



## Relatório Pré-Desafio LabSec

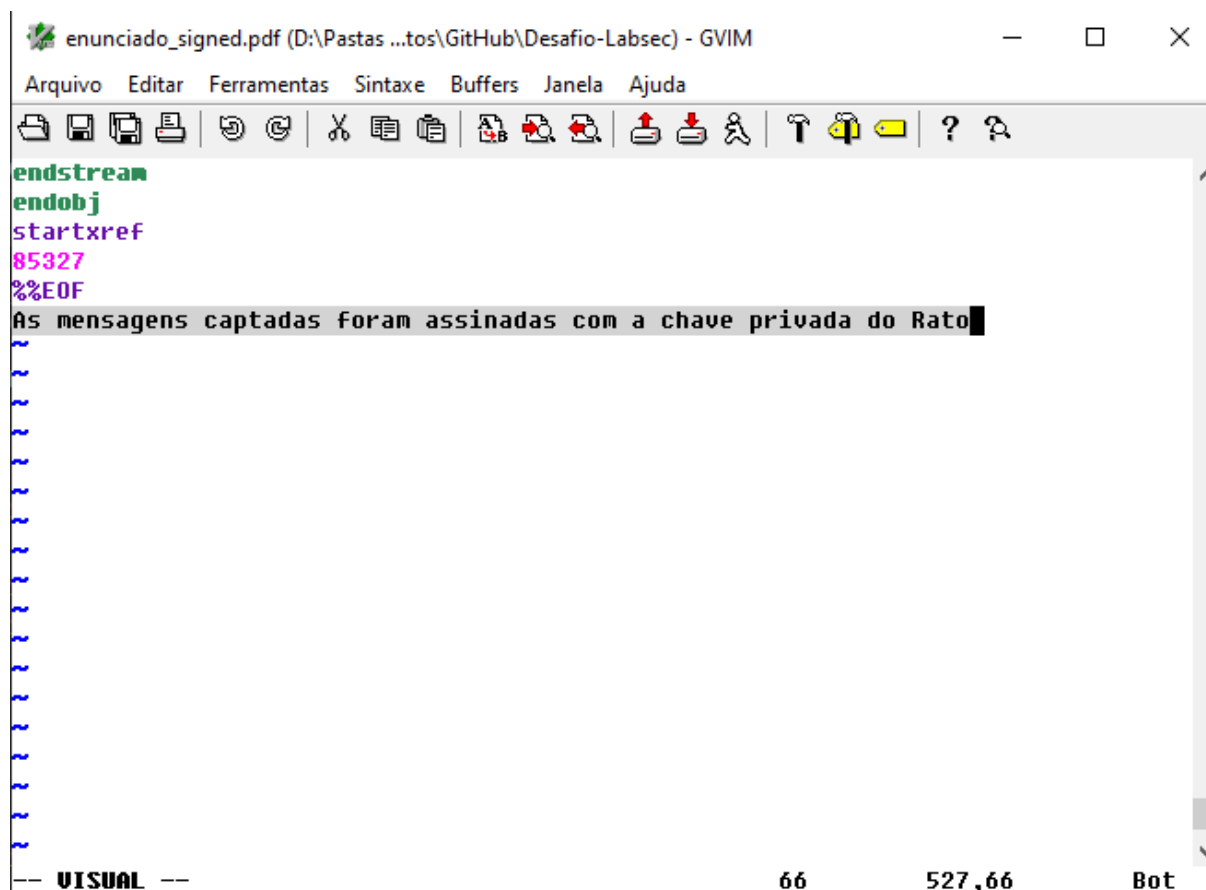
**Autor: Pedro Henrique Scheidt Prazeres**

07/10/2024

- [1. A dica escondida dentro PDF](#)
- [2. O certificado em formato PEM](#)
- [3. A chave pública em formato PEM](#)
- [4. O login do usuário](#)
- [5. A url da conexão](#)
- [6. A senha do usuário](#)
- [7. O nome verdadeiro do Rato](#)
- [8. O nome verdadeiro do Cobra](#)

