1. Enzo Zanatta

2.Pesquisa

1. O que é o HMAC e qual sua relação com funções hash como SHA-256?

O HMAC (Hash-based Message Authentication Code) é um mecanismo criptográfico usado para garantir a integridade e autenticidade de uma mensagem. Ele combina uma função hash (como SHA-256) com uma chave secreta compartilhada. Enquanto uma função hash simples gera um resumo fixo da mensagem, o HMAC adiciona uma camada de segurança ao incluir uma chave secreta no cálculo.

2. Qual é o papel da chave secreta no processo de geração do HMAC?

A chave secreta autentica a origem da mensagem. Somente quem conhece a chave consegue gerar o mesmo HMAC. Assim, mesmo que um atacante veja o hash, ele não consegue criar outro válido sem conhecer a chave.

3. Quais as diferenças entre integridade, confidencialidade e autenticidade?

Integridade: garante que os dados não foram alterados.
Autenticidade: confirma que a mensagem veio de quem afirma ter enviado.
Confidencialidade: protege o conteúdo contra leitura não autorizada.

4. Cite dois protocolos ou sistemas reais que utilizam HMAC e explique como ele é aplicado.

TLS (HTTPS): usa HMAC para garantir que os pacotes de dados não foram modificados durante a transmissão.
JWT (JSON Web Token): usa HMAC-SHA256 para assinar o token, garantindo que o conteúdo não foi adulterado.

5. Por que o uso de apenas um hash (sem chave) não garante autenticidade?

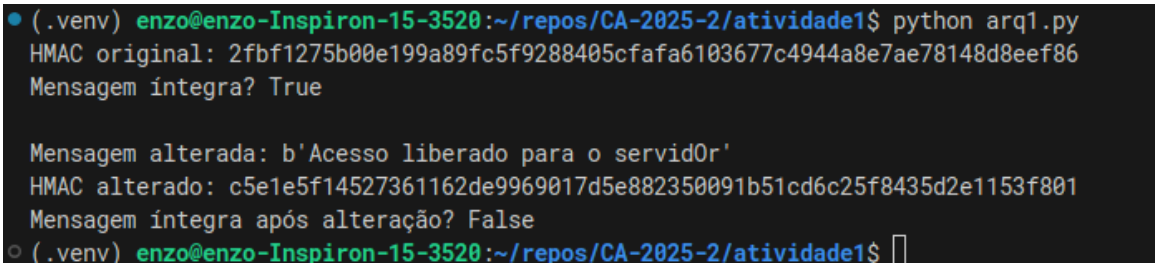
Porque qualquer pessoa pode calcular o hash de uma mensagem. Sem uma chave secreta, o hash só verifica integridade, não autenticidade.

3. Testes práticos

Experimento 1 - Verificação de integridade com HMAC

Neste experimento, geramos o HMAC de uma mensagem e verificamos se ela foi alterada. Uma simples modificação em um caractere faz com que o HMAC mude completamente.

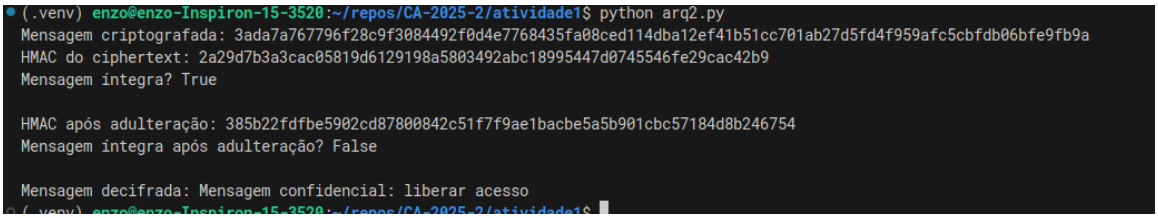
Código-fonte:
Em anexo arq1.py



Experimento 2 - Combinação de Criptografia (AES) e HMAC

Neste experimento, criptografamos a mensagem com AES e aplicamos HMAC sobre o texto cifrado. Isso garante confidencialidade, integridade e autenticidade.

Código-fonte:
Em anexo como arq2.py



4. Análise final

O que o HMAC garante?

Garante integridade e autenticidade das mensagens.

O que ele não garante?

Não garante confidencialidade (o conteúdo ainda pode ser lido).

Como ele pode ser combinado com criptografia?

Usando o padrão Encrypt-then-MAC, onde a mensagem é primeiro criptografada e depois autenticada com HMAC.