FACULDADE ADVENTISTA DA BAHIA

PDP – IV

AMILTON PEREIRA DE CARVALHO JUNIOR

DAVI ALBUQUERQUE DE SOUZA PINHO

RELATÓRIO PENTEST'S

CACHOEIRA-BA

2022

AMILTON PEREIRA DE CARVALHO JUNIOR

DAVI ALBUQUERQUE DE SOUZA PINHO

RELATÓRIO PENTEST'S

Projeto Final

Tema: Relatório Pentest's

- Realizar um Pentest's sobre os sites disponibilizados;

- Elaboração e apresentação do relatório.

CACHOEIRA – BA

2022

1. OBJETIVO

Realizar uma análise do site redox escolhido para apontar vulnerabilidades na aplicação web desenvolvida.

2. Informações do Alvo

https://www.redoxengine.com/

Esta instância do nosso Dashboard oferece a mesma funcionalidade da nossa instância de produção. Incentivamos os pesquisadores a criar várias contas (organizações) neste painel.

3. Ferramentas de analise

- Rapidscan
- Hunter.io
- Have i been pwned
- What is MyIPAdress
- dnsdumpster

4. Contato e Declaração de Limite da responsabilidade e confidencialidade do Pentester

- O teste só é autorizado nos alvos listados como Dentro do escopo. Qualquer domínio/propriedade do Redox não listado na seção de destinos está fora do escopo. Isso inclui qualquer/todos os subdomínios não listados acima.

- 0 dias relacionados ao software de outro fornecedor serão aceitos após 30 dias do lançamento de um patch. Se a empresa de origem não tiver uma maneira de você enviar sua descoberta, o Redox pode trabalhar para notificá-la em seu nome.

5. Data de Testes

- ✓ 28/11
- ✓ 29/11
- ✓ 30/11

✓ 01/12

6. Introdução e descrição da Empresa Avaliada

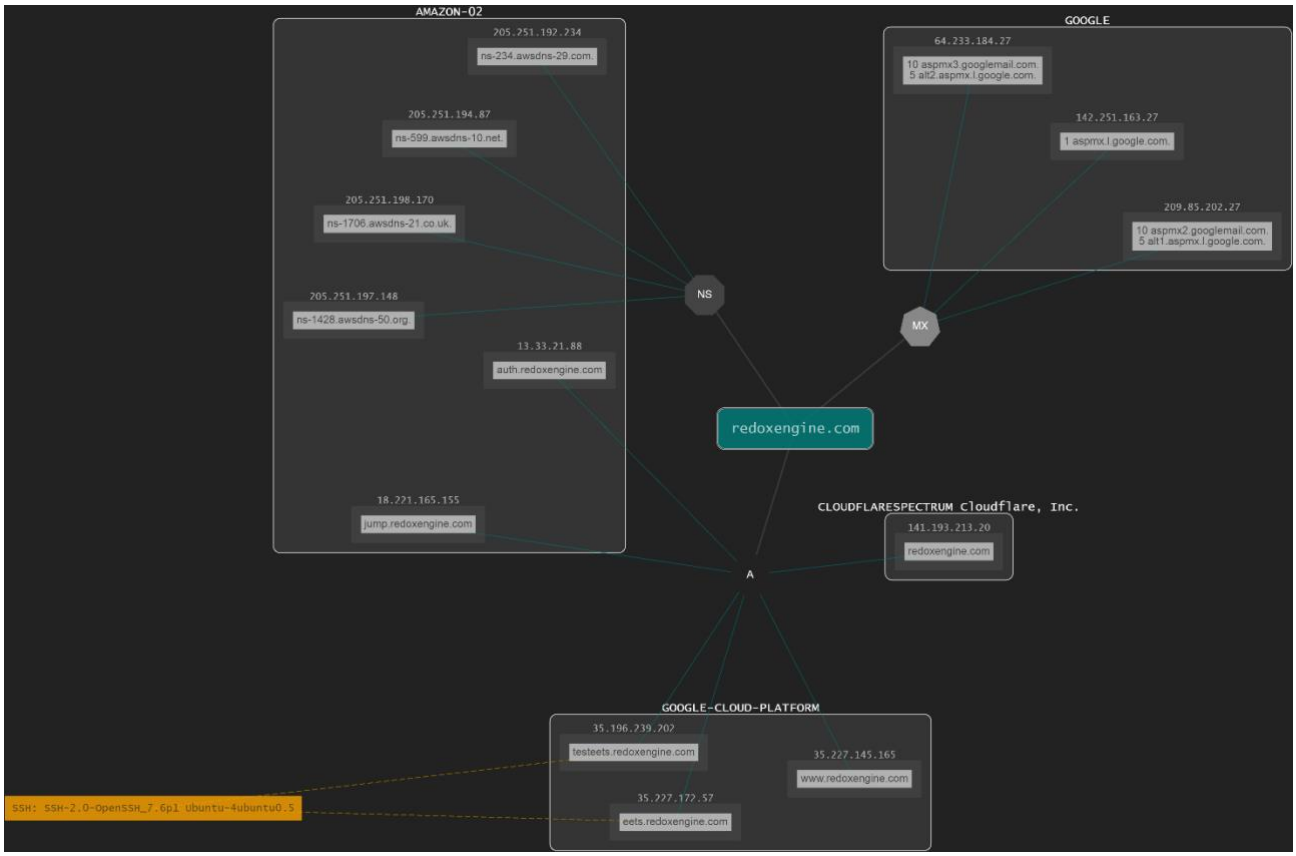
A integração de assistência médica entre aplicativos de software críticos e inovadores prejudica as experiências de assistência médica nos Estados Unidos todos os dias. As estimativas são de que há mais de $ 750 bilhões desperdiçados em saúde a cada ano. Redox pretende se tornar uma das marcas mais confiáveis na área da saúde. Com sua ajuda, vamos superar as diretrizes de regulamentação da indústria HIPAA e atender a todos os pacientes de forma suprema.

