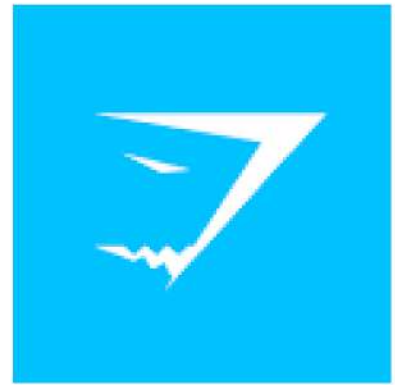


**CASO PRÁCTICO**

# **RECONOCIMIENTO DE UNA ORGANIZACIÓN**



**GYMSHARK**

Gymshark es una marca, fabricante y minorista británico de ropa y accesorios de fitness. Crea y distribuye su propia gama de ropa deportiva.

DOMINIOS "IN SCOPE" ELEGIDOS: \*.gymshark.com  
\*.gymshark.io

```
DOMINIOS "OUT OF SCOPE" :      onboarding.gymshark.com
                                gymshark.okta.com
                                creators.gymshark.com
```

## SUBDOMINIOS

Lo primero para conseguir los subdominios de gymshark es hacer uso de dos herramientas: amass y puredns

Los resultados de amass serán guardados en la carpeta : gymshark-amass

## AMASS

Primero amass. No sin antes configurarlo :

**Resolvers** (los que se encargan de hacer consultas a un servidor DNS) ,se decide usar el de google, Clouflare,Verisign,Hurricane Electric,las secundarias de dos de estas y por cuenta propia se decide investigar sobre otros resolvers para añadir

En **Scope**, viendo que se puede ser bastante especifico poniendo desde el ASN hasta los puertos,se decide mantener los puertos que venían seleccionados por defecto para igualmente conseguir la mayor información posible.

```
# Root domain names used in the enumeration. The findings
[scope.domains]
domain = gymshark.com
domain = gymshark.io
#domain = appsec.eu
#domain = appsec-labs.com

# Are there any subdomains that are out of scope?
[scope.blacklisted]
subdomain = onboarding.gymshark.com
subdomain = creators.gymshark.com
subdomain = gymshark.okta.com
```

En **scope.domains**, el alcance respecto a las direcciones, puse los que estaban dentro del scope en hackerone. De igual forma se escriben los dominios fuera del scope

```
kali@kali: ~/config/amass

File Actions Edit View Help

kali@ka...ig/amass x kali@kali: ...fo/practica x kali@ka...ig/amass x kali@k...

# Settings related to DNS name brute forcing.
[bruteforce]
enabled = true
recursive = true
# Number of discoveries made in a subdomain before performing recursive brute forcing.
minimum_for_recursive = 1
wordlist_file = /home/kali/recoinfo/SecLists/Discovery/DNS/namelist.txt
#wordlist_file = /usr/share/wordlists/all.txt # multiple lists can be used

# Would you like to permute resolved names?
[alterations]
enabled = true
# edit_distance specifies the number of times a primitive edit operation will be
# performed on a name sample during fuzzy label searching.
edit_distance = 1 ; Setting this to zero will disable this expensive feature.
flip_words = true # test-dev.owasp.org → test-prod.owasp.org
flip_numbers = true # test1.owasp.org → test2.owasp.org
add_words = true # test.owasp.org → test-dev.owasp.org
add_numbers = true # test.owasp.org → test1.owasp.org
# Multiple lists can be used.
wordlist_file = /home/kali/recoinfo/SecLists/Discovery/DNS/namelist.txt
#wordlist_file = /usr/share/wordlists/all.txt
```



Se activa la fuerza bruta y la recursividad. Y se hace uso del SecLists proporcionado en el módulo para el tema de los diccionarios de palabras. En este caso para abarcar más, **se hará uso de dos diccionarios**

También se activa la opción de alteración de palabras para conseguir aun mas posibilidades, activando que cambie el orden de las palabras y los números unicamente. Haciendo uso del mismo diccionario

Tenemos la posibilidad de desactivar algunas fuentes de datos o hacer uso de alguna que no se encuentre por defecto. En este caso se opta por manteber lo ya configurado.

