# Relatório de Reconhecimento - ReconX

## Alvo: www.sophinfinity.com.br

Data da Análise: 2025-07-14

## Análise da IA (Gemini)

## Análise Técnica do Relatório de Pentest

Este relatório apresenta os resultados de um pentest básico realizado na infraestrutura da `sophinfinity.com.br` utilizando as ferramentas Nmap, WhatWeb e Amass. A análise a seguir detalha as descobertas e suas implicações de segurança.

**1. Sumário Executivo:**

O pentest identificou que o website está hospedado na Netlify e utiliza um servidor Golang para servir conteúdo. A porta 80 redireciona para a porta 443, implementando HTTPS. A configuração parece segura, com HSTS habilitado. A principal preocupação reside na identificação de versões dos serviços, que o Nmap não conseguiu determinar precisamente, e na necessidade de investigar a segurança da plataforma Netlify e do código Go. A presença de um endereço de e-mail no código fonte (identificado pelo WhatWeb) também pode ser um vetor de ataque de engenharia social.

**2. Nmap - Mapeamento de Portas e Serviços:**

* **Alvo:** `www.sophinfinity.com.br` (IP: `54.232.119.62`)
* **Resultados:**
  * Porta 80/tcp: Aberta, identificada como servidor HTTP Golang `net/http server`.
  * Porta 443/tcp: Aberta, identificada como `ssl/https Netlify`.
  * 998 portas TCP filtradas (sem resposta).
* **Análise:**
  * A presença das portas 80 e 443 abertas indica que o servidor web está acessível via HTTP e HTTPS.
  * O uso de HTTPS (porta 443) é crucial para proteger a comunicação entre o cliente e o servidor.
  * A identificação do servidor HTTP como "Golang net/http server" sugere que o backend da aplicação é desenvolvido em Go.
  * A identificação da porta 443 como Netlify indica que a aplicação está hospedada nesta plataforma de serviços web.
  * A alta quantidade de portas filtradas pode indicar a presença de um firewall protegendo a infraestrutura. Contudo, a ausência de portas fechadas impede uma identificação mais precisa do sistema operacional.
* **Vulnerabilidades Potenciais:**
  * **Vulnerabilidades no Servidor Golang:** É crucial manter o servidor Go atualizado com as últimas versões para mitigar vulnerabilidades conhecidas.
  * **Configuração Incorreta do Servidor Web:** Uma configuração inadequada do servidor web pode levar a ataques de injeção de código, cross-site scripting (XSS) ou divulgação de informações sensíveis.
  * **Vulnerabilidades na Plataforma Netlify:** A segurança depende da robustez da plataforma Netlify. É importante verificar se a plataforma está atualizada e se os procedimentos de segurança estão sendo seguidos.
  * **Falta de Detecção de Versão:** A dificuldade do Nmap em identificar a versão precisa dos serviços dificulta a pesquisa por vulnerabilidades específicas. A submissão das *fingerprints* para o Nmap (como sugerido no relatório) é recomendada para melhorar a precisão em futuros escaneamentos.

* **Recomendações:**
  * Realizar uma análise de vulnerabilidades específica do servidor Golang `net/http server`.
  * Verificar a configuração de segurança do servidor web.
  * Analisar a configuração e as políticas de segurança implementadas na plataforma Netlify.
  * Submeter as *fingerprints* geradas pelo Nmap para auxiliar na identificação de versões de serviços.
  * Investigar a possibilidade de realizar um escaneamento com mais intensidade para tentar identificar portas fechadas e obter uma identificação mais precisa do sistema operacional.