A plataforma Redox fornece uma solução altamente escalável que elimina barreiras técnicas. Desde a obtenção de dados HL7 por VPNs até uma infinidade de APIs de fornecedores de EHR (registro eletrônico de saúde) e até mesmo XML por SFTP, precisamos fazer tudo com segurança.

7. Detalhamento dos Dados do Site e subdomínios

redoxengine.com HTTP: cloudflare TCP8080: cloudflare	141.193.213.20	CLOUDFLARESPECTRUM Cloudflare, Inc. Estados Unidos
auth.redoxengine.com	13.33.21.88 server-13-33-21-88.lax53.r.cloudfront.net	AMAZON-02 Estados Unidos
jump.redoxengine.com	18.221.165.155 ec2-18-221-165-155.us-east-2.compute.amazonaws.com	AMAZON-02 Estados Unidos
eets.redoxengine.com SSH:SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5	35.227.172.57 57.172.227.35.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Estados Unidos
testeets.redoxengine.com SSH:SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5	35.196.239.202 202.239.196.35.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Estados Unidos
www.redoxengine.com HTTP: nginx HTTP TECH: nginx	35.227.145.165 165.145.227.35.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Estados Unidos

Mapa de domínio:



8. Detalhamento dos Softwares Instalados

- RapidScan é uma ferramenta gratuita e de código aberto, que se baseia em Open Source Intelligence (OSINT). Esta ferramenta pode ser usada para obter informações sobre nosso alvo (domínio), que pode ser um site ou um endereço IP.
- Hunter.io é uma ferramenta de localização de e-mail mais poderosa. Encontra endereços de e-mail de qualquer nome de empresa ou site em segundo.
- Have i been pwned é uma ferramenta que descobre violações de e-mails.
- What is MyIPAdress é uma ferramenta gratuita para localizar geograficamente a localização do endereço IP.
- DNSDumpster é uma ferramenta de varredura de domínio para encontrar informações relacionadas ao host.

9. Vulnerabilidades de engenharia social

- **Informações da empresa**

- Eastwood Dr.

