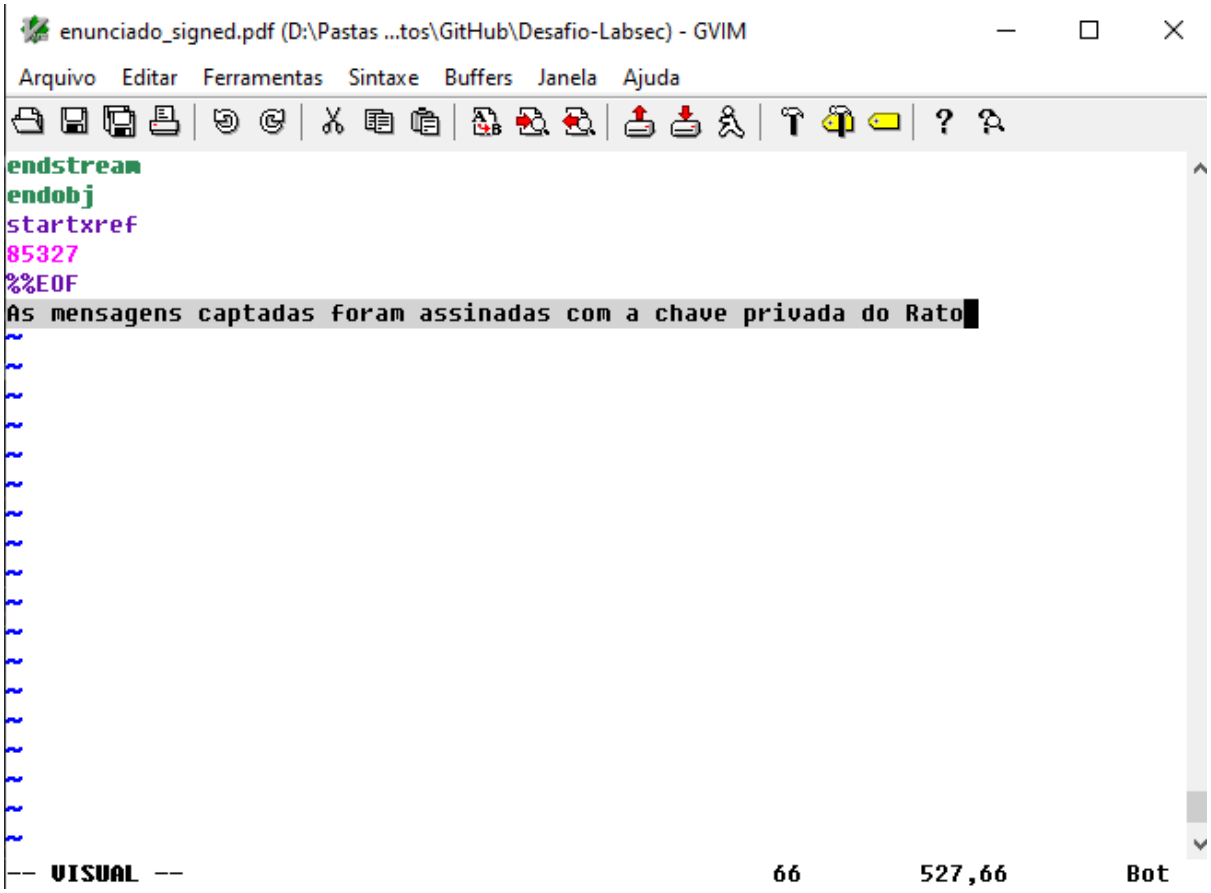
Relatório Pré-Desafio LabSec

Autor: Pedro Henrique Scheidt Prazeres

07/10/2024

1. a dica escondida dentro PDF

Abri o documento com o VIM e encontrei a dica no final no PDF



2. o certificado em formato PEM

Exportei o certificado pelo Acrobat Reader (o que gerou um arquivo no formato .crt), e converti para formato .pem pelo comando do openssl

“openssl x509 -inform DER -in CertExchange.crt -out certificado.pem”

3. a chave pública em formato PEM

Utilizei o comando do openssl

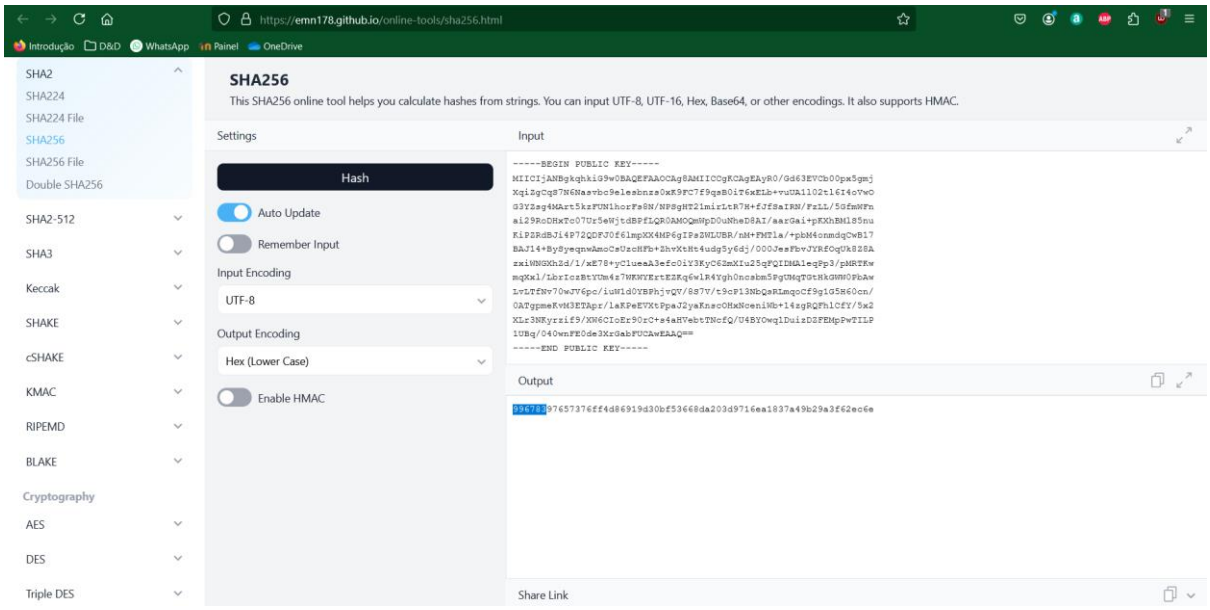
"openssl x509 -in certificado.pem -pubkey -noout"

