

LICENCIATURA EM SEGURANÇA INFORMÁTICA EM REDES DE
COMPUTADORES

Encriptação e Desencriptação

Método AES-256-CBC

Relatório

Realizado por: Hugo Leite Martins (8230273)

Unidade Curricular: Segurança Informática

Índice

1. Introdução	3
2. Desenvolvimento	4
2.1. Execução do projeto	4
2.2. Secção de registo	5
2.2.1. Página de login	7
2.2.2 Página de verificação de login	8
3. Página principal	9
3.1. Página do utilizador	10
3.2 Página de detalhes do utilizador	11
3.3. Página de descriptação	12
4. Método de descriptação	13
4.1. Resultados	14
5. Conclusão	15
6. Referências	16

Índice de figuras

Figura 1 – Base de dados	4
Figura 2 – Página de registo	5
Figura 3 – Verificação da conta	6
Figura 4 – Página de login	7
Figura 5 – Código autenticação dois fatores	8
Figura 6 – Página de verificação	9
Figura 7 – Página principal	10
Figura 8 – Página do utilizador	11
Figura 9 – Página de detalhes do utilizador	12
Figura 10 – Página de descriptação	13
Figura 11 – Descriptação da palavra-passe	14
Figura 12 – Palavra-passe descriptografada	15

1.Introdução

Este projeto consiste no desenvolvimento de um website, no qual o objetivo principal é implementar métodos de segurança para o fortificar.

De forma a atingir este objetivo elaborei quatro métodos de segurança, os quais foram:

- Palavra-passe segura, obrigando à utilização de mais de 8 caracteres e o uso de um símbolo especial;
- Verificação da conta via email;
- Autenticação dois fatores;
- Encriptação da palavra-passe.

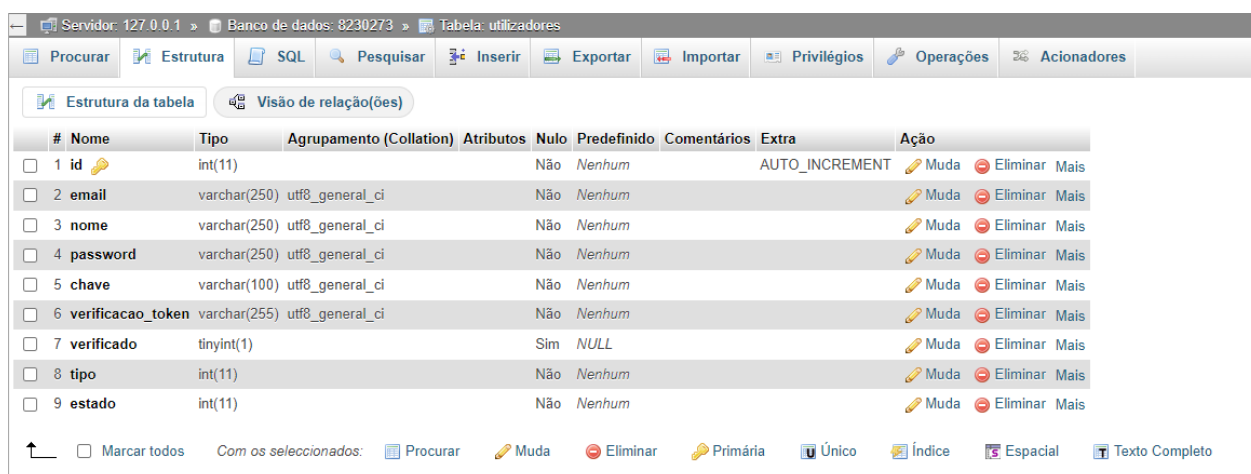
Tendo mostrado os objetivos do projeto, vou agora explicar como é que implementei estes métodos.