**3. WhatWeb - Identificação de Tecnologias e Informações:**

* **Resultados:**
  * Redirecionamento HTTP para HTTPS (301 Moved Permanently).
  * Servidor web: Netlify.
  * Localização (País): Estados Unidos (US).
  * HSTS (Strict-Transport-Security) habilitado (`max-age=31536000`).
  * Encontrado um endereço de e-mail: `lucasmourateixeirasrx@gmail.com`.
* **Análise:**
  * O redirecionamento HTTP para HTTPS garante que todas as comunicações sejam criptografadas, protegendo contra ataques *man-in-the-middle*.
  * A presença de HSTS indica que o navegador será instruído a sempre usar HTTPS para acessar o site, mesmo que o usuário digite "http://".
  * A descoberta do endereço de e-mail `lucasmourateixeirasrx@gmail.com` no código-fonte representa um potencial risco de engenharia social. Atacantes podem usar esse endereço para phishing ou outras tentativas de ataque direcionadas.
* **Vulnerabilidades Potenciais:**
  * **Engenharia Social:** O endereço de e-mail exposto pode ser usado para ataques de phishing e outras formas de engenharia social.
* **Recomendações:**
  * Remover o endereço de e-mail do código-fonte do website.
  * Implementar medidas de conscientização sobre segurança para os funcionários, alertando sobre os riscos de ataques de phishing e engenharia social.

**4. Amass - Enumeração de Subdomínios e Informações de DNS:**

* **Resultados:**
  * Informações sobre os servidores de nomes (NS records) do domínio `sophinfinity.com.br`.
  * Endereço IP associado ao domínio e ao subdomínio `www.sophinfinity.com.br`.
  * Informações sobre os blocos de IP e ASNs (Autonomous System Numbers) relacionados.
* **Análise:**
  * O Amass forneceu informações valiosas sobre a infraestrutura de DNS do domínio.
  * A identificação dos servidores de nomes e seus respectivos endereços IP pode ser útil para análises forenses ou para entender a arquitetura da rede.
  * As informações sobre os blocos de IP e ASNs podem ser usadas para identificar outros ativos pertencentes à organização.
* **Vulnerabilidades Potenciais:**
  * **Ataques a DNS:** Informações detalhadas sobre a infraestrutura de DNS podem ser usadas para realizar ataques de DNS spoofing ou negação de serviço (DoS) direcionados aos servidores de nomes.
  * **Exposição de Informações:** Embora as informações coletadas pelo Amass sejam públicas, elas podem fornecer aos atacantes uma visão mais clara da infraestrutura da organização, facilitando a identificação de alvos e a

elaboração de ataques.
* **Recomendações:**
  * Monitorar os servidores de nomes para detectar atividades suspeitas ou ataques em andamento.
  * Revisar as configurações de DNS para garantir que estejam protegidas contra ataques de spoofing e DoS.
  * Considerar a implementação de medidas de segurança adicionais para proteger a infraestrutura de DNS, como DNSSEC (DNS Security Extensions).

**5. Conclusões e Recomendações Gerais:**

O pentest básico identificou a utilização de Netlify e um servidor Go. As principais recomendações para melhorar a postura de segurança são:

* **Fortalecer a Segurança do Servidor Go:** Realizar testes de segurança mais aprofundados no código Go e na configuração do servidor.
* **Monitorar a Segurança da Netlify:** Manter-se atualizado sobre as políticas de segurança da Netlify e garantir que a plataforma esteja configurada corretamente.
* **Remover Informações Sensíveis:** Remover o endereço de e-mail do código-fonte do website para mitigar o risco de engenharia social.
* **Conscientização sobre Segurança:** Realizar treinamentos regulares de conscientização sobre segurança para os funcionários, abordando os riscos de phishing e engenharia social.
* **Monitoramento de DNS:** Monitorar a infraestrutura de DNS para detectar atividades suspeitas e proteger contra ataques direcionados.
* **Realizar Pentests Regulares:** Realizar pentests regulares e mais abrangentes para identificar e corrigir vulnerabilidades em tempo hábil.

**6. Próximos Passos:**

* Realizar um teste de vulnerabilidade automatizado (ex: Nessus, OpenVAS) para identificar vulnerabilidades conhecidas nos serviços web e na plataforma Netlify.
* Conduzir um teste de penetração manual para explorar as vulnerabilidades identificadas e avaliar o impacto potencial.
* Revisar as configurações de segurança da Netlify e do servidor web para garantir que estejam de acordo com as melhores práticas.
* Implementar um programa de gerenciamento de vulnerabilidades para rastrear e corrigir vulnerabilidades em tempo hábil.
* Considerar a implementação de um sistema de detecção de intrusão (IDS) para monitorar o tráfego de rede e detectar atividades suspeitas.

