

shopify.com

Recopilación de información

1. Introducción

Vamos a hacer una recopilación de información usando como objetivo el servidor shopify.com

El objetivo se ha elegido de la página hackerone y el scope permitido es *.shopify.com, respetándose el mismo en todo momento.

El proceso se ha dividido en cuatro etapas:

1. Footprinting
2. Fingerprinting
3. Análisis de vulnerabilidades
4. OSINT y redes sociales (esta se ha limitado a LinkedIn)

Para el reconocimiento se han utilizado tanto herramientas de línea de comandos, web y escritorio.

Junto al informe, en el repositorio de Github, están los archivos dónde se han almacenado los resultados. En la carpeta "shopify.com".

2. Resultados obtenidos

Footprinting	
Se han obtenido 137 subdominios verificados	

Fingerprinting	
Escaneo de puertos abiertos	80, 8080, 443, 8443
Tecnologías encontradas	Stimulus, Ruby on Rails, Ruby, Google Tag Manager, PHP, Site Kit: 1.118.0, WordPress, MySQL, React, AngularJS, Jquery 1.9.1, Bootstrap 2.3.1
URLs con login	https://inbox.shopify.com/ https://partnership.shopify.com/ https://admin.shopify.com/ https://collabs.shopify.com/
WAF	Cloudflare (Cloudflare Inc.)
Google Analytics	https://au.checkout.hardware.shopify.com/ UA-82702-52

Análisis de vulnerabilidades		
vulnerabilidad	Descripción	Gravedad
CVE-2013-0169	Permite el cifrado TLS 1.0 y 1.1 haciéndolo vulnerable un ataque LUCKY13	Baja

OSINT	
Google Drive	Carpeta pública con fotografías de empleados y directivos, incluido el CEO. De esa carpeta se ha extraído el correo de 3 empleados verificados en LinkedIn. Cada foto va nombrada con el nombre completo y puesto
Mails validados	samantha.tam@shopify.com jackie.warren@shopify.com kristina.caracciolo@shopify.com scott.francis@shopify.com
Linkedin	https://www.linkedin.com/in/tobiaslutke/ https://www.linkedin.com/in/samantha-tam-08181278/ https://www.linkedin.com/in/jackiewarren/ https://www.linkedin.com/in/kristina-caracciolo-7bb840b6/ https://www.linkedin.com/in/scott-francis-57ab79/
Foca	La siguiente URL (https://cnd.shopify.com/) permite descargar documentación de proveedores o clientes.

3. Footprinting

DNS Brute-force

shuffledns

Validación de servidores DNS con dnsvalidator

```
dnsvalidator -tL https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt -threads 100 -o $HOME/recopilacion/lists/resolvers.txt
```

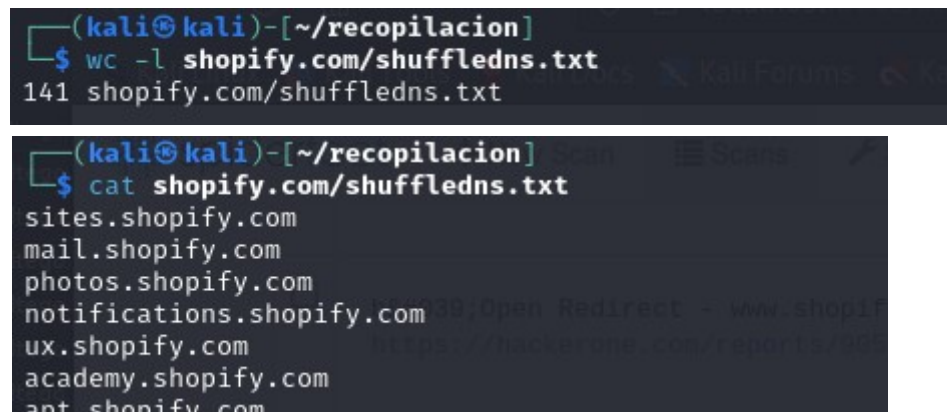
Obtención del wordlist

<https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/namelist.txt>

Ejecutamos shuffledns

```
shuffledns -d shopify.com -w $HOME/recopilacion/lists/wordlist.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > $HOME/recopilacion/shopify.com/shuffledns.txt
```

Resultado: Obtenemos 141 subdominios



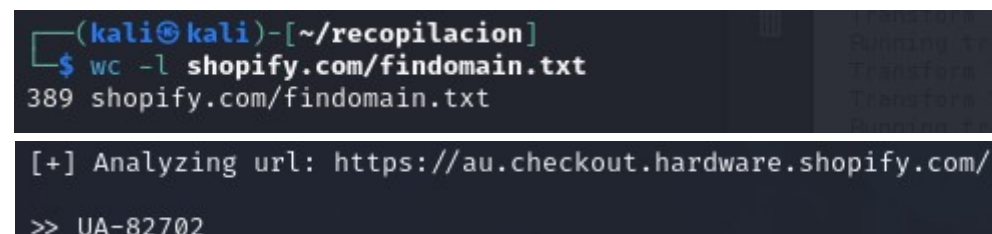
```
(kali@kali)-[~/recopilacion]
$ wc -l shopify.com/shuffledns.txt
141 shopify.com/shuffledns.txt

(kali@kali)-[~/recopilacion]
$ cat shopify.com/shuffledns.txt
sites.shopify.com
mail.shopify.com
photos.shopify.com
notifications.shopify.com
ux.shopify.com
academy.shopify.com
ant.shopify.com
```