## 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"
```

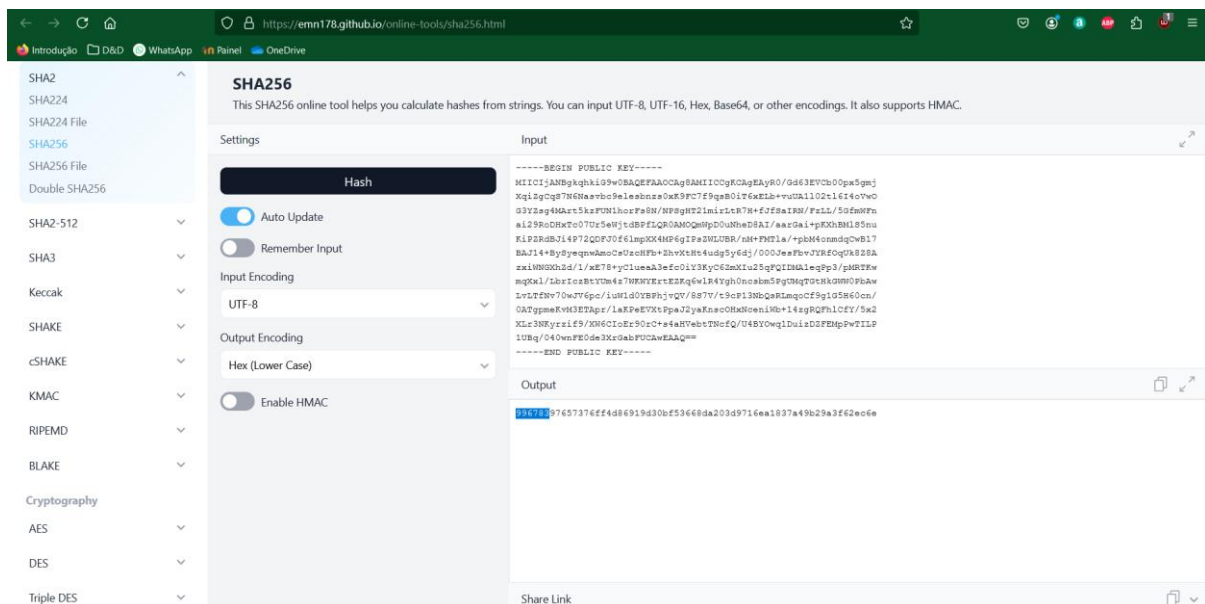
Para transformar o certificado em uma chave pública .pem

## 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

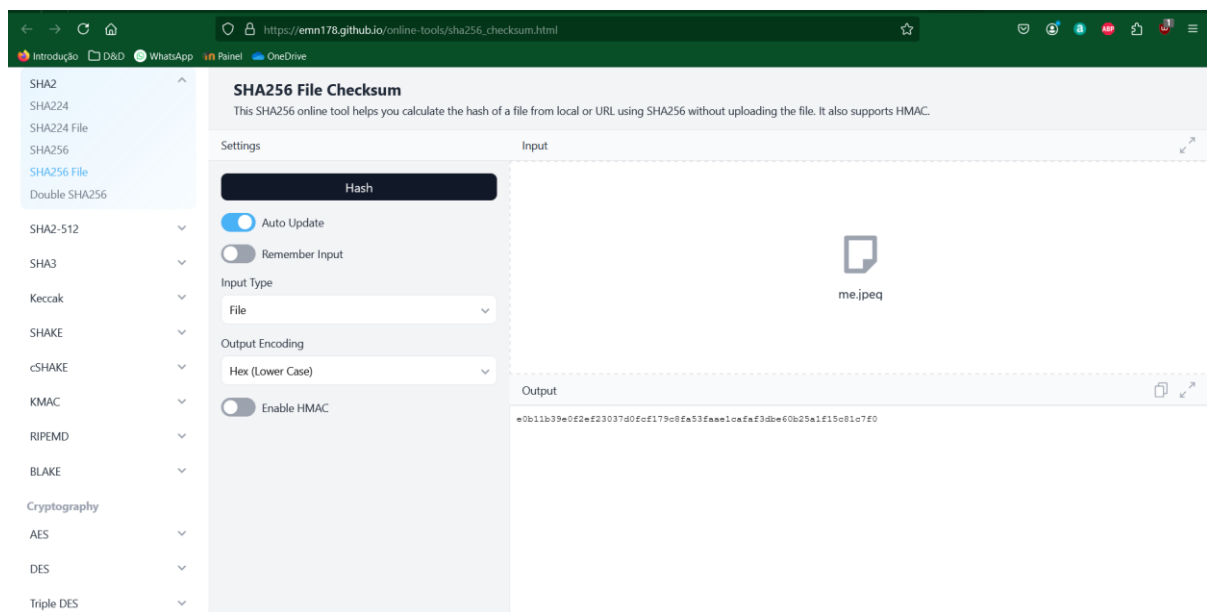
A antepenúltima mensagem ao ser decodificada fornece o link

<https://pbad.labsec.ufsc.br/592288ab9d7d0531a4d1d7885063ce2537e47744dfc1839fe3da337ad3a2cbdf/YDyBNZvmtdHZkNkWCubinJJSjIhIMgBlpwRFaohTkukuDHnsjQpTdawvNTApCpbHknuHZxZZmdiRFVYIkFfVjx>

OVEJBSUFywaDwYaMiZaTJSZmrKonlSTPldNYvXwGVkcjbwgequTaHrZXV  
PTaGmLwDCDRZrPUuoCKXtBtCRZWWcmXDhGWmXXceRMIqFFEiwuLZ  
XCxn.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

```
extensions [3] (1 elem)
├── Extensions SEQUENCE (3 elem)
│   ├── Extension SEQUENCE (2 elem)
│   │   ├── extnID OBJECT IDENTIFIER 1.2.3.4.5.6.7.8.9
│   │   └── extnValue OCTET STRING (57 byte) 0C3768747470733A2F2F706261642E6C616273656332E756673632E62722F6361746368...
│   │       └── UTF8String https://pbad.labsec.ufsc.br/catch-me-if-you-can/me.jpeg
│   ├── Extension SEQUENCE (2 elem)
│   │   ├── extnID OBJECT IDENTIFIER 1.8.9.6.5.4.3.2.1
│   │   └── extnValue OCTET STRING (14 byte) 0C0C436872697320437572746973
│   │       └── UTF8String Chris Curtis
│   └── Extension SEQUENCE (2 elem)
│       ├── extnID OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
│       └── extnValue OCTET STRING (22 byte) 0414C9376D07C307AC3D5E65A672D584606174E21A0F
│           └── OCTET STRING (20 byte) C9376D07C307AC3D5E65A672D584606174E21A0F
├── signatureAlgorithm AlgorithmIdentifier SEQUENCE (2 elem)
│   ├── algorithm OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
│   └── parameters ANY NULL
└── signature BIT STRING (4096 bit) 000101011110111111111111100101110101010000000101011000111001001011100110...
```

```
</ide>
▼<emit>
  <CNPJ>51977471000195</CNPJ>
  <xNome>Chris Curtis</xNome>
▼<enderEmit>
```

## 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](#).

```
</emit>
▼<dest>
  <CPF>74163304916</CPF>
  <xNome>Norma Fisher</xNome>
```