El comando quedaría así. Con **-v** para ver lo que va pasando, **-src** enseñará la fuente de donde ha sacado esa dirección, dándole la configuración y donde se quiere que se guarde y la página :

```
(kali@kali)-[~/config/amass]
$ amass enum -src -v -config /home/kali/.config/amass/config.ini -dir /home/kali/Desktop/practica/gymshark-amass/ -d gymshark.com
Querying Maltiverse for gymshark.com subdomains
```

Cabe notar que la mayor fuente de datos fue HacketTarget y AnubisDb , como curiosidad.

## PUREDNS

Mientras AMASS hace su trabajo, de forma paralela se pone a trabajar a PureDNS. Primero hay que hacerse con un archivo de gran cantidad de resolvers para agilizar este trabajo. Esto se hará con **dnsvalidator**. Con esta página proporcionada en clase se sacarán de ahí una lista de varios resolvers validos. Todo esto con el siguiente comando Aquí se usa el siguiente comando:

```
(kali@kali)-[~/Desktop/herramientas]
$ dnsvalidator -tL https://public-dns.info/nameservers.txt -threads 100 -o resolvers.txt
```

Confirmando que se ha creado y su contenido con **"cat"**.

Ya con la lista, ahora si se puede pasar a trabajar con puredns y hacer uso de estos resolvers para conseguir la mayor cantidad de webs. Todo esto con el siguiente comando :

```
(kali@kali)-[~/Desktop/herramientas]
$ puredns bruteforce /home/kali/Desktop/tools/SecLists/Discovery/DNS/namelist.txt gymshark.com -r resolvers.txt -write purednsresults1.txt
```

## El archivo creado será adjuntado con el nombre de : resolvers.txt

Indicando donde se encuentra el diccionario de palabras a usar, junto con el nombre de la página, adjuntando el archivo con los resolvers y pidiendo que todo se guarde en el archivo purednsresults.txt con **-w**

Se usa otro diccionario para la misma pagina y asi se puede recoger más resultados

```
(kali@kali)-[~/Desktop/herramientas]
$ puredns bruteforce /home/kali/Desktop/tools/SecLists/Discovery/DNS/subdomains-top1million-110000.txt gymshark.com -r resolvers.txt -w purednsresults2.txt
```

Aún queda por usar puredns con el segundo dominio. Se aplican ambos diccionarios de igual manera

### 1º Diccionario

```
(kali@kali)-[~/Desktop/herramientas]
$ puredns bruteforce /home/kali/Desktop/tools/SecLists/Discovery/DNS/namelist.txt gymshark.io -r resolvers.txt -w purednsresults3.txt
```

### 2º Diccionario

```
(kali@kali)-[~/Desktop/herramientas]
$ puredns bruteforce /home/kali/Desktop/tools/SecLists/Discovery/DNS/subdomains-top1million-110000.txt gymshark.io -r resolvers.txt -w purednsresults4.txt
```

Ahora teniendo las listas de los resultados de puredns de ambos sitios web. Se juntan y se limpian para que ningún sitio se repita

Para juntar listas

```
(kali@kali)-[~/Desktop/herramientas]
$ cat purednsresults4.txt >> purednsresults

(kali@kali)-[~/Desktop/herramientas]
$ cat purednsresults | sort | uniq
```

66.gymshark.com  
admintest.gymshark.com  
api.gymshark.com  
api.staging.gymshark.com  
app.gymshark.com  
apply.gymshark.com  
au.gymshark.com  
auth.gymshark.com  
autodiscover.gymshark.com  
autodiscover.mail.gymshark.com  
autodiscover.s.gymshark.com  
backstage.gymshark.io  
ca.gymshark.com  
calendar.gymshark.com  
callback.gymshark.com  
careers.gymshark.com  
cdn.gymshark.com  
central.gymshark.com  
ch.gymshark.com  
community.gymshark.com  
config.gymshark.io  
content.gymshark.com  
creators.gymshark.com  
currencies.gymshark.com  
de.gymshark.com  
design.gymshark.com  
develop.gymshark.com  
dev.gymshark.com  
dk.gymshark.com  
e.gymshark.com