Google Analytics

Comprobamos con **analyticsrelationships** si el objetivo utiliza este servicio. Probamos en dos URLs:

- shopify.com
- <https://au.checkout.hardware.shopify.com/>



```
(kali@kali)-[~/recopilacion]
$ wc -l shopify.com/findomain.txt
389 shopify.com/findomain.txt

[+] Analyzing url: https://au.checkout.hardware.shopify.com/
>> UA-82702
```

Reconocimiento de dominios

findomain

Ejecutamos la herramienta findomain

```
findomain -t shopify.com > recopilacion/shopify.com/findomain.txt
```

Resultados: 389 subdominios

```
(kali@kali)-[~/recopilacion]
$ wc -l shopify.com/findomain.txt
389 shopify.com/findomain.txt

(kali@kali)-[~/recopilacion]
$ cat shopify.com/findomain.txt
amazon-ads.shopify.com
summit2018.shopify.com
o.ssl.shopify.com
pointofsale.shopify.com
```

assetfinder

Ejecución de assetfinder

```
assetfinder -subs-only shopify.com | unfurl -u domains > shopify.com/assetfinder.txt
```

Resultados: 427 subdominios

```
(kali@kali)-[~/recopilacion]
$ wc -l shopify.com/assetfinder.txt
427 shopify.com/assetfinder.txt

(kali@kali)-[~/recopilacion]
$ cat shopify.com/assetfinder.txt
ab978c-2.myshopify.com
burst.shopify.com
cdn.shopify.com
www.shopify.com
academy.shopify.com
acceleration.shopify.com
```

TLS Probing

cero

Buscamos posible subdominios en los certificados SSL/TLS del dominio

Ejecutamos la herramienta **cero**

```
cero -d shopify.com | grep shopify.com$ | unfurl -u domains > shopify.com/cero.txt
```

Resultados: 1

```
(kali@kali)-[~/recopilacion]
$ wc -l shopify.com/cero.txt
1 shopify.com/cero.txt
```

Web Scrapping

katana

Vamos a recorrer la web (shopify.com) para obtener las URLs y extraer dominios únicos

```
echo shopify.com | katana -silent -jc -o shopify.com/katana.txt -kf robots,sitemapxml
```

```
cat shopify.com/katana.txt | unfurl -u domains > shopify.com/katana.txt
```

Resultados: 2

```
(kali@kali)-[~/recopilacion]
$ wc -l shopify.com/katana.txt
2 shopify.com/katana.txt
```

```
(kali@kali)-[~/recopilacion]
$ cat shopify.com/katana.txt
www.shopify.com
shopify.com
```

Certificate Transparency Logs

ctfr

Buscamos subdominios en los logs asociados a un certificado

```
ctfr -d shopify.com | unfurl -u domains > shopify.com/ctfr.txt
```

```
# Limpiamos
```

```
# Habría que quitar los dominios con *
```

```
cat shopify.com/ctfr.txt | grep shopify.com$ | unfurl -u domains > ctfr.txt
```

Resultados: 56

```
(kali@kali)-[~/recopilacion/shopify.com]
$ wc -l ctfr.txt
56 ctfr.txt
```

```
(kali@kali)-[~/recopilacion/shopify.com]
$ cat ctfr.txt
cs.shopify.com
cs.staging.shopify.com
data.shopify.com
rb.shopify.com
shopify.com
```

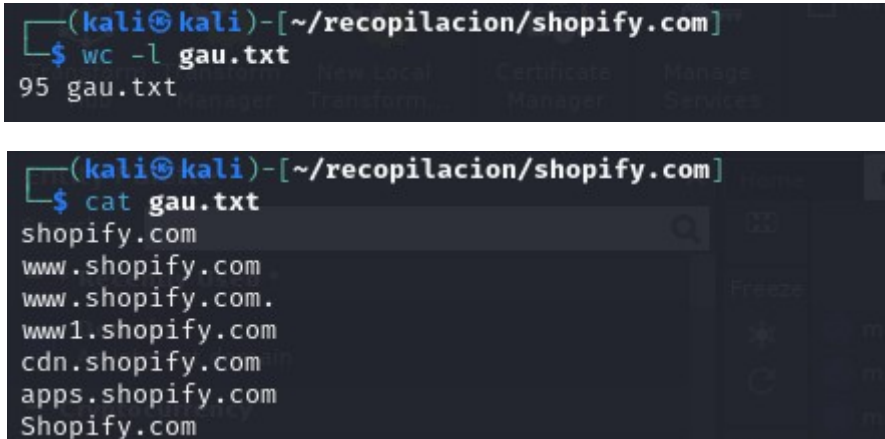
Archivos web y caché

gau

Recuperamos URLs conocidas guardadas en caché web tipo URLScan, Common Crawl, etc

```
gau --threads 10 shopify.com --o shopify.com/gau.txt
# Limpiamos
cat shopify.com/gau.txt | unfurl -u domains > shopify.com/gau.txt
```

Resultados:



```
(kali@kali)-[~/recopilacion/shopify.com]
$ wc -l gau.txt
95 gau.txt

(kali@kali)-[~/recopilacion/shopify.com]
$ cat gau.txt
shopify.com
www.shopify.com
www.shopify.com.
www1.shopify.com
cdn.shopify.com
apps.shopify.com
Shopify.com
```

