

Pbkdf2PasswordEncoder

Criptografia baseada em hashes iterados

A PBKDF2 é uma função de derivação de chave com um custo computacional maleável, usada para reduzir vulnerabilidades de ataques de força bruta que buscam reverter o hash.

fonte : <https://cryptobook.nakov.com/mac-and-key-derivation/pbkdf2>

Quais atributos formam a chave ?

key = pbkdf2(senha, salt, iteracoes, funcao-hash, tamanho-chave-derivada)

Senha

O segredo da aplicação, representado por um array de bytes, string. Que deve ter, minimamente (na recomendação do método criptográfico) de 8 a 10 chars de comprimento.

Iterações

Número de iterações da função hash, a qual é reaplicada sobre os resultados anteriores da criptografia.

Salt

Sequência de bytes gerada randomicamente, com o intuito de serem concatenadas/embralhadas de forma metódica com a senha antes de passar pela função hash.

Tamanho-Chave

Tamanho do output desejado pela chave encriptada.

Função Hash

Algoritmos matemáticos unilaterais usados para mapear dados de qualquer tamanho para uma sequência de bits de tamanho fixo.

Como a chave é formada ?

A função de criptografia é a operação xor da enésima iteração da cadeia de funções hash.

- A primeira iteração usa a senha(segredo), concatenada com o “salt” e adicionada o número da iteração no formato “big-endian 32-bit integer”.
- As seguintes iterações usam a primeira chave gerada como o novo input, e isso acontece n vezes.