2. Desenvolvimento

2.1. Execução do projeto

A programação deste projeto foi dividida em secções, utilizando diversas linguagens de programação, entre as quais:

- HTML5;
- CSS3;
- JavaScript;
- PHP;
- MySQL como servidor de gestão de base de dados (Figura 1).



The screenshot shows a MySQL database management interface. The top bar indicates the server is '127.0.0.1', the database is '8230273', and the table is 'utilizadores'. Below the bar are tabs for 'Procurar', 'Estrutura', 'SQL', 'Pesquisar', 'Inserir', 'Exportar', 'Importar', 'Privilégios', 'Operações', and 'Acionadores'. The 'Estrutura' tab is active, showing the table structure. The table has 9 columns: #, Nome, Tipo, Agrupamento (Collation), Atributos, Nulo, Predefinido, Comentários, Extra, and Ação. The columns are: 1 id (int(11), AUTO_INCREMENT), 2 email (varchar(255), utf8_general_ci), 3 nome (varchar(255), utf8_general_ci), 4 password (varchar(255), utf8_general_ci), 5 chave (varchar(100), utf8_general_ci), 6 verificacao_token (varchar(255), utf8_general_ci), 7 verificado (tinyint(1), NULL), 8 tipo (int(11)), and 9 estado (int(11)). Each row has a checkbox and a 'Muda' button. At the bottom, there are buttons for 'Marcar todos', 'Com os seleccionados', 'Procurar', 'Muda', 'Eliminar', 'Primária', 'Único', 'Índice', 'Espacial', and 'Texto Completo'.

#	Nome	Tipo	Agrupamento (Collation)	Atributos	Nulo	Predefinido	Comentários	Extra	Ação
<input type="checkbox"/>	1 id	int(11)			Não	Nenhum		AUTO_INCREMENT	<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	2 email	varchar(255)	utf8_general_ci		Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	3 nome	varchar(255)	utf8_general_ci		Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	4 password	varchar(255)	utf8_general_ci		Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	5 chave	varchar(100)	utf8_general_ci		Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	6 verificacao_token	varchar(255)	utf8_general_ci		Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	7 verificado	tinyint(1)			Sim	NULL			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	8 tipo	int(11)			Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais
<input type="checkbox"/>	9 estado	int(11)			Não	Nenhum			<input type="checkbox"/> Muda <input type="checkbox"/> Eliminar Mais

Figura 1 – Base de dados

2.2. Secção de registo

A secção de registo é talvez a mais simples em termos de programação.

No entanto, é de grande importância na plataforma, como etapa inicial para registo dos utilizadores na plataforma.

Esta página (Figura 2) possui um formulário simples de registo do utilizador. O mesmo deverá inserir o nome desejado, um email válido e uma palavra-passe de acesso que será criptografada para haver uma maior segurança na criação de contas.

Com esse método implementado, decidi, então, introduzir outro, pois a segurança nunca é demais. Neste caso, foi a palavra-passe forte, ou seja, é necessário a implementação de uma palavra-passe com mais de 8 carateres e um elemento especial para ser possível que o registo seja concluído com sucesso.

PT ENG

ENTRAR

PÁGINA PRINCIPAL

Registar

NOME*

ENDEREÇO DE E-MAIL*

PALAVRA-PASSE*

CONFIRMAR PALAVRA-PASSE*

submit

2024 ESTG - Escola Superior de Tecnologia e Gestão (Hugo Martins)

Figura 2 – Página de registo

Caso o registo seja bem-sucedido, o utilizador será imediatamente redirecionado para a página login e ser-lhe-á enviado um email para verificar a sua conta criada na plataforma. Assim sendo, terá de verificar a conta antes de realizar o login, pois, se não verificar, não será possível a realização do mesmo.

Com o email, também é enviado o código de descriptação random de 32 bytes (256 bits) de binário para hexadecimal. Ao mesmo tempo, é enviado para a base de dados um token de 50 bytes (400 bits) de binário para hexadecimal que será o código temporário, enquanto o email não for verificado. Quando tal suceder, o token irá ser apagado automaticamente da base de dados, passando o “verificado” de 0 para 1, sendo assim possível a realização do login.