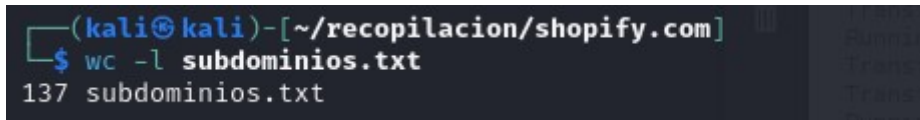
Limpiar resultados

Juntamos los resultados de todas las herramientas aplicadas y eliminamos los duplicados
Guardamos los resultados en el archivo subdominios.txt

```
# Juntamos todos los resultados en un solo archivo
cat shopify.com/assetfinder.txt shopify.com/cero.txt shopify.com/ctfr.txt
shopify.com/findomain.txt shopify.com/gau.txt shopify.com/katana.txt
shopify.com/shuffledns2.txt > shopify.com/subdominios.txt
```

```
# Quitamos duplicados y los que están fuera de scope
# Lo ponemos todo en minúsculas
cat shopify.com/subdominios.txt | grep -E shopify.com$ | tr '[:upper:]' '[:lower:]' |
unfurl -u domains > shopify.com/subdominios_ok.txt
```

Resultado final: 137 subdominios



```
(kali@kali)-[~/recopilacion/shopify.com]
$ wc -l subdominios.txt
137 subdominios.txt
```

4. Fingerprinting

Validar resultados del Footprinting

recopilacion/shopify.com/subdominios.txt

Antes de continuar con el Fingerprinting tenemos que validar los subdominios obtenidos es el Footprinting para confirmar que siguen vivos y filtrar aquellos que no lo estén.

httpx

Con esta herramienta validaremos los subdominios obtenidos
También comprobaremos si alguno admite el directorio /admin

```
cat shopify.com/subdominios.txt | /home/kali/go/bin/httpx -silent -mc 200,401,403 -t 10
-r1 50 -o shopify.com/subdominios_ok.txt
cat shopify.com/subdominios.txt | /home/kali/go/bin/httpx --path=admin --status-code
```

Resultados: 137

```
(kali@kali)-[~/recopilacion/shopify.com]
$ wc -l httpxAdmin.txt
137 httpxAdmin.txt
```

Escaneo de puertos

masscan

Previamente a usar masscan debemos convertir los subdominios a IP, ya que la herramienta no es capaz de hacerlo por si misma.

Lo haremos con la herramienta **dig**

recopilacion/shopify.com/subdominiosIP.txt

Ejecutamos masscan

Sólo se han encontrado los siguientes puertos abiertos: 80, 8080, 443, 8443

```
-33899,34571-34573,35500-35500,38292-38292,40193-40193,40911-40911,41511-41511,42510-42510,44501-44501,45100-45100,48080-48080,49152-49161,49163-49163,49165-49165,49167-49167,50003-50006,50300-50300,50389-50389,50500-50500,50636-50636,50800-50800,51103-51103,522-52822,52848-52848,52869-52869,54045-54045,54328-54328,55055-55056,55555-55555,57797-57797,58080-58080,60020-60020,60443-60443,61532-61532,61900-61900,62078-62078,64680-64680,65000-65000,65129-65129,65389-65389) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1707003696 Host: 54.231.198.117 () Ports: 80/open/tcp//http//
Timestamp: 1707003698 Host: 54.84.134.174 () Ports: 443/open/tcp//https//
Timestamp: 1707003701 Host: 104.17.73.206 () Ports: 8443/open/tcp//unknown//
Timestamp: 1707003705 Host: 23.227.60.200 () Ports: 443/open/tcp//https//
Timestamp: 1707003706 Host: 108.157.98.101 () Ports: 443/open/tcp//https//
Timestamp: 1707003713 Host: 34.117.159.98 () Ports: 80/open/tcp//http//
Timestamp: 1707003725 Host: 104.16.186.173 () Ports: 80/open/tcp//http//
Timestamp: 1707003726 Host: 104.17.74.206 () Ports: 8443/open/tcp//unknown//
Timestamp: 1707003728 Host: 52.84.45.101 () Ports: 80/open/tcp//http//
Timestamp: 1707003729 Host: 52.1.119.170 () Ports: 80/open/tcp//http//
```


Análisis web

GoWitness

Ejecutamos la herramienta Gowitness sobre nuestra lista de subdominio ya validada

recopilacion/shopify.com/screenshots/

```
gowitness file -f shopify.com/subdominios.txt -P shopify.com/screenshots
#gowitness report serve http://localhost:7171
gowitness server http://localhost:7171 -P shopify.com/screenshots
```

Tecnologías encontradas: Stimulus, Ruby on Rails, Ruby, Google Tag Manager, PHP, Site Kit: 1.118.0, WordPress, MySQL, React, AngularJS

URLs con login:


- <http://inbox.shopify.com/>
- <https://partnerships.shopify.com/>
- <https://admin.shopify.com/>
- <http://collabs.shopify.com/>

Detectar WAF

Usaremos esta herramienta para detectar si shopify.com utiliza un WAF y que versión:

Utiliza WAF (Cloudflare)

```
(kali@kali)-[~/recopilacion]
$ cat shopify.com/wafw00f.txt
```



```
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://shopify.com
[+] The site https://shopify.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

Descubrimiento de contenido

ffuf

Mediante una wordlist comprobaremos que directorios son visitables del dominio shopify.com

recopilacion/shopify.com/ffuf.txt

```
wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/common.txt -O lists/wordlistFuff.txt
ffuf -w lists/wordlistFuff.txt -t 20 -mc 200,401,403 -u https://www.shopify.com/FUZZ >
shopify.com/ffuf.txt
```

Se han obtenido bastantes directorios que responden positivamente, aunque ninguno de ellos parece tener mayor relevancia.

