ANTIXEROX

NOVEMBRO 2025 |
ISTEC

SEED LABS

Trabalho de Criptografia
Aplicada a Cibersegurança

ANTIXEROX

ANTIXEROX

PKI

PKI (Public Key Infrastructure) é um sistema que usa chaves e certificados digitais para garantir autenticação, confidencialidade e integridade nas comunicações eletrônicas.

Também permite validar identidades e assegurar transações seguras em redes como a Internet.

ANTIXEROX

PKI

COMPONENTES PRINCIPAIS

- Autoridade Certificadora (CA)
- Autoridade de Registo (RA)
- Certificados Digitais
- Chaves Pública e Privada

FUNÇÕES

- Emissão e gestão de certificados
- Validação e revogação de certificados

- HTTPS
- Assinaturas digitais
- Autenticação de utilizadores

ANTIXEROX

TLS

TLS (Transport Layer Security) é um protocolo de segurança que protege a comunicação entre sistemas na Internet.

Usa criptografia para garantir confidencialidade, integridade e autenticação dos dados transmitidos. Também é a base da navegação segura em sites HTTPS.

ANTIXEROX

PARÂMENTROS

- Tipo
- Tamanho
- Formato
- Codificação
- Passphrase

- Nome
- Cidade
- Validade
- País
- Empresa
- MUITA INFO

ANTIXEROX

REENTRANCY ATTACK

Um ataque de «reentrancy» ocorre quando um contrato chama um contrato externo não confiável, que então reentra no contrato original antes que o seu estado seja atualizado, permitindo a execução repetida que esgota fundos ou corrompe o estado.

withdraw()

getBalance()

deposit()

fallback()

ANTIXEROX

OUTROS LABS FEITOS

ORACLE PADDING ATTACK

Explora as respostas de erro de preenchimento (padding) de um sistema na encriptação CBC para revelar o texto simples sem a chave.

PSEUDO RANDOM NUMBER GENERATION

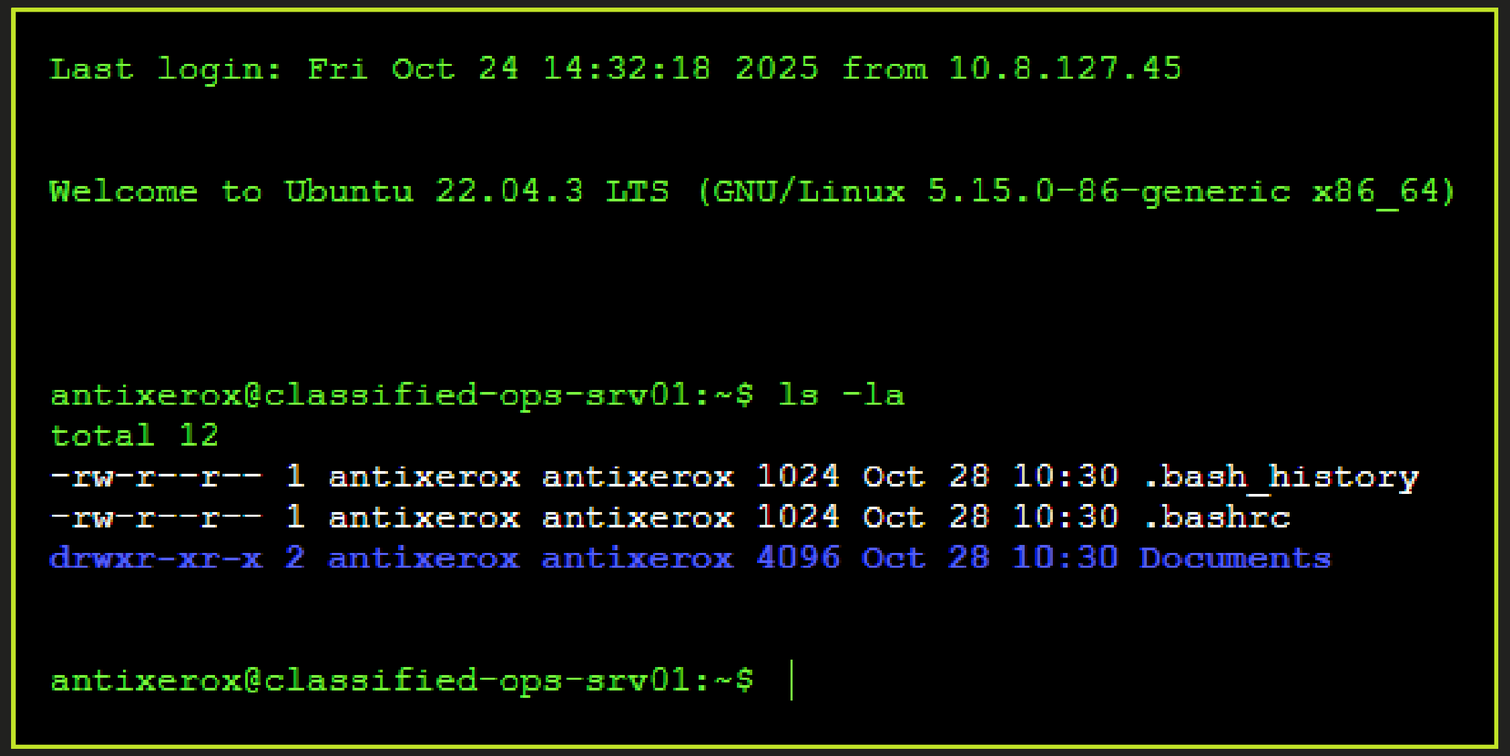
Produz números de forma determinística que parecem aleatórios a partir de uma semente curta; as versões seguras são chamadas de CSPRNGs.

ANTIXEROX

ANTI-ANTIXEROX LAB

A Real Use for Cyberchef!

GPT won't help this time!



Riddle - Hint - Answer

ANTIXEROX

ANTI-ANTIXEROX LAB

ANTIXEROX

NOVEMBRO 2025 |
ISTEC

SEED LABS

Trabalho de Criptografia
Aplicada a Cibersegurança