Relatório de Reconhecimento - ReconX

Alvo: sophinfinity.com.br

Data da Análise: 2025-07-14

Análise da IA (Gemini)

Análise Técnica do Relatório de Pentest - sophinfinity.com.br

Este relatório apresenta uma análise técnica das informações coletadas por meio de ferramentas de pentest, incluindo Nmap, WhatWeb e Amass, direcionadas ao domínio sophinfinity.com.br. O objetivo é identificar possíveis vulnerabilidades e áreas de atenção para a segurança do sistema.

1. Sumário Executivo:

O relatório revela que o domínio sophinfinity.com.br está hospedado na plataforma Netlify e utiliza a infraestrutura da Amazon (AWS). A análise das portas abertas (80 e 443) indica a presença de um servidor web Golang. A falta de identificação precisa dos serviços rodando nessas portas e a dificuldade na detecção do sistema operacional podem indicar medidas de segurança para ofuscação ou configurações incomuns. A exposição de um endereço de e-mail no conteúdo da página HTTPS é uma preocupação de privacidade e potencial vetor de ataque para engenharia social.

2. Análise Detalhada das Ferramentas:

2.1 Nmap:

* **Alvos:** sophinfinity.com.br (54.232.119.62)
* **Portas Abertas:**
  * 80/tcp: HTTP - Servidor Golang net/http
  * 443/tcp: HTTPS - Servidor Golang net/http

* **Problemas Identificados:**
  * **Fingerprinting Incompleto:** O Nmap não conseguiu identificar a versão específica dos serviços nas portas 80 e 443. Isso dificulta a identificação de vulnerabilidades conhecidas para essas versões. A ferramenta sugere submeter os fingerprints para análise, o que pode ajudar a refinar as detecções futuras.
  * **Dificuldade na Detecção do Sistema Operacional:** A mensagem "OSScan results may be unreliable" indica que o Nmap não conseguiu determinar o sistema operacional com precisão devido à falta de uma porta TCP fechada para análise. Isso pode dificultar a identificação de vulnerabilidades específicas do sistema operacional. A configuração do firewall pode estar dificultando a identificação de portas fechadas.
  * **Respostas HTTP 400 (Bad Request):** As respostas HTTP 400 para diversas requisições (GET, OPTIONS, etc.) podem indicar:
    * **Configuração do servidor web:** Pode ser uma configuração intencional para rejeitar requisições não padronizadas ou malformadas como uma medida de segurança.
    * **Problemas de configuração:** Pode haver um problema na configuração do Netlify ou do servidor Golang que está gerando essas respostas inesperadas.

* **Implicações de Segurança:**
  * A falta de informações precisas sobre os serviços e o sistema operacional aumenta a dificuldade de identificar e explorar vulnerabilidades.

* A presença de um servidor Golang requer atenção, pois vulnerabilidades podem ser específicas para implementações em Golang.

2.2 WhatWeb:

* **Informações Coletadas:**
  * Redirecionamento de HTTP para HTTPS (301 Moved Permanently).
  * Hospedagem: Netlify.
  * Localização Geográfica: Estados Unidos (US).
  * Email exposto: `lucasmourateixeirasrx@gmail.com`.
  * Strict-Transport-Security (HSTS) ativado com `max-age=31536000`.

* **Problemas Identificados:**
  * **Exposição de Endereço de E-mail:** A presença do endereço de e-mail `lucasmourateixeirasrx@gmail.com` no conteúdo da página HTTPS é uma preocupação de privacidade e pode ser explorada para ataques de engenharia social (phishing, spam, etc.).

* **Implicações de Segurança:**
  * A exposição de informações pessoais (como o endereço de e-mail) aumenta o risco de ataques direcionados.

2.3 Amass:

* **Informações Coletadas:**
  * Mapeamento de DNS: Registros A, AAAA e NS para o domínio e subdomínio `www.sophinfinity.com.br`.
    * Servidores de Nomes (NS): `dns1.p08.nsone.net`, `dns2.p08.nsone.net`, `dns3.p08.nsone.net`, `dns4.p08.nsone.net`.
  * Blocos de IP e ASNs (Autonomous System Numbers) associados ao domínio e seus servidores de nomes.

* **Problemas Identificados:**
  * Nenhum problema de segurança específico foi identificado diretamente pela análise do Amass. No entanto, o mapeamento detalhado da infraestrutura é valioso para entender a superfície de ataque e identificar possíveis alvos para testes mais aprofundados.