```
error_log [Status: 403, Size: 12725, Words: 237, Lines: 1, Duration: 29ms]
enterprise [Status: 200, Size: 159900, Words: 11727, Lines: 1062, Duration: 788ms]
es [Status: 200, Size: 453853, Words: 22726, Lines: 13, Duration: 217ms]
examples [Status: 200, Size: 323135, Words: 19855, Lines: 6, Duration: 270ms]
faq [Status: 200, Size: 200287, Words: 17007, Lines: 807, Duration: 837ms]
fr [Status: 200, Size: 484726, Words: 24832, Lines: 8, Duration: 236ms]
flow [Status: 200, Size: 273123, Words: 16617, Lines: 10, Duration: 2061ms]
forms [Status: 200, Size: 323736, Words: 18628, Lines: 16, Duration: 2744ms]
healthz [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 251ms]
google [Status: 200, Size: 282220, Words: 15818, Lines: 6, Duration: 2080ms]
id_rsa [Status: 403, Size: 12712, Words: 237, Lines: 1, Duration: 9ms]
id [Status: 200, Size: 371965, Words: 17535, Lines: 7, Duration: 186ms]
ie [Status: 200, Size: 400882, Words: 19081, Lines: 8, Duration: 257ms]
idea [Status: 200, Size: 159131, Words: 13966, Lines: 805, Duration: 422ms]
in [Status: 200, Size: 377847, Words: 17822, Lines: 7, Duration: 295ms]
```

whatweb

Lanzamos whatweb a ver que tecnologías encontramos
recopilacion/shopify.com/whatweb.txt

- <https://au.checkout.hardware.shopify.com/>
 - Google-Analytics[Universal][UA-82702-52]
 - JQuery[1.9.1]
- <https://eu.checkout.hardware.shopify.com/>
 - Email[Hardware-Store-Software2_600x600@2x.png,WISEPAD_COMP008_PREV2_900x_3674342b-fe05-461e-af0b-18263feae152_600x600@2x.png,mlllegeorgesand@gmail.com]
 - JQuery[1.9.1]
- <https://partnerships.shopify.com/>
 - Bootstrap
 - Via-Proxy[1.1 62a32701712a1c992cbde6a244acac8c.cloudfront.net (CloudFront)]
- <https://themes.shopify.com/>
 - XFrame-Options[sameorigin]
- <https://photos.shopify.com/>
 - Bootstrap[2.3.1]
 - JQuery[1.9.1]

5. Análisis de vulnerabilidades

Greenbone

Se ha lanzado un escaneo con sobre este dominio con los siguientes resultados
Presenta una gravedad baja

Vulnerability	Severity ▼	QoD	Host IP	Name	Location
TCP Timestamps Information Disclosure	2.0 (Low)	80 %	23.227.38.33	checkout.shopify.com	general/tcp

No ha encontrado ningún CVE



Report: Fri, Feb 2, 2024 11:47 PM UTC

Done

Information	Results (1 of 366)	Hosts (1 of 1)	Ports (0 of 13)	Applications (2 of 2)	Operating Systems (1 of 1)	CVEs (0 of 0)	Closed CVEs (0 of 0)
-------------	-----------------------	-------------------	--------------------	--------------------------	-------------------------------	------------------	-------------------------

No CVEs available

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Presenta una única vulnerabilidad muy baja que permite ver el tiempo que lleva encendido el host

Mitigable deshabilitando la propiedad timestamps

- Aunque en Windows Server no tiene una solución definitiva

Se ha encontrado un solo Host que monta un kernel Linux

Los certificados encontrados eran todos válidos

Subject DN ▲	Serial	Activates	Expires	IP
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
C=US,ST=California,L=San Francisco,O=Cloudflare, Inc.,CN=shopify.com	06B387654B9892C500A669B4F2250E2B	Wed, May 3, 2023 12:00 AM UTC	Thu, May 2, 2024 11:59 PM UTC	23.227.38.33
CN=shopify.com	04A25E4CD8E92162A82B1EC214BA345E3B26	Sat, Jan 20, 2024 6:36 PM UTC	Fri, Apr 19, 2024 6:36 PM UTC	23.227.38.33

Nuclei

recopilacion/shopify.com/nuclei.txt

Información recopilada

- Tecnología
 - [tech-detect:nginx] [http] [info] <https://kerwin.shopify.com>
 - [tech-detect:cloudflare] [http] [info] <https://lbperf2.ash.shopify.com>
 - [tech-detect:google-tag-manager] [http] [info] <https://partnerships.shopify.com>