Esta análise fornece uma visão geral da postura de segurança da `sophinfinity.com.br` com base nos resultados do pentest. A implementação das recomendações apresentadas ajudará a fortalecer a segurança da infraestrutura e a proteger contra ameaças cibernéticas.

## Resultados do Módulo: NMAP

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-14 01:28 CDT
Nmap scan report for www.sophinfinity.com.br (54.232.119.62)
Host is up (0.15s latency).
rDNS record for 54.232.119.62: ec2-54-232-119-62.sa-east-1.compute.amazonaws.com

# Relatório de Reconhecimento - ReconX

Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Golang net/http server
443/tcp open  ssl/https Netlify
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=7/14%Time=6874A412%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,92,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x2014\x2
SF:0Jul\x202025\x2006:30:42\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Request-I
SF:d:\x2001K03T1TC4CGAZSSERN06PC85M\r\nContent-Length:\x200\r\n\r\n")%r(HT
SF:TPOptions,92,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x2014
SF:\x20Jul\x202025\x2006:30:43\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Reques
SF:t-Id:\x2001K03T1VGQQNQYBV734VHJXZT7\r\nContent-Length:\x200\r\n\r\n")%r
SF:(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x2
SF:0text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad
SF:\x20Request")%r(FourOhFourRequest,92,"HTTP/1\.0\x20400\x20Bad\x20Reques
SF:t\r\nDate:\x20Mon,\x2014\x20Jul\x202025\x2006:30:45\x20GMT\r\nServer:\x
SF:20Netlify\r\nX-Nf-Request-Id:\x2001K03T1WRECTKP2JMD3WRZ3NF2\r\nContent-
SF:Length:\x200\r\n\r\n")%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x
SF:20close\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConne
SF:ction:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP
SF:/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20chars
SF:et=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(LPDSt
SF:ring,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/pl
SF:ain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Requ
SF:est")%r(SIPOptions,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\
SF:x20Bad\x20Request")%r(Socks5,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Content-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r
SF:\n\r\n400\x20Bad\x20Request")%r(OfficeScan,A3,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request:\x20missing\x20required\x20Host\x20header\r\nContent-Type:\x
SF:20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Ba
SF:d\x20Request:\x20missing\x20required\x20Host\x20header");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=7/14%Time=6874A418%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,92,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x
SF:2014\x20Jul\x202025\x2006:30:48\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Re
SF:quest-Id:\x2001K03T1ZNRWKM0A17SWM7A0KPR\r\nContent-Length:\x200\r\n\r\n
SF:")%r(HTTPOptions,92,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon
SF:,\x2014\x20Jul\x202025\x2006:30:48\x20GMT\r\nServer:\x20Netlify\r\nX-Nf
SF:-Request-Id:\x2001K03T1ZY5PBE32PHB6DRAYGCK\r\nContent-Length:\x200\r\n\
SF:r\n")%r(FourOhFourRequest,92,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDat
SF:e:\x20Mon,\x2014\x20Jul\x202025\x2006:30:49\x20GMT\r\nServer:\x20Netlif
SF:y\r\nX-Nf-Request-Id:\x2001K03T218MRMPY6X6JBPAZDVT8\r\nContent-Length:\
SF:x200\r\n\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

