modulo_cripto

Módulo externo para criptografia de senhas.

Dependências necessárias

Biblioteca hashlib - https://pypi.org/project/hashlib/

Sobre o módulo

O módulo contém apenas uma função de chamada, "generate_hashed_password", que pode ser chamada ao importar o módulo para dentro da aplicação.

generate_hashed_password(cryptography, password, salt, iterations, dklen)

Recebe um tipo de criptografia, uma senha, um salt, o número de iterações para hasheamento e o tamanho da chave derivada que se deseja criar e retorna uma chave derivada, sendo essa a chave recebida já criptografada.

Parâmetros da função

cryptography: Recebe uma string com o tipo de algoritmo de hasheamento que deseja que seja usado. Essa string deve conter um dos nomes que estão implementados no módulo e que serão descritos a seguir (pode ser colocado tanto em maiúsculo quanto em minúsculo). Os tipos que estão previsto em nossa aplicação são:

Criptografias Recomendadas

SHA256 - recomendado para criptografia de senhas para usuários

MD5 - recomendado para criptografia de senhas para usuários

SHA384 - recomendado para criptografia de mensagens

SHA224 - recomendado para criptografia de senhas para usuários

BLAKE2B - recomendado para criptografia de senhas para usuários

BLAKE2S - recomendado para criptografia de senhas para usuários

Criptografias não recomendadas

SHA512 - recomendado para criptografia de senhas para bancos

SHA1 - recomendado para salvar dados de aplicações em que a segurança não é tão importante, visto que já existem formas de quebrar

password: Recebe uma string com a senha se que deseja criptografar

salt: Recebe uma string contendo um salt, uma cadeia de caracteres hexadecimais gerados de forma aleatória visando o aumento na complexidade da senha. Não se deve armazenar 2 salts iguais em uma aplicação e o salt deve ter o tamanho de 32 bytes.

iterations: Um número inteiro contendo o número de iterações que serão feitas no hasheamento. Números baixos podem facilitar a quebra da criptografia com um ataque de colisão, enquanto números muito altos podem diminuir a eficiência da mesma. Recomenda-se utilizar no mínimo 100 iterações no módulo.

dklen: O número, em bytes, do tamanho da chave que se quer gerar. Aumentando o tamanho da chave, aumenta-se, também, a complexidade para criá-la, por isso recomenda-se o tamanho de 64 bytes para senhas geradas.

Retorno da função

A função retorna uma string com o número de bytes de tamanho do parâmetro dklen, sendo essa a chave derivada. Essa chave pode ser recriada somente chamando a função novamente com exatamente os mesmos parâmetros. Caso se mude algum dos parâmetros diferentes de dkle, uma chave sem nenhuma conexão com a anterior será gerada, independente da mudança que foi feita.

Caso a função receba um parâmetro “cryptography” com uma string não prevista na documentação o valor de retorno será -1.

Exemplo

Se quisermos criptografar a senha “123456” utilizando o algoritmo sha256 com 100 iterações e com o salt “60122ddcef63a220bb78e9e41d380146”, gerando uma senha de 64 bytes chamaremos a função:

```
from modulo_cripto import generate_hashed_password

generate_hashed_password('sha256','123456','60122ddcef63a220bb78e9e41d380146', 100, 64)
```

```
# Gera a chave derivada
cc33f240d3a3494c1b23771a373be24ddce39327503ab7c39fb1b67ccdab27d6
```

Alexandre Leite de Moraes Coelho

Bernardo da Costa Tomaz Delgado

Enrico Vergolino Gnani

Eric Ruas Leão

Felipe Khouri Gameleira

Gabrielle Trajano Mulinari