 - [tech-detect:angular] [http] [info] <https://partnerships.shopify.com>
 - [tech-detect:angularjs] [http] [info] <https://partnerships.shopify.com>
 - [tech-detect:next.js] [http] [info] <https://polaris.shopify.com>
 - [aws-detect:aws-service] [http] [info] <http://apt.shopify.com>
- Cifrado
 - [weak-cipher-suites:tls-1.0] [ssl] [low] collabs.shopify.com:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
 - [weak-cipher-suites:tls-1.1] [ssl] [low] collabs.shopify.com:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
 - [weak-cipher-suites:tls-1.0] [ssl] [low] egress-ips.shopify.com:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
 - [weak-cipher-suites:tls-1.1] [ssl] [low] egress-ips.shopify.com:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
 - [weak-cipher-suites:tls-1.0] [ssl] [low] ux.shopify.com:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
 - [weak-cipher-suites:tls-1.1] [ssl] [low] ux.shopify.com:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]

Wordpress

wpscan

recopilacion/shopify.com/wpscan.txt

Parece que el objetivo no utiliza wordpress



Análisis SSL/TLS

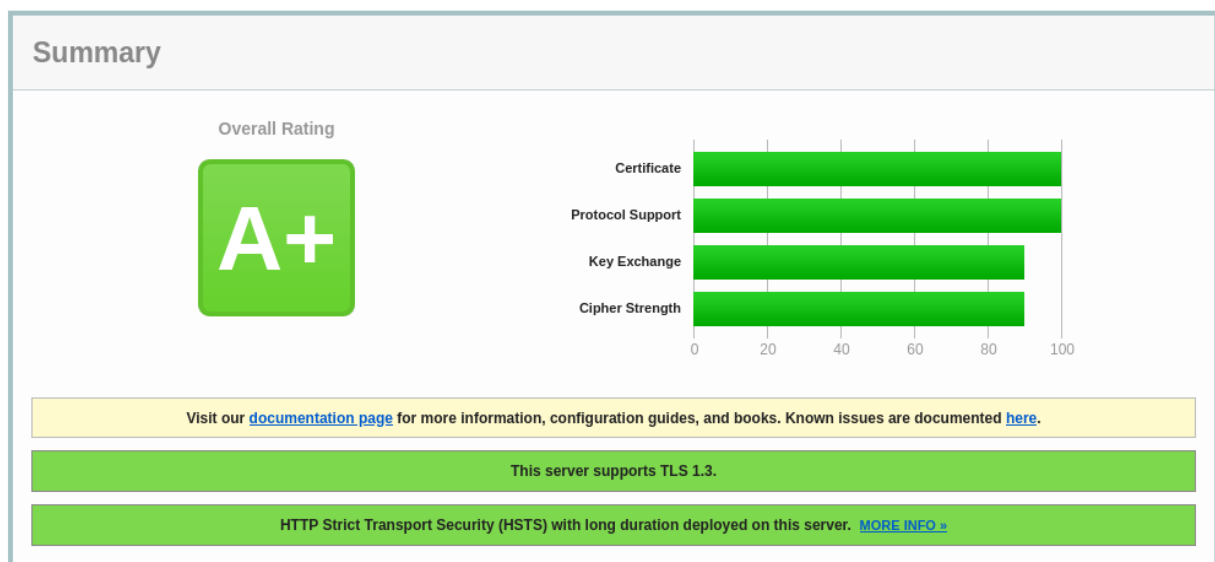
SSL Labs

Parece que en general el objetivo goza de buena salud

SSL Report: shopify.com (23.227.38.33)

Assessed on: Sat, 03 Feb 2024 12:05:34 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



testssl

recopilacion/shopify.com/testssl.txt

La única vulnerabilidad destacable, hace referencia al cifrado TLS, que permite el 1.0 y 1.1 que lo haría vulnerable a un ataque LUCKY13

BEAST (CVE-2011-3389)	not vulnerable (OK), no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental	potentially VULNERABLE , uses cipher block chaining (CBC) ciphers with TLS. Check patches
Winshock (CVE-2014-6321), experimental	not vulnerable (OK)

Por lo demás, el objetivo se defiende bien

Rating (experimental)	
Rating specs (not complete)	SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation	https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)	100 (30)
Key Exchange (weighted)	90 (27)
Cipher Strength (weighted)	90 (36)
Final Score	93
Overall Grade	A+
Done 2024-02-03 13:56:21 [165s] —> 23.227.38.33:443 (shopify.com) <—	

Análisis de servidores de correo

mxtoolbox

<https://mxtoolbox.com/spf.aspx>

Comprobamos como están los servicios de correo

No se encuentran vulnerabilidades apreciables

v=spf1 include:_spf.google.com include:mail.zendesk.com include:mailgun.org include:sendgrid.net ip4:23.227.61.129 ip4:23.227.61.130 ~all

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	include	_spf.google.com	Pass	The specified domain is searched for an 'allow'.
+	include	mail.zendesk.com	Pass	The specified domain is searched for an 'allow'.
+	include	mailgun.org	Pass	The specified domain is searched for an 'allow'.
+	include	sendgrid.net	Pass	The specified domain is searched for an 'allow'.
+	ip4	23.227.61.129	Pass	Match if IP is in the given range.
+	ip4	23.227.61.130	Pass	Match if IP is in the given range.
~	all		SoftFail	Always matches. It goes at the end of your record.

✓ DMARC

Your domain has a valid DMARC record and your DMARC policy will prevent abuse of your domain by phishers and spammers.

+ [Details](#)

✓ SPF

Great job! You have a valid SPF record, which specifies a soft fail (~all).

+ [Details](#)

✓ DKIM

We found at least one DKIM valid record. It's likely that you have others as each email sending source should have its own DKIM keys. DMARC visibility can help you discover each of your DKIM keys and much more.

+ [Details](#)

spoofcheck

recopilacion/shopify.com/spoofcheck.txt

No permite hacer spoofing

