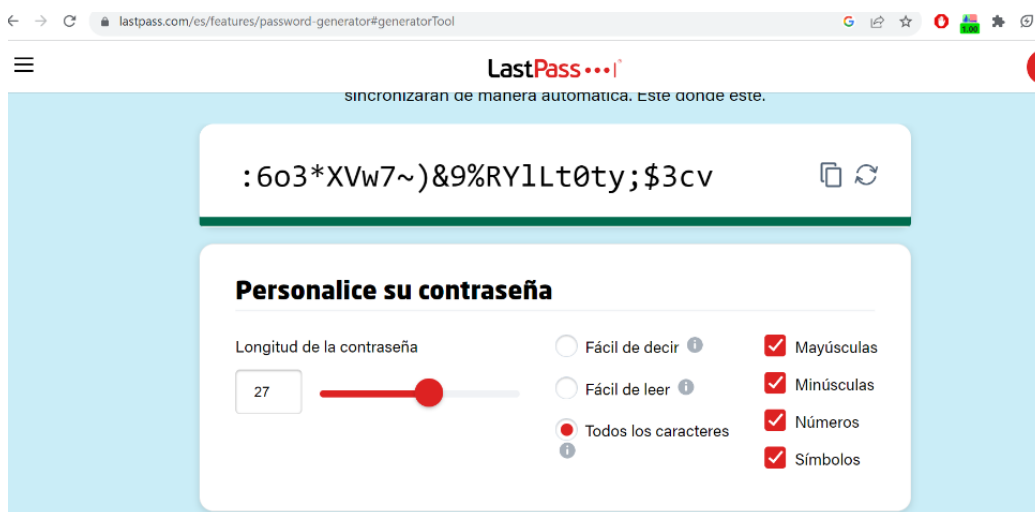
Con esta página puedes generar contraseñas robustas con la longitud, y robustez que desee el usuario, lo que le puede venir muy bien ya que te aseguras de que la contraseña va a ser robusta, además puedes descargarla como pide el cliente en su página principal registrándote como usuario o empresa.

Menos contraseñas, menos complicaciones

Prepárese para un futuro sin contraseñas con una protección sin fisuras.



Además tiene la ventaja de ser de una empresa líder del sector con múltiples planes, atención al cliente etc que pueden servir de mucha ayuda para gestionar las contraseñas de nuestra empresa.



Y con la segunda que puede servir para almacenar en local las contraseñas guardando la key y el encriptado en sitios distintos, ya que uno de los ataques más usuales viene por parte de brechas de seguridad físicas en nuestros empleados como apuntar las contraseñas en papeles etc, con esta página necesitarían ambas para recuperar la contraseña:

<https://www.devglan.com/online-tools/text-encryption-decryption>

El usuario elegiría una palabra como contraseña, la que él prefiera, por ejemplo patata, con la página la encriptaría y usaría una palabra clave la cual puede ser por ejemplo frita, si en algún momento se le olvida la palabra que él usó para encriptar, que sería patata, con la clave en este caso frita y el encriptado que debe tener guardado en un lugar seguro puede recuperarla donde quiera, o sea le servirá como seguridad por si le roban la palabra guardada encriptada ya que no podrán hacer nada con ella sin la clave que es frita.

Ambas páginas se pueden combinar para dar un paso más en seguridad.

Text Encryption	Text Decryption
Enter any text to be Encrypted	Enter encrypted text to Decrypt
<input type="text" value="patata"/>	<input type="text" value="0oqiYkfT0m/YiywMiAZ6dA=="/>
<input type="checkbox"/> Encrypt with a custom secret key	<input type="checkbox"/> Decryption requires a custom secret key
Enter Secret Key (Remember, the encrypted text can't be decrypted without this secret key)	Enter Secret Key (The same key used during encryption)
<input type="text" value="frita"/>	<input type="text" value="frita"/>
<input type="button" value="Encrypt"/>	<input type="button" value="Decrypt"/>
Encrypted Output:	Decrypted Text:
<input type="text" value="0oqiYkfT0m/YiywMiAZ6dA=="/>	<input type="text" value="patata"/>

