

FACULDADE ADVENTISTA DA BAHIA

Jefer Habib
Marcel Molinari

Relatório de segurança

Cachoeira, Bahia
2022

Escopo:

A confiança e a segurança do comerciante são nossa prioridade.

O programa de recompensas de bugs da Shopify é nossa forma de recompensar os pesquisadores de segurança por encontrarem vulnerabilidades de segurança graves na In Scope.

O escopo do programa de recompensas por bugs é limitado aos domínios listados

Completo em: <https://hackerone.com/shopify?type=team>

O que é a Shopify :

A Shopify é uma empresa de comércio canadense com sede em Ottawa, Ontário, que desenvolve softwares de computadores para lojas online e sistemas de varejo de ponto de venda.

Ela foi fundada em 2004 e era inicialmente baseada em um software anterior desenvolvido por seus fundadores para a sua loja online de snowboard. Supostamente, a empresa tem 150 mil comerciantes utilizando a plataforma, com volume total de mercadoria bruta superior a 8 bilhões de dólares.

Data de Iteração: 28/11 – 30/11/2022

Informações da empresa:

Shopify Inc.

Perfil de Tecnologia Perfil Detalhado de Tecnologia Metaperfil Relação redirecionar Recom

Informações da empresa Shopify Inc.

Melhor domínio shopify.com Este é o domínio de classificação mais alta da Shopify Inc. com base no tráfego/classificação da página.	Endereços
Pegada global 49 Shopify Inc. tem conexões relacionadas em 49 países.	Ottawa ON, K2P Canadá 
Gastos com tecnologia da Web US\$ 89.124 /ano A Shopify Inc. tem US\$ 89.124 em gastos atuais detectáveis com tecnologia da Web por ano.	San Francisco CA, 94105 Estados Unidos 
Redução de gastos A Shopify Inc. diminuiu seus gastos detectáveis com tecnologia nos últimos 12 meses.	Dublin 4 , D04 Irlanda 
Consolidação de tecnologia A Shopify Inc. diminuiu a quantidade de tecnologias em uso nos últimos 12 meses.	Ottawa (Cidade Central) ON, K2P Canadá 
Contatos listados 37 Contatos listados no total em páginas públicas.	Ottawa (Parliament Hill) Ontário, K1P Canadá 
	Telefones
	Reino Unido - +44-800-8085233 
	Estados Unidos - +1-613-241-2828 +1-416-238-6705 
	Estados Unidos - Ligação +1-855-816-3857 

Detalhamento de softwares:

Análise e rastreamento:

Análise e Rastreamento	Detectado pela primeira vez	Detectado pela última vez	
 SpeedCurve Desempenho do aplicativo	julho de 2019	novembro de 2022	\$
 datadog Desempenho do aplicativo	maio de 2022	novembro de 2022	\$
 CrazyEgg Otimização de sites	janeiro de 2008	novembro de 2022	\$
 Google Analytics Desempenho do aplicativo · Medição do público · Rastreamento da contagem de visitantes	outubro de 2006	novembro de 2022	
 Acompanhamento de conversões do Google Otimização de conversão · Rastreamento de conversão	janeiro de 2011	novembro de 2022	
 Google Universal Analytics	outubro de 2013	novembro de 2022	
 Insights de domínio do Facebook Gestão Social	agosto de 2014	novembro de 2022	

Estruturas:

Estruturas			
 Token Ruby on Rails	Set 2014	novembro de 2022	
 Esquema Corporativo Esquema	outubro de 2020	novembro de 2022	
 Esquema da Organização Esquema	janeiro de 2017	novembro de 2022	
 Adobe Enterprise Cloud	julho de 2021	novembro de 2022	\$
 Verificação de domínio do Facebook	outubro de 2018	novembro de 2022	
 Verificação de Domínio GlobalSign	abril de 2019	novembro de 2022	
 OpenRestyName	agosto de 2019	novembro de 2022	
 Inseto Recompensa	maio de 2021	novembro de 2022	\$
 Funções do Google Cloud	junho de 2022	novembro de 2022	
 perl	julho de 2022	novembro de 2022	
 Expressar	Set 2022	outubro de 2022	
 PHP	novembro de 2021	dezembro de 2021	🔒
 Ruby on Rails	janeiro de 2011	novembro de 2021	🔒
 Shockwave Flash Incorporado	janeiro de 2011	fevereiro de 2021	🔒
Rede de entrega de conteúdo			
 CloudFront	outubro de 2011	novembro de 2022	
 Cloudflare	maio de 2020	novembro de 2022	
 Amazon S3	Set 2008	novembro de 2022	
 API de bibliotecas AJAX	janeiro de 2010	novembro de 2022	
 CDN de imagem do Yahoo	maio de 2020	junho de 2022	