Eu usei este tipo de código random, pois é o melhor para o método de descriptação que foi utilizado e que irei explicar mais á frente.

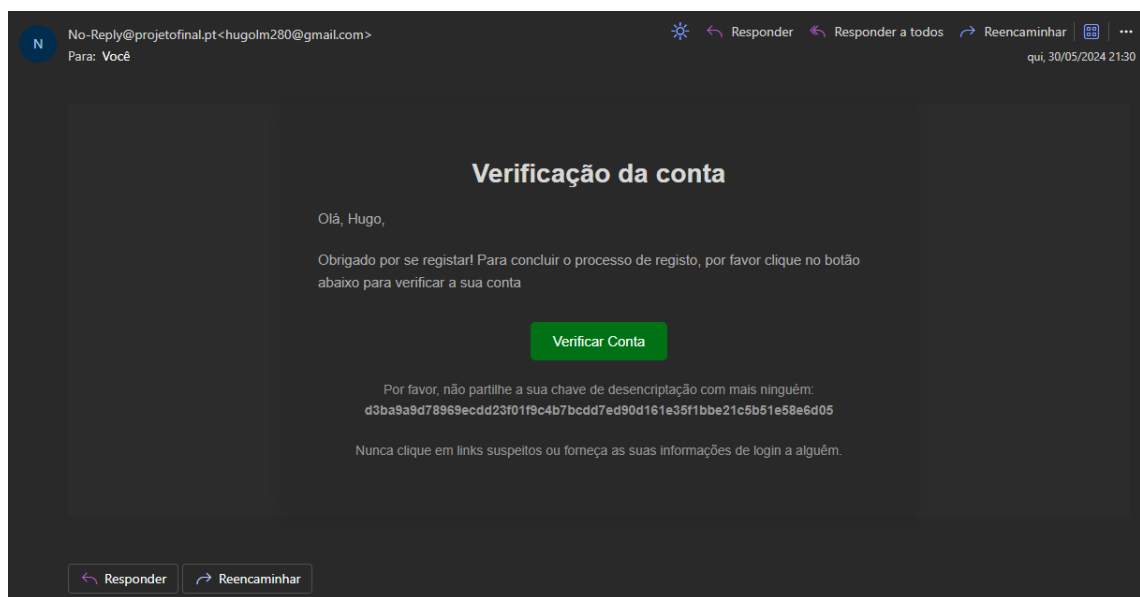


Figura 3 – Verificação da conta

2.2.1. Página de login

Esta página é muito conhecida para uma grande parte dos utilizadores, pois tornou-se universal em qualquer site.

O utilizador tem, apenas, de colocar a combinação de email e palavra-passe com que se registou para efetuar o login na plataforma.

Figura 4 – Página de Login

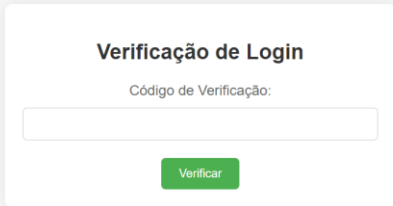
De acordo com o que foi pedido, implementei um método de segurança adicional, a autenticação de dois fatores, ou seja, sempre que o utilizador vai realizar o login na plataforma será lhe enviado um email com um código único de 6 dígitos que será para introduzir na página de verificação do código para ver se realmente é o utilizador certo que esta a tentar entrar.

Figura 5 – Código autenticação dois fatores

2.2.2 Página de verificação de login

Esta página apresenta um formulário para introduzir o código único de 6 dígitos enviado para o email para realizar a verificação do utilizador para entrar na conta.

Após a verificação, se o código for aprovado, será redirecionado para a página do utilizador.