```
(kali@kali)-[~/recopilacion]
$ cat shopify.com/spoofcheck.txt
[*] Found SPF record:
[*] v=spf1 include:_spf.google.com include:mail.zendesk.com include:mailgun.org include:sendgrid.net ip4:23.227.61.129 ip4:23.227.61.130 ~all
[*] SPF record contains an All item: ~all
[*] Found DMARC record:
[*] v=DMARC1; p=reject; pct=100; fo=1; rua=mailto:dmARC-aggregate@shopify.com;ruf=mailto:dmARC-reports@shopify.com
[-] DMARC policy set to reject
[*] Aggregate reports will be sent: mailto:dmARC-aggregate@shopify.com
[*] Forensics reports will be sent: mailto:dmARC-reports@shopify.com
[-] Spoofing not possible for shopify.com
```

Subdomain takeover

subzy

recopilacion/shopify.com/subzy.txt

Aparentemente, el objetivo no parece vulnerable a ataques de subdomain takeover

```
(kali@kali)-[~/recopilacion]
$ cat shopify.com/subzy.txt
[ * ] Loaded 1 targets
[ * ] Loaded 44 fingerprints
[ No ] HTTPS by default (--https)
[ 10 ] Concurrent requests (--concurrency)
[ No ] Check target only if SSL is valid (--verify_ssl)
[ 10 ] HTTP request timeout (in seconds) (--timeout)
[ No ] Show only potentially vulnerable subdomains (--hide_fails)
[ NOT VULNERABLE ] - shopify.com
```


6. OSINT y redes sociales

Maltego

Archivo: recopilacion/shopify.com/maltego.mtgl

Descubrimientos

Personas

 maltego.Person	Elvin Efendiev
 maltego.Person	Monica
 maltego.Person	Julian Nadeau
 maltego.Person	Dylan Kendal
 maltego.Person	Peiwen Chen
 maltego.Person	dylankendal@gmail.com
 maltego.Person	Richard McGain
 maltego.Person	Burke Libbey
 maltego.Person	Dylan Kendal
 maltego.Person	Scott Francis
 maltego.Person	Vlad Gorodetsky
 maltego.Person	Bouke van der Bijl
 maltego.Person	Yandu Oppacher

Emails

@ maltego.EmailAddress	hostmaster@nsone.net.
@ maltego.EmailAddress	abusecomplaints@markmonitor.com
@ maltego.EmailAddress	julian@shopify.com
@ maltego.EmailAddress	bouke@shopify.com
@ maltego.EmailAddress	peiwen.chen@shopify.com
@ maltego.EmailAddress	dylan.kendal@shopify.com
@ maltego.EmailAddress	vlad.gorodetsky@shopify.com
@ maltego.EmailAddress	burke.libbey@shopify.com
@ maltego.EmailAddress	richard.mcgain@shopify.com
@ maltego.EmailAddress	monica.gallant@shopify.com
@ maltego.EmailAddress	yandu.oppacher@shopify.com
@ maltego.EmailAddress	elvin.efendiev@shopify.com
@ maltego.EmailAddress	scott.francis@shopify.com
@ maltego.EmailAddress	thomas.mcgoeysmith@shopify.com

Alguno de los correos parece preparado para aceptar todo el correo entrante.


- IPQS Info

Indicates this email is likely to be a "catch all" where the mail server verifies all emails tested against it as valid. It is difficult to determine if the address is truly valid in these scenarios, since the email's server will not confirm the account's status.

- Generator detail

Source	yandu.oppacher@shopify.com	(Email Address)
Transform	Get tags and indicators for email address [IPQS]	
Gen. date	2024-02-03 19:52:16.814 +0100	

haveibeenpwned

Node
cmlh.Node