# Relatório de Reconhecimento - ReconX

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.97 seconds

## Resultados do Módulo: WhatWeb

[1m [34mhttp://www.sophinfinity.com.br [0m [301 Moved Permanently] [1mCountry [0m[ [0m [22mUNITED STATES [0m][ [1m [31mUS [0m], [1mHTTPServer [0m[ [1m [36mNetlify [0m], [1mIP [0m[ [0m [22m54.232.119.62 [0m], [1mRedirectLocation [0m[ [0m [22mhttps://www.sophinfinity.com.br/ [0m], [1mUncommonHeaders [0m[ [0m [22mx-nf-request-id [0m]
[1m [34mhttps://www.sophinfinity.com.br/ [0m [301 Moved Permanently] [1mCountry [0m[ [0m [22mUNITED STATES [0m][ [1m [31mUS [0m], [1mHTTPServer [0m[ [1m [36mNetlify [0m], [1mIP [0m[ [0m [22m54.232.119.62 [0m], [1mRedirectLocation [0m[ [0m [22mhttps://sophinfinity.com.br/ [0m], [1mStrict-Transport-Security [0m[ [0m [22mmax-age=31536000 [0m], [1mUncommonHeaders [0m[ [0m [22mx-nf-request-id [0m]
[1m [34mhttps://sophinfinity.com.br/ [0m [200 OK] [1mCountry [0m[ [0m [22mUNITED STATES [0m][ [1m [31mUS [0m], [1mEmail [0m[ [0m [22mlucasmourateixeirasrx@gmail.com [0m], [1mHTTPServer [0m[ [1m [36mNetlify [0m], [1mIP [0m[ [0m [22m54.232.119.62 [0m], [1mScript [0m, [1mStrict-Transport-Security [0m[ [0m [22mmax-age=31536000 [0m], [1mTitle [0m[ [1m [33mSophinfinitY [0m], [1mUncommonHeaders [0m[ [0m [22mcache-status,x-nf-request-id [0m]

## Resultados do Módulo: AMASS

sophinfinity.com.br (FQDN) --> ns_record --> dns3.p08.nsone.net (FQDN)
sophinfinity.com.br (FQDN) --> ns_record --> dns4.p08.nsone.net (FQDN)
sophinfinity.com.br (FQDN) --> ns_record --> dns2.p08.nsone.net (FQDN)
sophinfinity.com.br (FQDN) --> ns_record --> dns1.p08.nsone.net (FQDN)
sophinfinity.com.br (FQDN) --> a_record --> 54.232.119.62 (IPAddress)
sophinfinity.com.br (FQDN) --> node --> www.sophinfinity.com.br (FQDN)
dns3.p08.nsone.net (FQDN) --> a_record --> 198.51.44.72 (IPAddress)
dns3.p08.nsone.net (FQDN) --> aaaa_record --> 2620:4d:4000:6259:7:8:0:3 (IPAddress)
dns4.p08.nsone.net (FQDN) --> a_record --> 198.51.45.72 (IPAddress)
dns4.p08.nsone.net (FQDN) --> aaaa_record --> 2a00:edc0:6259:7:8::4 (IPAddress)
dns2.p08.nsone.net (FQDN) --> a_record --> 198.51.45.8 (IPAddress)
dns2.p08.nsone.net (FQDN) --> aaaa_record --> 2a00:edc0:6259:7:8::2 (IPAddress)
dns1.p08.nsone.net (FQDN) --> a_record --> 198.51.44.8 (IPAddress)
dns1.p08.nsone.net (FQDN) --> aaaa_record --> 2620:4d:4000:6259:7:8:0:1 (IPAddress)
www.sophinfinity.com.br (FQDN) --> a_record --> 54.232.119.62 (IPAddress)
54.232.0.0/15 (Netblock) --> contains --> 54.232.119.62 (IPAddress)
198.51.44.0/23 (Netblock) --> contains --> 198.51.45.8 (IPAddress)
198.51.44.0/23 (Netblock) --> contains --> 198.51.44.8 (IPAddress)
198.51.44.0/23 (Netblock) --> contains --> 198.51.45.72 (IPAddress)
198.51.44.0/23 (Netblock) --> contains --> 198.51.44.72 (IPAddress)
2a00:edc0:6259::/48 (Netblock) --> contains --> 2a00:edc0:6259:7:8::2 (IPAddress)
2a00:edc0:6259::/48 (Netblock) --> contains --> 2a00:edc0:6259:7:8::4 (IPAddress)

# Relatório de Reconhecimento - ReconX

2620:4d:4000::/48 (Netblock) --> contains --> 2620:4d:4000:6259:7:8:0:1 (IPAddress)
2620:4d:4000::/48 (Netblock) --> contains --> 2620:4d:4000:6259:7:8:0:3 (IPAddress)
16509 (ASN) --> managed_by --> AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) --> announces --> 54.232.0.0/15 (Netblock)
62597 (ASN) --> managed_by --> NSONE (RIROrganization)
62597 (ASN) --> announces --> 198.51.44.0/23 (Netblock)
62597 (ASN) --> announces --> 2a00:edc0:6259::/48 (Netblock)
62597 (ASN) --> announces --> 2620:4d:4000::/48 (Netblock)