* **Implicações de Segurança:**
  * As informações coletadas pelo Amass fornecem uma visão completa da infraestrutura DNS, permitindo que atacantes identifiquem possíveis pontos de entrada e vetores de ataque.

3. Recomendações:

* **Investigar as respostas HTTP 400:** Analise a configuração do Netlify e do servidor Golang para entender por que as requisições estão sendo rejeitadas. Corrija quaisquer problemas de configuração que possam estar causando essas respostas.
* **Refinar o Fingerprinting do Nmap:** Submeta os fingerprints dos serviços nas portas 80 e 443 para o Nmap para melhorar a precisão da detecção futura.
* **Fortalecer a Detecção do Sistema Operacional:** Revise a configuração do firewall para garantir que o Nmap possa acessar pelo menos uma porta TCP fechada, permitindo uma detecção mais precisa do sistema operacional.
* **Remover o Endereço de E-mail:** Remova o endereço de e-mail `lucasmourateixeirasrx@gmail.com` do conteúdo da página HTTPS para proteger a privacidade do proprietário e reduzir o risco de ataques de engenharia social.
* **Monitoramento Contínuo:** Implemente um sistema de monitoramento contínuo para detectar mudanças na

configuração do servidor, novas vulnerabilidades e atividades suspeitas.
* **Testes de Penetração Adicionais:** Realize testes de penetração mais aprofundados para identificar e explorar vulnerabilidades nos serviços web e na infraestrutura subjacente. Isso deve incluir testes de segurança da aplicação (OWASP Top 10) e testes de configuração de segurança do servidor web.
* **Análise de Logs:** Implemente uma solução centralizada de coleta e análise de logs para monitorar a atividade do servidor web e identificar padrões de ataque.

4. Conclusão:

O relatório de pentest inicial identificou alguns pontos de atenção para a segurança do domínio sophinfinity.com.br. As recomendações apresentadas devem ser implementadas para fortalecer a postura de segurança e proteger o sistema contra possíveis ataques. É crucial realizar testes de penetração mais aprofundados e implementar um sistema de monitoramento contínuo para garantir a segurança a longo prazo. A exposição de informações sensíveis como o email deve ser imediatamente corrigida.

Resultados do Módulo: NMAP

Starting Nmap 7.95 (https://nmap.org) at 2025-07-14 01:45 CDT
Nmap scan report for sophinfinity.com.br (54.232.119.62)
Host is up (0.057s latency).
rDNS record for 54.232.119.62: ec2-54-232-119-62.sa-east-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (time-exceeded)
PORT STATE SERVICE VERSION
80/tcp open http Golang net/http server
443/tcp open ssl/http Golang net/http server
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=6874A79B%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\x2006:45:47\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Request-I
SF:d:\x2001K03TXDRXZ0X1NW97RX84YX3F\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\x2006:45:47\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Reques
SF:t-Id:\x2001K03TXDY6R370M5WN3SDHWEES\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\x2006:45:52\x20GMT\r\nServer:\x
SF:20Netlify\r\nX-Nf-Request-Id:\x2001K03TXK4T2Z6S6SZBC66632AE\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=6874A7A5%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,92,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nDate:\x20Mon,\x
SF:2014\x20Jul\x202025\x2006:45:57\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Re
SF:quest-Id:\x2001K03TXQ49YXZZ48B0K4R8GGB5\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\x2006:45:57\x20GMT\r\nServer:\x20Netlify\r\nX-Nf
SF:-Request-Id:\x2001K03TXQCMJSKREHXWFB8RQGMG\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\x2006:45:58\x20GMT\r\nServer:\x20Netlif
SF:y\r\nX-Nf-Request-Id:\x2001K03TXRM9N11224HGTWME2T3W\r\nContent-Length:\
SF:x200\r\n\r\n")%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\
SF:nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\
SF:r\n\r\n400\x20Bad\x20Request")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnec
SF:tion:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r
SF:\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSessionReq,6
SF:7,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x
SF:20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%
SF:r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(SIPOptions,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCon
SF:tent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\
SF:r\n400\x20Bad\x20Request")%r(Socks5,67,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20
SF:close\r\n\r\n400\x20Bad\x20Request")%r(OfficeScan,A3,"HTTP/1\.1\x20400\
SF:x20Bad\x20Request:\x20missing\x20required\x20Host\x20header\r\nContent-
SF:Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n40
SF:0\x20Bad\x20Request:\x20missing\x20required\x20Host\x20header");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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 97.86 seconds
```

Resultados do Módulo: WhatWeb

Relatório de Reconhecimento - ReconX

[1m [34mhttp://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],
[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)
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)