Para limpiarla y no se repita nada

Los resultados de puredns serán guardados en la carpeta : gymshark-puredns



Una vez estan los resultados de amass, se juntan también esta lista con la de puredns con el mismo procedimiento mostrado anteriormente .  
Quedaría algo así :

```
(kali@kali)-[~/Desktop]
$ cat /home/kali/Desktop/practica/subdomains | sort | uniq

2048.develop.gymshark.com
2048-game.develop.gymshark.com
66.gymshark.com
ablink.app.gymshark.com
ablink.e.gymshark.com
ablink.mail.gymshark.com
ablink.store.gymshark.com
ablink.train.gymshark.com
admin.tableau.develop.gymshark.io
admin.tableau.gymshark.io
admin.tableau.staging.gymshark.io
admintest.gymshark.com
api-creators.gymshark.com
api.develop.gymshark.com
api.gymshark.com
api.staging.gymshark.com
api.teabreak.gymshark.io
api.teabreak.staging.gymshark.io
app.gymshark.com
apply.gymshark.com
athens.staging.gymshark.com
au.gymshark.com
au.pwks.gymshark.io
au.shop.gymshark.com
auth.develop.gymshark.com
auth.develop.gymshark.io
auth.gshq.gymshark.io
auth.gshq.staging.gymshark.io
```

La lista completa de subdominios se encontrará en el archivo : subdomains

## COMPROBAR PUERTOS

### HTTPX

Ya con una lista limpia, con todos los subdominios recolectados, se comprueban las webs. Saber si tienen puertos http abiertos. Esto se puede solucionar con HTTPX.

Se dan los puertos que se quieren revisar y un **-silent** para hacer el minimo ruido posible. Todos estos resultados guardados en "httpxresults.txt" gracias al **-o**

```
(kali@kali)-[~/Desktop/practica]
$ httpx -p 80,443,8080,8000,8001,8443,8008 -list subdomains.txt -silent -o httpxresults.txt
Traceback (most recent call last):
  File "/usr/bin/httpx", line 33, in <module>
    sys.exit(load_entry_point('httpx==0.23.0', 'console_scripts', 'httpx')())
  File "/usr/bin/httpx", line 25, in importlib_load_entry_point
    return next(matches).load()
  File "/usr/lib/python3.10/importlib/metadata/__init__.py", line 171, in load
    module = import_module(match.group('module'))
```

Desgraciadamente en este caso no se pudo ejecutar el programa, ya que se ejecutaba un httpx de python y no se descargaba tampoco de github correctamente.

Sin embargo queria dejar plasmado como se haría.

## NMAP

A continuación se va a usar nmap para usarlo en toda la lista de dominios y conseguir ver si tiene puertos abiertos.

```
(kali@kali)-[~/Desktop/herramientas]
$ sudo nmap -sS -Pn -sV -O --reason --open -oA nmapresults -iL subdomains
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-31 13:16 EST
Stats: 0:03:14 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.81% done; ETC: 13:21 (0:01:56 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
```

Esta linea de comandos esta conformada por :

- sS Es para un sondeo TCP SYN . Ayuda a que pueda realizarse rápidamente, sondeando miles de puertos por segundo en una red rápida en la que no existan cortafuegos. El sondeo SYN es relativamente sigiloso y poco molesto, ya que no llega a completar las conexiones TCP.
- Pn va a tratar a todos los host como online. Ya que muchas veces estos pueden ocultarse , asi que asi nos aseguramos de abarcar todo
- sV nos puede decir la version del servicio que hay detras de cada dirección que le demos
- O intentará proporcionarnos su sistema operativo
- reason proporcionará la razon por la que un puerto esta en determinado estado
- open mostrará unicamente puertos abiertos para no contar con datos que no aportan nada
- oA se pide que el output me lo de en tres formatos: normal, Linux-grep y XML. Como no sé sabe si vaya hacer falta alguno para emplearlo en otra herramienta, es mejor tener los tres para prevenir.
- iL ingresamos el archivo del que queremos que lea los subdominios en este caso

Los resultados de este es bastante extenso, se recuerda que se adjuntaran con este archivo. **Los puertos abiertos con los que cuentan estas paginas son el 80 y 443**

Entre estos documentos se pudo encontrar lo siguiente :

- Una de estas páginas hace uso de OpenSSH 7.4. Esta versión después de una breve investigación, se hayó con una vulnerabilidad. Esta se trata de una posible enumeración de usuarios y es que las aplicaciones web arrojen un mensaje indicando si el nombre de usuario existe o no. Gracias este tipo de mensajes, es posible realizar ataques de fuerza bruta e identificar los usuarios válidos para la aplicación. De hecho el exploit de esto no es complicado de conseguir. Si se copia y pega el siguiente enlace en el navegador, encontrará el exploit facilitado en la plataforma de Github