@haveibeenpwned - Not Listed within Pastes

- Relationships

- Incoming

scott.francis@shopify.com

thomas.mcgoeysmith@shopify.com

bouke@shopify.com

peiwen.chen@shopify.com

elvin.efendiev@shopify.com

- Generator detail

Source	scott.francis@shopify.com	(Email Address)
Transform	Get all pastes featuring the e-mail address [v3 @haveibeenpwned]	
Gen. date	2024-02-03 19:12:30.066 +0100	




Source	thomas.mcgoeysmith@shopify.com	(Email Address)
Transform	Get all pastes featuring the e-mail address [v3 @haveibeenpwned]	
Gen. date	2024-02-03 19:12:38.779 +0100	

Source	bouke@shopify.com	(Email Address)
Transform	Get all pastes featuring the e-mail address [v3 @haveibeenpwned]	
Gen. date	2024-02-03 19:12:21.136 +0100	














Source	peiwen.chen@shopify.com	(Email Address)
Transform	Get all pastes featuring the e-mail address [v3 @haveibeenpwned]	
Gen. date	2024-02-03 19:12:47.504 +0100	












Source	elvin.efendiev@shopify.com	(Email Address)
Transform	Get all pastes featuring the e-mail address [v3 @haveibeenpwned]	
Gen. date	2024-02-02 19:16:49.519 +0100	

Teléfonos

 maltego.PhoneNumber	+44 20 3206 2220
 maltego.PhoneNumber	+1 800 745 9229
 maltego.PhoneNumber	+1 208 685 1750

Archivos (wayback)

 maltego.wayback.FileSnapshot	2023 Mar 02: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Nov 01: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Jul 01: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Dec 02: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Aug 01: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Jul 09: assetlinks.json
 maltego.wayback.FileSnapshot	2023 May 31: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Oct 10: assetlinks.json
 maltego.wayback.FileSnapshot	2023 Jun 01: assetlinks.json
 maltego.wayback.FileSnapshot	2024 Jan 26: style.css
 maltego.wayback.FileSnapshot	2024 Jan 25: facebook-pixel.js
 maltego.wayback.FileSnapshot	2024 Jan 27: Pixels-fox-app-block.js
 maltego.wayback.FileSnapshot	2024 Jan 26: facebook-pixel.js

 maltego.documentcloud	6895195
 maltego.documentcloud	6895073
 maltego.documentcloud	23731434
 maltego.documentcloud	20518930
 maltego.documentcloud	20510822
 maltego.documentcloud	6592489
 maltego.documentcloud	5760763
 maltego.documentcloud	20691520
 maltego.documentcloud	7008916
 maltego.documentcloud	3438197
 maltego.documentcloud	6988997

Google drive







Encontramos un drive público con reportajes fotográficos de los empleados

https://drive.google.com/drive/folders/1QCWVckQ_-WXIYMZ1OG0njaWWbMorK6yb

Shopify Me... > Shopify Media Im... > SHO... ▾ 👤

✓ ≡ ☰ ⓘ

Tipo ▾ Personas ▾ Modificado ▾

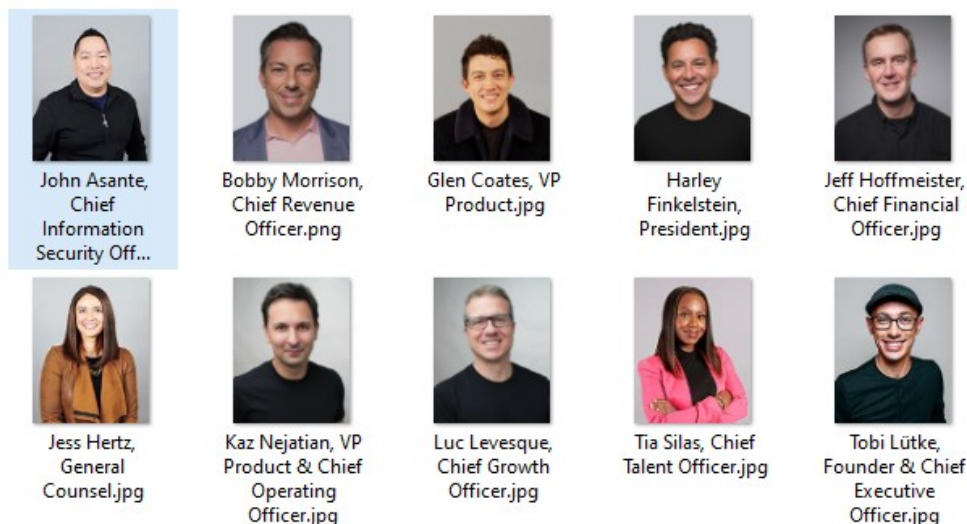
Nombre	Propietario	Última modificación	Tamaño de a
  kristina.caracciolo@shop...	5 oct 2021	kristina.caracciol...	28 kB
  kristina.caracciolo@shop...	5 oct 2021	kristina.caracciol...	1,4 MB
  kristina.caracciolo@shop...	5 oct 2021	kristina.caracciol...	29 kB