- Madison, WI 53704

- 608.535.9501

- hello@redoxengine.com

- **Mídia Social**

- Cartão do Twitter incompleto
- Tags Open Graph incompletas
- O URL do Open Graph não corresponde ao canônico
- Tags Open Graph ausentes
- Cartão do Twitter sumido

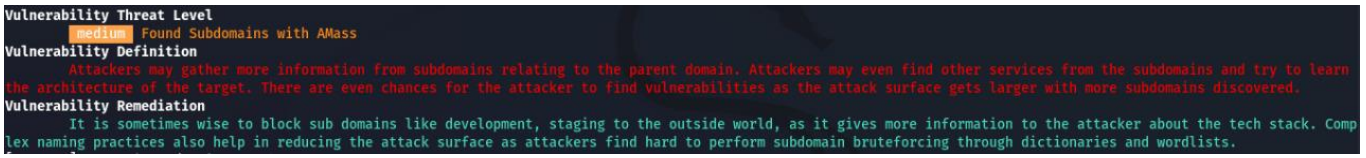
10. Lista de e-mails que já tem a sua senha exposta

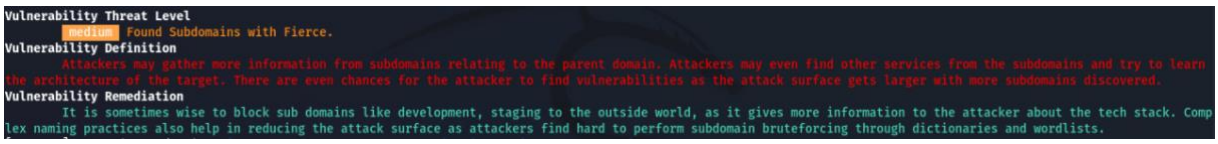
- **Ceo - luke@redoxengine.com**
- **Product Manager - nick@redoxengine.com**
- **Sales Engineering - liza@redoxengine.com**
- **Support - hello@redoxengine.com**

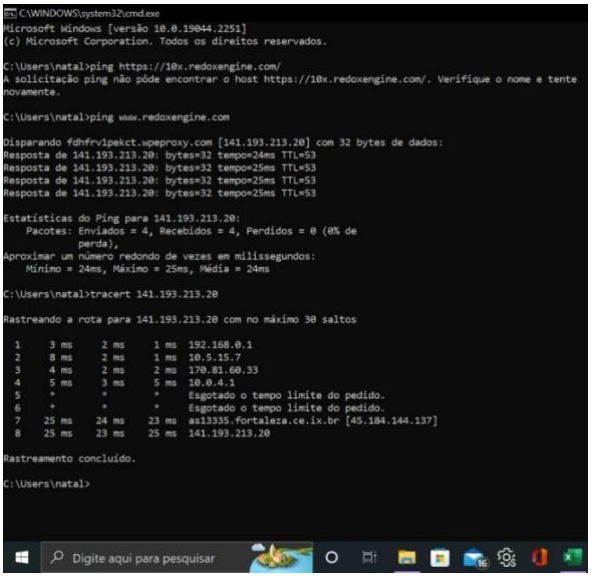
E-mail	Violações	Dados comprometidos
luke@redoxengine.com nick@redoxengine.com liza@redoxengine.com hello@redoxengine.com	Apollo	Endereços de e-mail, empregadores, localizações geográficas, cargos, nomes, números de telefone, saudações, perfis de mídia social
luke@redoxengine.com	Exactis	Informações de status de crédito, datas de nascimento, níveis de educação, endereços de e-mail, etnias, estrutura familiar, investimentos financeiros, sexos, status de propriedade residencial, níveis de renda, endereços IP, estado civil, nomes, patrimônio líquido, ocupações, interesses pessoais, Números de telefone, endereços físicos, religiões, idiomas falados
nick@redoxengine.com luke@redoxengine.com liza@redoxengine.com	Gravatar	Endereços de e-mail, nomes, nomes de usuário