<https://github.com/Sait-Nuri/CVE-2018-15473>



```

65 Nmap scan report for gdpr.gymshark.com (18.132.255.24)
66 Host is up, received user-set (0.044s latency).
67 rDNS record for 18.132.255.24: ec2-18-132-255-24.eu-west-2.compute.amazonaws.com
68 Not shown: 997 filtered tcp ports (no-response), 1 closed tcp port (reset)
69 Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
70 PORT      STATE SERVICE REASON          VERSION
71 22/tcp    open  ssh      syn-ack ttl 230    OpenSSH 7.4 (protocol 2.0)
72 80/tcp    open  http     syn-ack ttl 230    nginx 1.20.0
73 Aggressive OS guesses: Linux 5.0 - 5.4 (91%), Linux 5.1 (91%), Linux 2.6.32 - 3.13 (91%), Linux 2.6.22 - 2.6.36 (89%), Linux 3.10 (89%), Linux
  3.10 - 4.11 (89%), Linux 5.4 (89%), Linux 2.6.39 (89%), Linux 2.6.32 (88%), Linux 3.2 - 4.9 (88%)
74 No exact OS matches for host (test conditions non-ideal).
75

```

- Varias de las paginas hacen uso de Amazon CloudFront y CloudFlare

```

orted as filtered due to --defeat-rst-ratelimit
        VERSION
k ttl 247 Amazon CloudFront httpd
k ttl 247 Amazon CloudFront httpd
e unreliable because we could not find at least

```

```

rts (no-response)
ted as filtered due to --defeat-rst-ratelimit
        VERSION
k ttl 54 Cloudflare http proxy
k ttl 54 Cloudflare http proxy
k ttl 54 Cloudflare http proxy
k ttl 54 Cloudflare http proxy
unreliable because we could not find at least
n XPanel control system (91%), ASUS RT-N56U
k Camera (Linux 2.6.17) (88%), HP P2000 G3

```

Los resultados de nmap serán guardados en la carpeta : nmapresults

## EYEWITNESS

Con lo subdominios que ya se tienen se hace uso de eyewitness para recoger capturas de pantalla de cada una e información de estas.

Esto se consigue con el siguiente comando :

```

(kali@kali)-[~/Desktop/herramientas/EyeWitness/Python]
$ ./EyeWitness.py --web -f /home/kali/Desktop/herramientas/subdomains -d eyewitnessresults


```





Son bastantes los resultados debido al gran volumen de dominios con el que se cuenta.

De igual forma se puede destacar información de ciertas páginas:

- Esta nos muestra un formulario para ingresar a lo que sería su apartado de GitLab. Una suite completa que permite gestionar, administrar, crear y conectar los repositorios con diferentes aplicaciones y hacer todo tipo de integraciones con ellas

Web Request Info	Web Screenshot
<p><a href="http://gitlab.562366055580.sandbox.gymshark.io">http://gitlab.562366055580.sandbox.gymshark.io</a> <b>Resolved to:</b> 52.206.95.233</p> <p><b>Page Title:</b> Sign in · GitLab <b>Date:</b> Tue, 31 Jan 2023 19:14:04 GMT <b>Content-Type:</b> text/html; charset=utf-8 <b>Transfer-Encoding:</b> chunked <b>Connection:</b> close <b>Server:</b> nginx <b>Vary:</b> Accept-Encoding <b>Cache-Control:</b> max-age=0, private, must-revalidate <b>Content-Security-Policy:</b> <b>Etag:</b> W/"f301051513ee14dbdbbb8fc584b67b58" <b>Permissions-Policy:</b> interest-cohort=() <b>Pragma:</b> no-cache <b>Set-Cookie:</b> _gitlab_session=85a8babc567002b30b85851825ad8c69; path=/; expires=Tue, 31 Jan 2023 21:14:04 GMT; secure; HttpOnly; SameSite=None <b>X-Content-Type-Options:</b> nosniff <b>X-Download-Options:</b> noopen <b>X-Frame-Options:</b> SAMEORIGIN <b>X-Permitted-Cross-Domain-Policies:</b> none <b>X-Request-Id:</b> 64c0d4860c7910000750000000000000</p>	