O formulário, intitulado "Verificação de Login", está centralizado numa página cinzenta. Contém o rótulo "Código de Verificação:" seguido por um campo de entrada de texto. Abaixo do campo, há um botão verde com o texto "Verificar".

Figura 6 – Página de verificação

3. Página principal

Após efetuar o login, irá aparecer a página principal, que permite ao utilizador concluir, à primeira vista, que se trata de um site relacionado com segurança neste caso encriptação e desencriptação de dados, e também, gerir o fluxo de consultas do site, ou seja, visualizar quantos pessoas temos registadas no site.

Para além disso, existem vários menús como: utilizadores e encriptação e desencriptação.

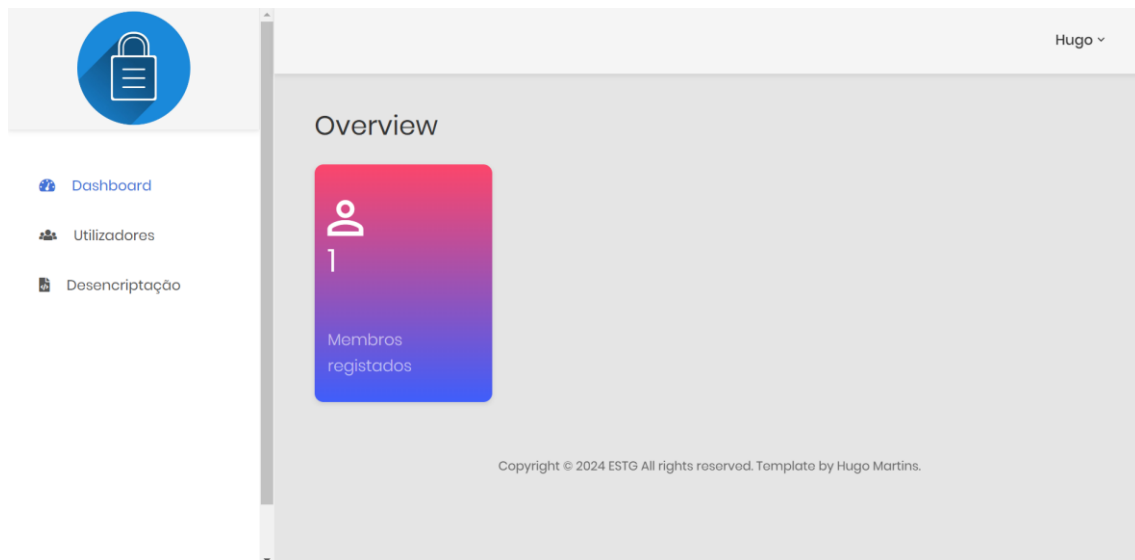


Figura 7 – Página principal

3.1. Página do utilizador

Ao seleccionar “utilizadores” será redireccionado para uma página onde terá o perfil que criou no registo e a palavra-passe criptografada.