luke@redoxengine.com	Dados extraídos do LinkedIn	Níveis de educação, endereços de e-mail, gêneros, localizações geográficas, cargos, nomes, perfis de mídia social
nick@redoxengine.com luke@redoxengine.com liza@redoxengine.com	Exposição de enriquecimento de dados do cliente PDL	Endereços de e-mail, empregadores, localizações geográficas, cargos, nomes, números de telefone, perfis de mídia social
nick@redoxengine.com	EatStreet	Datas de nascimento, endereços de e-mail, sexos, nomes, dados parciais de cartão de crédito, senhas, números de telefone, endereços físicos, perfis de mídia social
liza@redoxengine.com	Adapt	Endereços de e-mail, empregadores, cargos, nomes, números de telefone, endereços físicos, perfis de mídia social

11. Prints de Relatórios scans







12. Alerta de vulnerabilidade dos indicadores que demonstram preocupação por grau de severidade.

Nível	Vulnerabilidade	Definição	Solução
Médio	Subdomínios encontrados com AMass	Os invasores podem coletar mais informações de subdomínios relacionados ao domínio pai. Os invasores podem até encontrar outros serviços dos subdomínios e tentar aprender a arquitetura do alvo. Há ainda chances de o invasor encontrar vulnerabilidades à medida que a superfície de ataque aumenta com a descoberta de mais subdomínios.	Às vezes, é aconselhável bloquear subdomínios como desenvolvimento, preparando para o mundo externo, pois fornece mais informações ao invasor sobre a pilha de tecnologia. As práticas de nomenclatura complexa também ajudam a reduzir a superfície de ataque, pois os invasores acham difícil executar força bruta de subdomínio por meio de dicionários e listas de palavras.
Baixa	Algumas portas estão abertas.	As portas abertas dão aos invasores uma dica para explorar os serviços. Os invasores tentam	É recomendável fechar as portas de serviços não utilizados e usar um firewall para filtrar as portas sempre

	Execute uma varredura completa manualmente.	recuperar as informações do banner pelas portas e entender que tipo de serviço o host está em execução.	que necessário. Este recurso pode fornecer mais insights.
Médio	A renegociação iniciada pelo cliente seguro é suportada.	Também denominado ataque de injeção de texto sem formatação, que permite que invasores MiTM insiram dados em sessões HTTPS e possivelmente outros tipos de sessões protegidas por V TLS ou SSL, enviando uma solicitação não autenticada que é processada retroativamente por um servidor em uma postagem - contexto de renegociação.	Etapas detalhadas de correção podem ser encontradas nesses recursos. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
Médio	Subdomínios encontrados com Fierce.	Os invasores podem coletar mais informações de subdomínios relacionados ao domínio pai. Os invasores podem até encontrar outros serviços dos subdomínios e tentar aprender a arquitetura do alvo. Há chances de eventos para o invasor encontrar vulnerabilidades à medida que a superfície de ataque aumenta com mais subdomínios descobertos.	Às vezes, é aconselhável bloquear subdomínios como desenvolvimento, preparando para o mundo externo, pois fornece mais informações ao invasor sobre a pilha de tecnologia. As práticas de nomenclatura complexa também ajudam a reduzir a superfície de ataque, pois os invasores acham difícil executar força bruta de subdomínio por meio de dicionários e listas de palavras.

13. Quadro SWOT da segurança do site (FORÇAS, FRAQUEZAS, OPORTUNIDADES E AMEACAS)

FORÇAS:	**FRAQUEZAS:**
• **ATENDIMENTO AO CLIENTE** **Tem como valor ajudar organizações e equipes da saúde pública a ter acesso a dados para se capacitar totalmente suas iniciativas.**	• **SUBDOMINIOS DESPROTEGIGOS** • **DADOS PESSOAIS VULNERAVEIS** • **POUCA AVALIAÇÃO**

OPORTUNIDADES:	AMEAÇAS:
• **Campanha de marketing:** **Precisa melhorar a visibilidade e expandir mundialmente.**	• **Novo concorrente** **Através da tecnologia e inovação as empresas tentam buscar os melhores serviços e se manter em alta.**