- Varias páginas arrojan la misma opción de descargar la aplicación

<p><a href="http://training.gymshark.com">http://training.gymshark.com</a> <b>Resolved to:</b> 18.154.22.42</p> <p><b>Page Title:</b> Gymshark Training   Free Workout App   Gymshark <b>Content-Type:</b> text/html <b>Content-Length:</b> 53364 <b>Connection:</b> close <b>Date:</b> Tue, 31 Jan 2023 19:16:26 GMT <b>Last-Modified:</b> Tue, 15 Mar 2022 15:32:15 GMT <b>Etag:</b> "7803251146515a0da68952768ad9830" <b>Accept-Ranges:</b> bytes <b>Server:</b> AmazonS3 <b>X-Cache:</b> Miss from cloudfront <b>Via:</b> 1.1 c762436a1b7384144bad10e6ca25154.cloudfront.net (CloudFront) <b>X-Amz-CF-Pop:</b> MAD53-P1 <b>X-Amz-CF-Id:</b> 911E-MhCzE4-Fpdcma5fC9sTMnKp-w8t6uPqGdBN5GKNBElyxGw== <b>Response Code:</b> 200</p> <p><a href="#">Source Code</a></p>	
<p><a href="http://training.staging.gymshark.com">http://training.staging.gymshark.com</a> <b>Resolved to:</b> 18.154.41.3</p> <p><b>Page Title:</b> Gymshark Training   Free Workout App   Gymshark <b>Content-Type:</b> text/html <b>Content-Length:</b> 53364 <b>Connection:</b> close <b>Last-Modified:</b> Mon, 14 Mar 2022 09:58:17 GMT <b>Accept-Ranges:</b> bytes <b>Server:</b> AmazonS3 <b>Date:</b> Tue, 31 Jan 2023 18:23:46 GMT <b>Etag:</b> "f5e843ab91972b64a2e7e9858a91c782" <b>X-Cache:</b> Hit from cloudfront <b>Via:</b> 1.1 fb1721a57535e7448b0b6e00ca4494.cloudfront.net (CloudFront) <b>X-Amz-CF-Pop:</b> MAD53-P2 <b>X-Amz-CF-Id:</b> Bqbpqoq4UY9KJ_3-C_bFnd7BEh_k1YqDcpv0tHFOXVgLnWJYQ== <b>Age:</b> 2490 <b>Response Code:</b> 200</p> <p><a href="#">Source Code</a></p>	

- Algunas nos muestran lo que vendría a ser un "teabreak"(un descanso). Ofrecen servicios por medio de su aplicación, a cambio de una suscripción, ejercicios y rutinas. Seguramente esto este relacionado con descansos despues de ejercicios .

<p><a href="http://teabreak.gymshark.io">http://teabreak.gymshark.io</a> Resolved to: 52.6.80.188</p> <p><b>Page Title:</b> Gymshark Virtual Tea Break Service <b>Accept-Ranges:</b> bytes <b>Content-Length:</b> 2380 <b>Content-Security-Policy:</b> default-src 'none'; script-src 'self'; connect-src 'self' https://auth.gshq.gymshark.io https://api.teabreak.gymshark.io; img-src 'self' https://avatars.stack-edge.com https://secure.gravatar.com; style-src 'self' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; manifest-src 'self'; base-uri 'self'; form-action 'none'; frame-ancestors 'none'; frame-src https://auth.gshq.gymshark.io; <b>Content-Type:</b> text/html; charset=utf-8 <b>Date:</b> Tue, 31 Jan 2023 19:13:44 GMT <b>Etag:</b> "6373c30-94c" <b>Last-Modified:</b> Mon, 07 Feb 2022 12:10:35 GMT <b>Permissions-Policy:</b> accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()</p>	<p><b>VIRTUAL TEABREAK SERVICE</b></p> <p>You are required to login to access the virtual teabreak service.</p> <p><a href="#">Login</a></p>
<p><a href="http://teabreak.staging.gymshark.io">http://teabreak.staging.gymshark.io</a> Resolved to: 67.202.47.151</p> <p><b>Page Title:</b> Gymshark Virtual Tea Break Service <b>Accept-Ranges:</b> bytes <b>Content-Length:</b> 2380 <b>Content-Security-Policy:</b> default-src 'none'; script-src 'self'; connect-src 'self' https://auth.gshq.staging.gymshark.io https://api.teabreak.staging.gymshark.io; img-src 'self' https://avatars.stack-edge.com https://secure.gravatar.com; style-src 'self' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; manifest-src 'self'; base-uri 'self'; form-action 'none'; frame-ancestors 'none'; frame-src https://auth.gshq.staging.gymshark.io; <b>Content-Type:</b> text/html; charset=utf-8 <b>Date:</b> Tue, 31 Jan 2023 19:13:20 GMT <b>Etag:</b> "6373c30-94c" <b>Last-Modified:</b> Thu, 24 Nov 2022</p>	<p><b>VIRTUAL TEABREAK SERVICE</b></p> <p>You are required to login to access the virtual teabreak service.</p> <p><a href="#">Login</a></p>