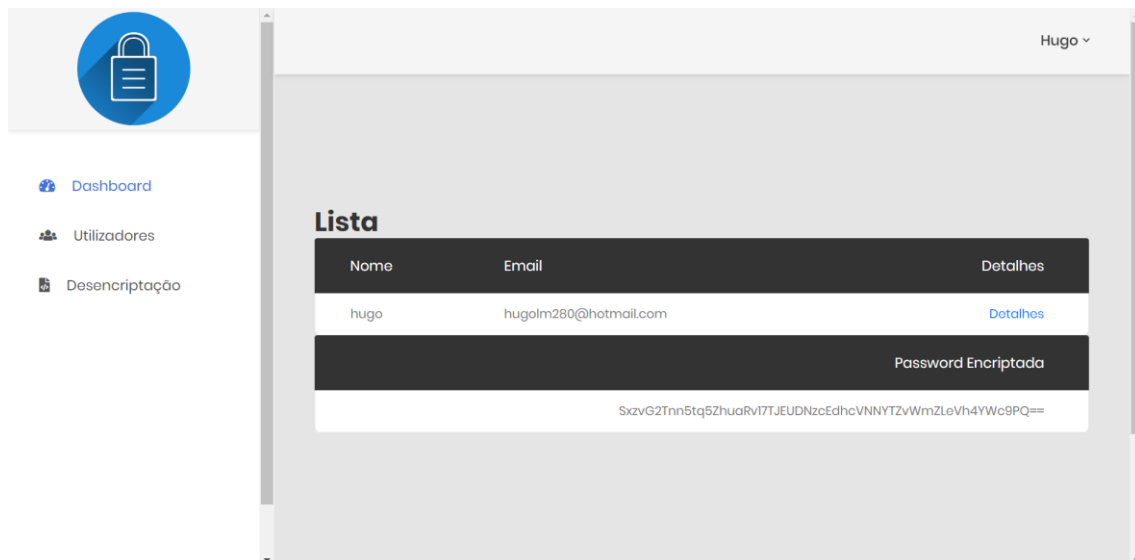


Figura 8 – Página do utilizador

3.2 Página de detalhes do utilizador

Se, por acaso, o utilizador tiver alguma informação errada, poderá clicar no botão detalhes, indo para página onde tem todas as informações da sua conta, onde terá a opção de editar o utilizador.

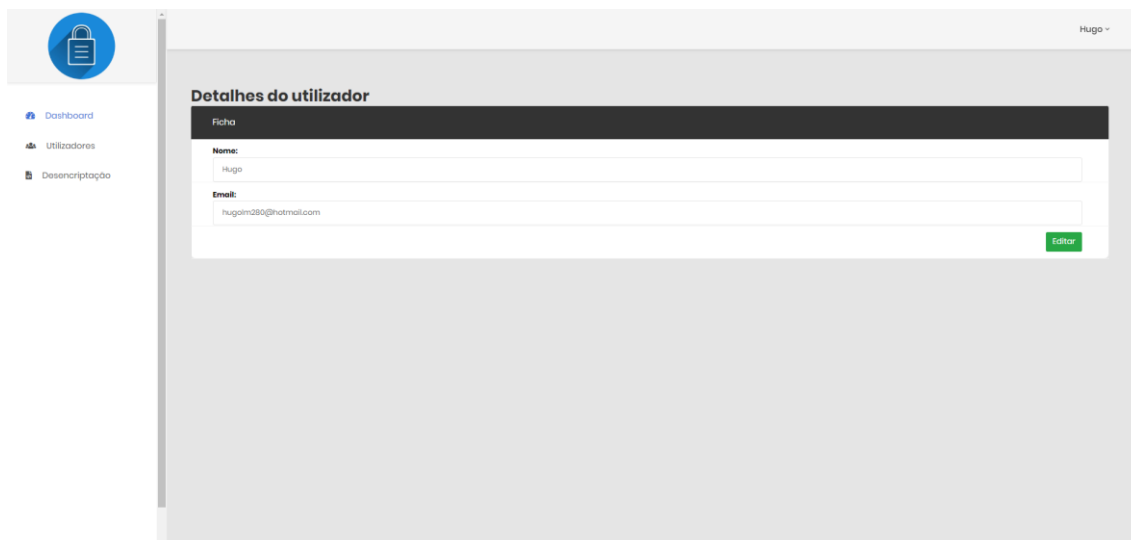


Figura 9 – Página de detalhes do utilizador

3.3. Página de descriptação

Nesta página será possível realizar a descriptação da palavra-passe, que foi previamente encriptada na página de registo quando criamos uma conta.