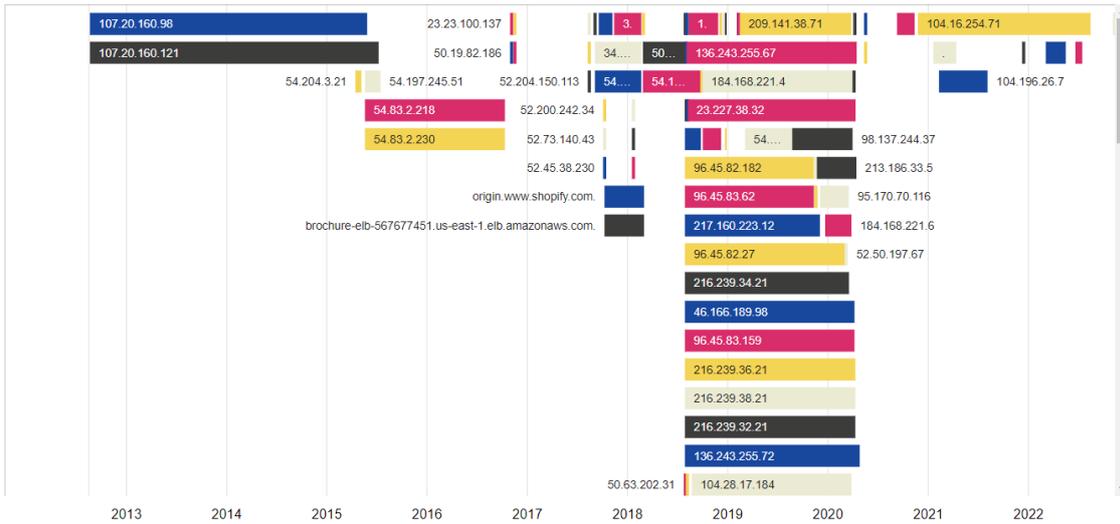
SSL e nome do servidor:

Certificados SSL			
 LetsEncrypt Autoridade Raiz	março de 2019	novembro de 2022	
 Cloudflare SSL	maio de 2020	novembro de 2022	
 HSTS IncludeSubdomains PreLoad	outubro de 2022	novembro de 2022	
 HSTS	outubro de 2022	novembro de 2022	
 SSL por padrão	Set 2015	novembro de 2022	
 DigiCert SSL Autoridade Raiz	Set 2014	novembro de 2022	
 GeoTrust SSL Autoridade Raiz	julho de 2013	novembro de 2020	🔒
 Heroku SSL	abril de 2016	junho de 2019	🔒
 DigiCert EV Validação Estendida	Set 2014	janeiro de 2015	🔒 \$
Nome do servidor			
 DNSsimpler	outubro de 2016	novembro de 2022	\$
 NSONE DNS empresarial	março de 2020	novembro de 2022	\$
 Redirecionamento de domínio da Irlanda	Set 2022	novembro de 2022	\$
 Redirecionamentos de 30 a 49 ccTLDs Redirecionamentos TLD	Set 2022	novembro de 2022	\$
 Redirecionamentos de 15 a 19 ccTLDs Redirecionamentos TLD	outubro de 2020	Set 2022	\$