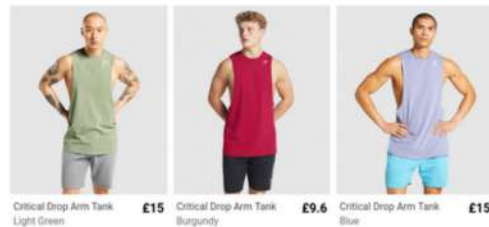
- Más formularios donde directamente nos piden una contraseña

<p><a href="http://shop.dk.staging.gymshark.com">http://shop.dk.staging.gymshark.com</a> Resolved to: 18.154.48.34</p> <p><b>Page Title:</b> Gymshark   Login required <b>Content-Type:</b> text/html; charset=utf-8 <b>Transfer-Encoding:</b> chunked <b>Connection:</b> close <b>Date:</b> Tue, 31 Jan 2023 19:05:10 GMT <b>X-Powered-By:</b> Next.js <b>Cache-Control:</b> private, no-cache, no-store, max-age=0, must-revalidate <b>Vary:</b> Accept-Encoding <b>X-Cache:</b> Miss from cloudfront <b>Via:</b> 1.1 43df20a5894fa784ae683a87c27deea8.cloudfront.net (CloudFront) <b>X-Amz-Cf-Pop:</b> MAD56-P3 <b>X-Amz-Cf-Id:</b> 7rAXeYMuzL5bV7g3-0TGQDlvqmF5QPNdvThTL0jPgqATixUYQr802W== <b>Response Code:</b> 200</p> <p><a href="#">Source Code</a></p>	<p><b>GYMSHARK STAGING STORE</b></p> <p><b>LOG IN</b></p> <p>Password</p> <p><a href="#">CONTINUE</a></p>
<p><a href="http://preview.staging.gymshark.com">http://preview.staging.gymshark.com</a> Resolved to: 76.76.21.164</p> <p><b>Page Title:</b> Gymshark   Login required <b>Content-Type:</b> text/plain <b>Location:</b> https://preview.staging.gymshark.com/ <b>Refresh:</b> 0;url=https://preview.staging.gymshark.com/ <b>server:</b> Vercel <b>Response Code:</b> 308</p> <p><a href="#">Source Code</a></p>	<p><b>GYMSHARK STAGING STORE</b></p> <p><b>LOG IN</b></p> <p>Password</p> <p><a href="#">CONTINUE</a></p>

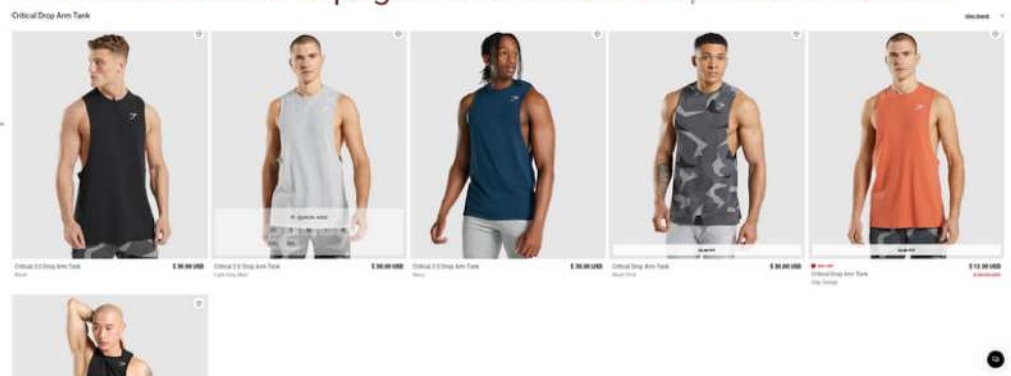
- Una página donde tal vez por un error o que se ha olvidado borrar contiene tres productos. Después de buscar en la tienda se puede ver que son productos que ya no están a la venta.