The screenshot shows a web application interface. On the left is a sidebar with a blue circular icon containing a white padlock. Below the icon are three menu items: 'Dashboard' with a person icon, 'Utilizadores' with a group of people icon, and 'Descriptação' with a document icon. The main content area has a light gray background. At the top right of this area is the name 'Hugo' followed by a downward arrow. The title 'Descriptação' is centered at the top of the main area. Below the title, the text 'Dados para descriptografar:' is followed by a large white rectangular input field. Below this is a smaller white rectangular input field. At the bottom of the main area is a button labeled 'descriptografar'.

Figura 10 - Página de descriptação

4. Método de descriptação

O método de descriptação que utilizei foi o AES-256-CBC, que é um algoritmo de criptografia de chave simétrica que utiliza uma chave de 256 bits para codificar e decodificar dados.

O AES é um algoritmo de criptografia muito seguro, tendo sido desenvolvido pelo Instituto Nacional de padrões e Tecnologia (NIST).

Os 256 bits, como referido em cima, é o tamanho da chave que é utilizada com o algoritmo. Quanto mais pequeno for o tamanho da chave, maior a chance de o atacante vir a descobrir o dado sensível criptografado. Por outro lado, quanto maior for a chave, mais difícil se vai tornar para o atacante descobrir os dados sensíveis introduzidos em qualquer plataforma atingida pelo ataque.

O CBC é um modo de operação de criptografia simétrica que é vastamente utilizada para garantir a confidencialidade e a integridade de todos os dados transmitidos pela internet. Este é um dos métodos mais utilizados e seguros da criptografia, pois é criado um conjunto de blocos de texto, os quais para serem descriptografados dependem da criptografia correta do bloco anterior, de forma a ser descriptografado o texto completo.

O que eu concluo sobre a utilização deste método de encriptação é que é muito utilizado para criptografar dados sensíveis, como por exemplo, transações financeiras e informações pessoais. Este também é suportado por vários tipos de Sistemas e linguagens.

4.1. Resultados

Vou apresentar os resultados da descriptação da palavra-passe introduzida na secção de registo da plataforma, sendo necessário, para a realização do mesmo, a chave de descriptação única que se encontra juntamente com o email que foi enviado para a verificação da conta.

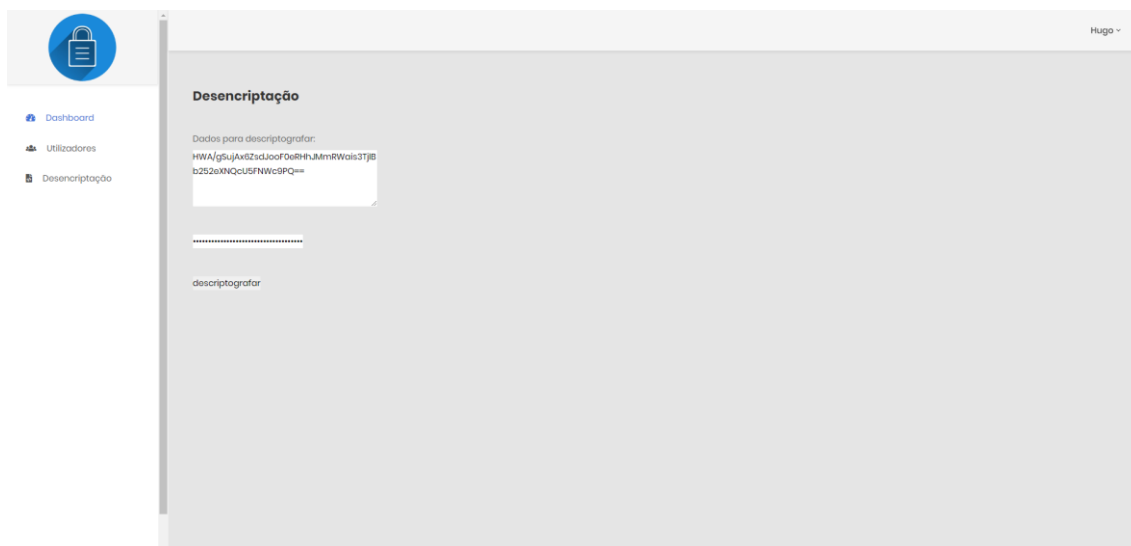


Figura 11 – Descriptação da palavra-passe

Após a descriptação conseguimos observar na figura a seguir que a palavra-passe aparece no seu formato original.