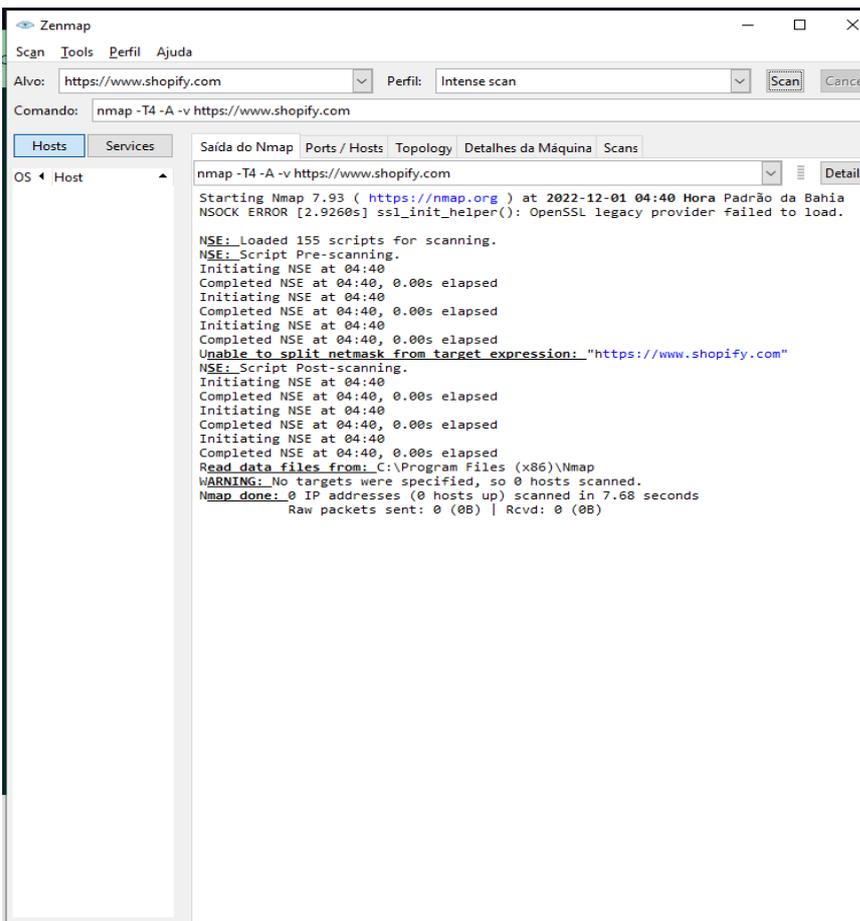
Hospedeiros e subdomínios:

```
root@kali: /home/gordo/shop
Arquivo  Ações  Editar  Exibir  Ajuda
(root@kali)~/home/gordo/shop
# cat shopify.com.txt
experiments.shopify.com
hardware-new.shopify.com
videomaker.shopify.com
events.shopify.com
secops01.ec2.shopify.com
console1.toronto.shopify.com
vpnify.tableau.data.shopify.com
burst.shopify.com
s1.shopify.com
gussieduponline.shopify.com
tim-exclusive.shopify.com
log2.ash.shopify.com
smtp4.shopify.com
origin.www.shopify.com
market.shopify.com
north.shopify.com
fund.shopify.com
summit2018.shopify.com
irl.shopify.com
unicorn.shopify.com
mta4.email.shopify.com
torontoretailtour.shopify.com
api.collabs.shopify.com
pointofsale.shopify.com
```

Historico de relações de IPs:



Saída ZENMAP:



Historico de e-mail e dados vazados:

O processo foi aberto no Tribunal Distrital de Delaware dos Estados Unidos na sexta-feira e alega que a Shopify “falha repetidamente e profundamente em proteger as identidades de seus clientes”.

A Shopify está sendo responsabilizada pelos reclamantes por vazar informações de identificação pessoal (PII) de compradores da Ledger, apesar das promessas de marketing que garantem a segurança total da plataforma. As vítimas do golpe de phishing, John Chu e Edward Baton , entraram com o processo na Califórnia contra o provedor de carteira criptográfica e seu parceiro de comércio eletrônico Shopify. Os demandantes afirmam que a Shopify e o TaskUs estavam cientes da violação de dados por mais de uma semana antes de notificar os clientes. Eles estão pedindo que o tipo exato de informação vazada seja divulgado pela Ledger e Shopify e por uma recompensa monetária que cubra danos reais e punitivos

Vulnerabilidade de engenharia social:

Estabelecimentos perto: Ottawa, ON K2P

Elgin street Dinner

Canadian museum os nature

The green door restaurant

Solução:

Treinamento e curso sobre os perigos do método engenharia social conscientizando e deixando os empregados alerta, o risco de funcionários usarem crachás em bares ou restaurantes é muito frequente Recomenda-se uma política de segurança para que crachás ou Informações de qualquer tipo que possam prejudicar a empresa.

Possível vulnerabilidade ip:

O ip testado não possui nenhuma vulnerabilidade avançada ou Moderado, mas potencialmente vulnerável a ataques Dos e DDoS (negação de acesso). serviço) vulnerabilidades de baixo nível. Em um ataque DDoS (Distributed Denial of Service), o invasor faz sua Segmente o tráfego indesejado da Internet para que o tráfego normal não chegue ao seu destino de propósito.

Solução:

O roteamento Blackhole é uma estratégia para reduzir o impacto de ataques DDoS. Isso inclui redirecionar solicitações para endereços IP inválidos. Essa medida torna o IP de destino dos pacotes maliciosos indisponível. Nesse caso, não há distinção entre solicitações de acesso legítimas e maliciosas. Sobre segurança de e-mail corporativo: Use senhas fortes não coloque dados pessoais em senhas use caracteres aleatórios para senhas misture números e caracteres especiais.

Vulnerabilidade de e-mail:

Solução:

- Ter senhas fortes
- Não colocar dados pessoais nas senhas
- Utilizar caracteres randômicos para sua senha
- Misture números e caracteres especiais
- Atualizar sempre o antivírus
- Configurar todos os e-mails da empresa com segurança de dois fatores

Softwares usados:

ZenMA

Nma

FindoMain

Builtwith