<http://headless.develop.gymshark.com>  
Resolved to: 108.157.98.84

Page Title: Headless  
Content-Type: text/html  
Content-Length: 5476  
Connection: close  
Date: Tue, 31 Jan 2023 18:29:14 GMT  
Last-Modified: Mon, 24 Jan 2022 10:57:19 GMT  
ETag: "e18a08479bcca5ff9303c960cd75d5f"  
Accept-Ranges: bytes  
Server: AmazonS3  
Vary: Accept-Encoding  
X-Cache: Hit from cloudfront  
Via: 1.1  
fftc37ec0e815384634f004781d4ffa4.cloudfront.net (CloudFront)  
X-Amz-CF-Pop: MAD56-P1  
X-Amz-CF-Id: XJRyx-GwB2eqgY1O6AtIW-R8Z9yqIT5Crx9yrAww0dqtohlWLBXQ==  
Age: 2448  
Response Code: 200  
[Source Code](#)



- Resultados de la página web al buscar el mismo artículo.



- La misma página desde diferentes direcciones IP sobre el compromiso de Gymshark con la sostenibilidad

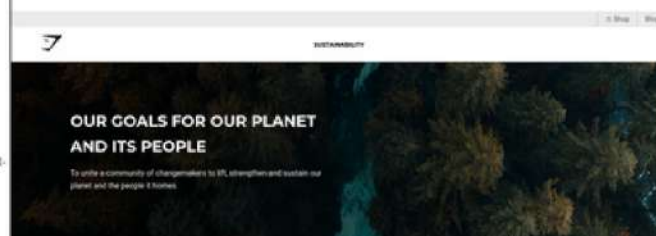
<http://sustainability.gymshark.com>  
Resolved to: 108.157.98.22

Page Title: Home  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked  
Connection: close  
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate  
Content-Security-Policy: frame-ancestors 'self' twitter.com t.co; block-all-mixed-content; script-src 'self' report-sample 'unsafe-inline' 'unsafe-eval' https://.googletagmanager.com https://.googleadservices.com https://.doubleclick.net https://.rmp.rskuten.com https://.ep-mimecast.ads-twitter.com https://.google.com https://analytics.tiktok.com https://content.linkedin.com https://cdn.cookiecutter.org https://googleads.g.doubleclick.net https://google-analytics.com https://googletagmanager.com https://platform.linkedin.com https://static-exp1.lcdn.com https://snap.lcdn.com https://static.ads-twitter.com https://ssl.google-analytics.com https://s.pinimg.com https://t.co https://tagmanager.google.com https://www.google-analytics.com https://www.google.com https://www.googleadmanager.com https://js.adsrvr.org; style-src 'self' report-sample 'unsafe-inline' 'google.com' 'lcdn.com platform.twitter.com' www.googletagmanager.com fonts.googleapis.com; object-src 'googleadsyndication.com; child-src 'self' blob: 'google.com' 'doubleclick.net' 'googleadsyndication.com ct.pinterest.com