Para transformar o certificado em uma chave pública .pem

4. o login do usuário

Tendo a chave pública e a dica da questão 1, decodifiquei as mensagens através desta ferramenta.

As mensagens revelaram que o login utilizado é “rato” com os seis primeiros dígitos do hash da chave pública, utilizei este site, que gerou o seguinte hash: “99678397657376ff4d86919d30bf53668da203d9716ea1837a49b29a3f62ec6e”



Portanto, o usuário é “rato996783”

5. a url da conexão

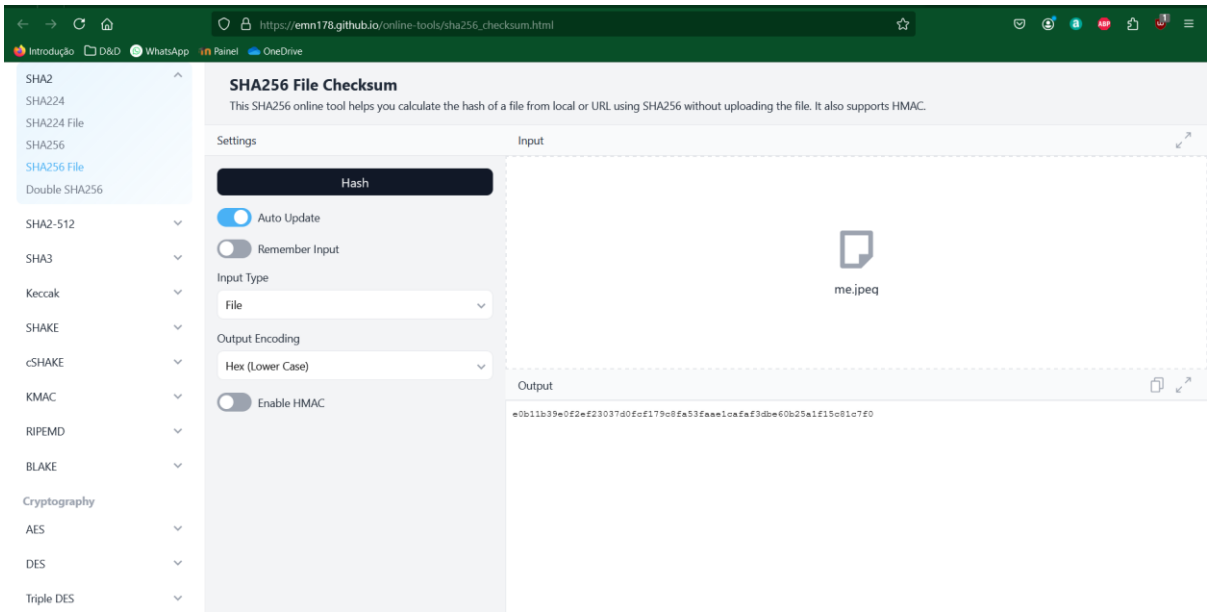
A antepenúltima mensagem ao ser decodificada fornece o link

https://pbad.labsec.ufsc.br/592288ab9d7d0531a4d1d7885063ce2537e47744dfc1839fe3da337ad3a2cbdf/YDyBNZvmtdHZkNkWCubinJJSjlhlMgBlpwRFaohTkukuDHnsjQpTdawvNTApCpbHknuHZxZZmdiRFVYIkFfVjx

OVEJBSUFywaDwYaMiZaTJSZmrKonlSTPldNYvXwGVkcjbwgequTaHrZXVPTaGmLwDCDRZrPUuoCKXtBtCRZWWcmXDhGWmXXceRMIqFFEiwuLZXCxn.xml

6. a senha do usuário

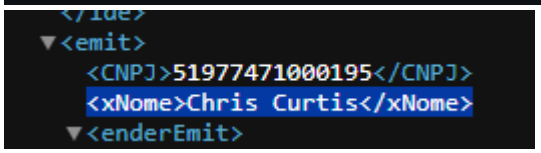
A senha do usuário é o hash da imagem na assinatura. Utilizei este site para pegar esse hash.



7. o nome verdadeiro do Rato

Inicialmente pego colocando o certificado em um decoder de asn1.

Confirmei o nome o vendo também na nota fiscal



8. o nome verdadeiro do Cobra

O nome está na nota fiscal como recebedor.

É possível acessar a nota fiscal juntando as respostas da 4, 5 e 6.