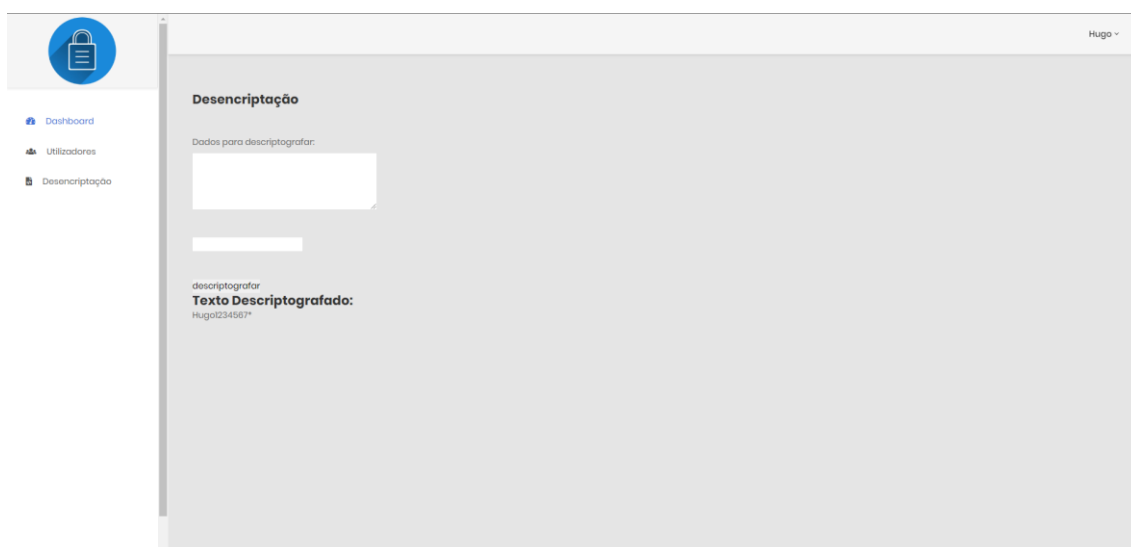


Figura 12 – Palavra-passe descriptografada

5. Conclusão

O objetivo foi desenvolver uma plataforma de encriptação e descriptação de dados e implementar métodos de segurança. A meta foi cumprida e superada.

Após a realização deste projeto, concluo que a criptografia é um bem essencial na proteção dos dados pessoais dos utilizadores de uma determinada plataforma ou aplicação, como as que todos usamos diariamente.

Ademais, de forma a garantir uma maior proteção das contas dos utilizadores, é essencial implementar uma verificação da conta e/ou uma autenticação dois fatores, através de um email, SMS ou aplicação.

6. Referências

Cipher Block Chaining CBC-MAC. (25 de 02 de 2024). Obtido de HatTricks:

<https://book.hacktricks.xyz/v/portugues-ht/crypto-and-stego/cipher-block-chaining-cbc-mac-priv>

Para Você Fazer. (10 de 08 de 2023). Obtido de O que é : Ciphertext Block

Chaining: <https://paravocefazer.com/glossario/o-que-e-ciphertext-block-chaining/>

Programmer, E. (10 de Agosto de 2023). *Secure Text Encryption and Decryption*

using PHP. Obtido de Medium:
<https://medium.com/@everydayprogrammer/secure-text-encryption-and-decryption-using-php-ddc85c116aa2>

What is AES-256-CBC? (09 de Janeiro de 2023). Obtido de Anchor:

<https://docs.anchormydata.com/docs/what-is-aes-256-cbc>