También obtenemos de ahí la dirección de correo de tres empleados y los verificamos con su cuenta de linkedin

- samantha.tam@shopify.com
 - <https://www.linkedin.com/in/samantha-tam-08181278/>
- jackie.warren@shopify.com
 - <https://www.linkedin.com/in/jackiewarren/>
- kristina.caracciolo@shopify.com
 - <https://www.linkedin.com/in/kristina-caracciolo-7bb840b6/>

Hay una carpeta con fotos de ejecutivos

- Incluye nombre y puesto
- <https://drive.google.com/drive/folders/1XAIJhEUOJNYNL9mWqH2Q-TcFJdIS38on>
- Jonh Asante de ciber ya no trabaja en shopify



Metadatos

Imágenes

- Información sobre el estudio de fotografía que las hizo

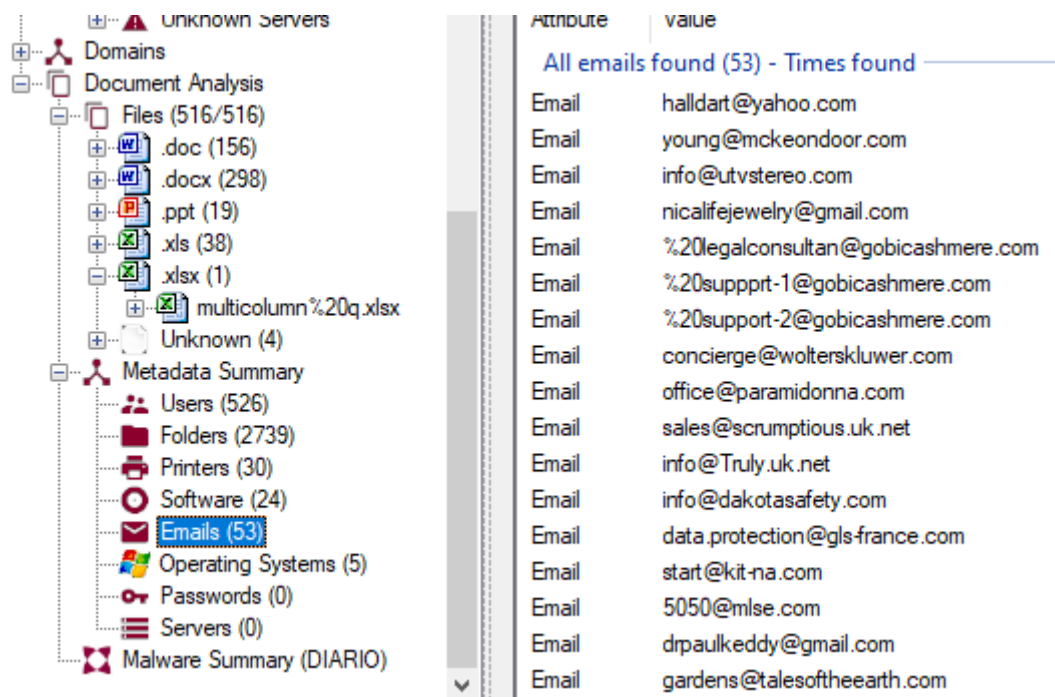
Documentos

- Sólo aparece un archivo
- site:shopify.com ext:docx
 - N/A
 - https://www.google.com/url?sa=i&url=https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F1916%2F3265%2Ffiles%2FRW1_Manual.docx&psig=AOvVaw2EQk8uPW9ZyLuN551EN7dl&ust=1707079990042000&source=images&cd=vfe&opi=89978449&ved=0CAYQn5wMahcKEwjIxbXUhpCEAxUAAAAAHQAAAAAQBA
- site:shopify.com ext:xlsx
 - https://www.google.com/url?sa=i&url=https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F2391%2F5185%2Ffiles%2FSoldering_Services_usa_sample.xlsx&psig=AOvVaw0VIXLeqoO2IsDsC00_TPEk&ust=1707080020520000&source=images&cd=vfe&opi=89978449&ved=0CAYQn5wMahcKEwj44vnihpCEAxUAAAAAHQAAAAAQBA

Foca

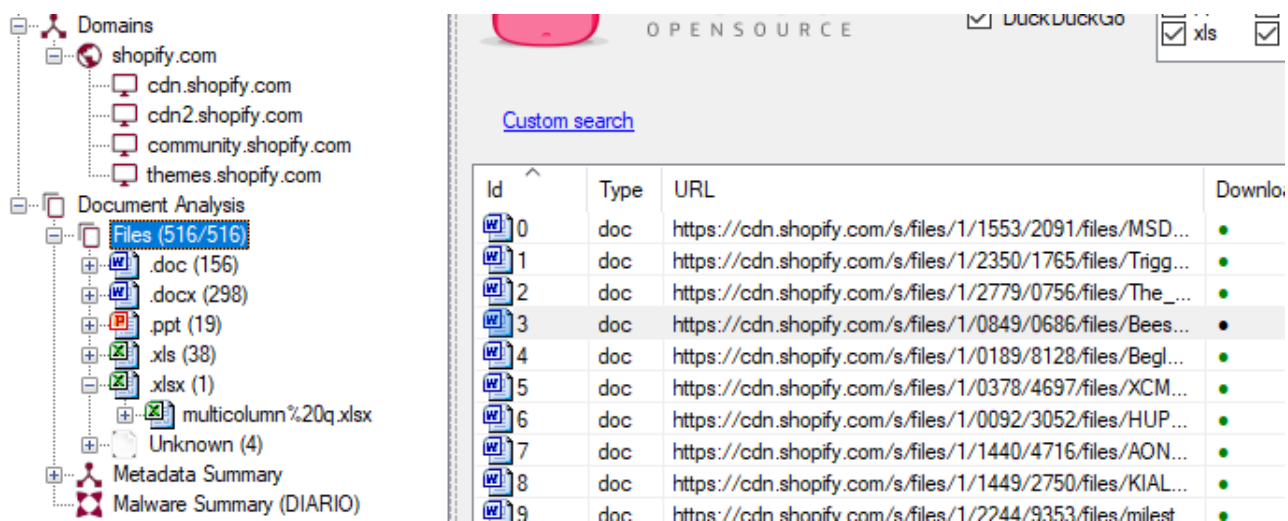
archivos en cdn.shopify.com

- Parecen enviados por proveedores
 - Nada relevante en metadatos
 - Desde ese subdominio se ven muchos archivos e info de Clientes/proveedores
 - Tal vez no deberían poder verse
- Obtenemos una lista de email pero ninguno perteneciente al objetivo



Attribute	Value
All emails found (53) - Times found	
Email	halldart@yahoo.com
Email	young@mckeondoor.com
Email	info@utvstereo.com
Email	nicalifejewelry@gmail.com
Email	%20legalconsultan@gobicashmere.com
Email	%20supprt-1@gobicashmere.com
Email	%20support-2@gobicashmere.com
Email	conciierge@wolterskluwer.com
Email	office@paramidonna.com
Email	sales@scrumptious.uk.net
Email	info@Truly.uk.net
Email	info@dakotasafety.com
Email	data.protection@gls-france.com
Email	start@kit-na.com
Email	5050@mlse.com
Email	drpaulkeddy@gmail.com
Email	gardens@talesoftheearth.com

Archivos descargable desde ciertos dominios



Id	Type	URL	Download
0	doc	https://cdn.shopify.com/s/files/1/1553/2091/files/MSD...	●
1	doc	https://cdn.shopify.com/s/files/1/2350/1765/files/Trigg...	●
2	doc	https://cdn.shopify.com/s/files/1/2779/0756/files/The_...	●
3	doc	https://cdn.shopify.com/s/files/1/0849/0686/files/Bees...	●
4	doc	https://cdn.shopify.com/s/files/1/0189/8128/files/Begl...	●
5	doc	https://cdn.shopify.com/s/files/1/0378/4697/files/XCM...	●
6	doc	https://cdn.shopify.com/s/files/1/0092/3052/files/HUP...	●
7	doc	https://cdn.shopify.com/s/files/1/1440/4716/files/AON...	●
8	doc	https://cdn.shopify.com/s/files/1/1449/2750/files/KIAL...	●
9	doc	https://cdn.shopify.com/s/files/1/2244/9353/files/milest	●