<http://sustainability.gymshark.com>  
Resolved to: 108.157.98.52

<http://sustainability.gymshark.com>  
Resolved to: 108.157.98.95

Page Title: Home  
Content-Type: text/html; charset=utf-8



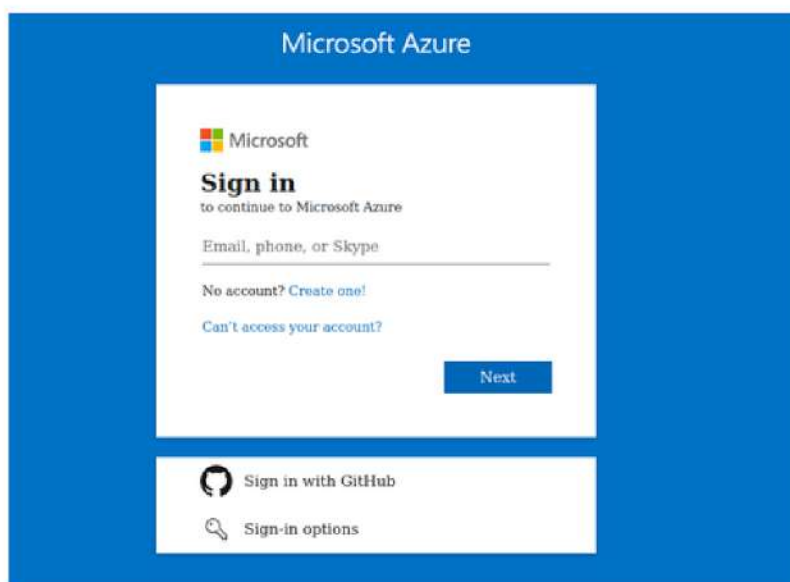


- Nos muestran una página sobre almacenamiento en la nube


<p><a href="http://careerstorm.gymshark.com">http://careerstorm.gymshark.com</a> Resolved to: 178.62.27.199</p> <p><b>Page Title:</b> PHP Stack <b>Server:</b> nginx <b>Date:</b> Tue, 31 Jan 2023 19:10:35 GMT <b>Content-Type:</b> text/html; charset=UTF-8 <b>Transfer-Encoding:</b> chunked <b>Connection:</b> close <b>Vary:</b> Accept-Encoding <b>Response Code:</b> 200</p> <p><a href="#">Source Code</a></p>	
--	--

- Otra página donde no cargó al 100% pero revisandola por nuestra cuenta podemos ver que trata de un formulario para entrar a la cuenta de Microsoft Azure. Donde seguramente administren sus aplicaciones

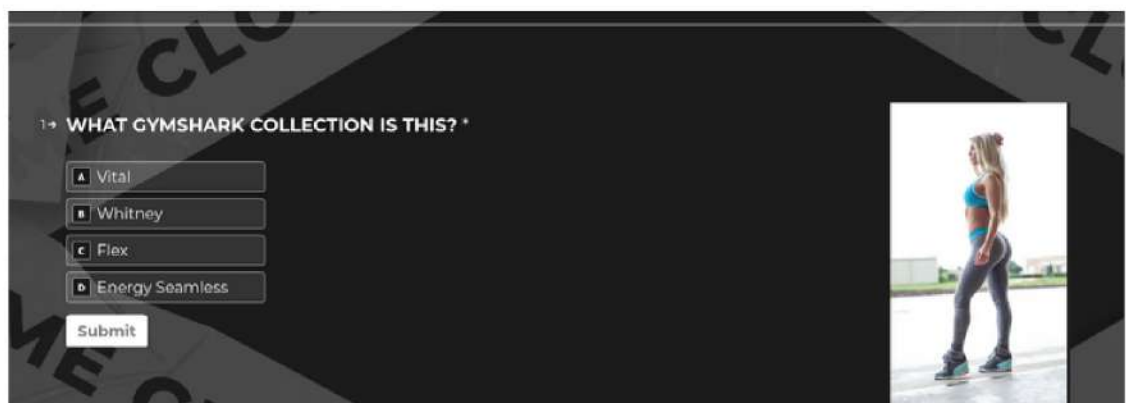
Web Request Info	Web Screenshot
<p><a href="http://enterpriseenrollment.gymshark.com">http://enterpriseenrollment.gymshark.com</a> Resolved to: 20.91.147.72</p> <p><b>Page Title:</b> Sign in to Microsoft Azure <b>Date:</b> Tue, 31 Jan 2023 19:19:41 GMT <b>Content-Type:</b> text/html; charset=utf-8 <b>Content-Length:</b> 29605 <b>Connection:</b> close <b>Cache-Control:</b> no-cache, must-revalidate <b>Pragma:</b> no-cache <b>Expires:</b> -1 <b>ETag:</b> "h6--bhPYdc2V" <b>x-content-type-options:</b> nosniff <b>X-XSS-Protection:</b> 1; mode=block <b>x-ms-version:</b> 10.227.0.1 (production#669ed02851.221205-2257) Signed <b>Strict-Transport-Security:</b> max-age=31536000; includeSubDomains <b>Set-Cookie:</b> browserId=09fb376-8a19-48d5-90d7-014d450da914; domain=intune.microsoft.com; path=/; secure; HttpOnly; SameSite=None <b>Content-Security-Policy:</b> frame-ancestors 'self' <b>X-Frame-Options:</b> SAMEORIGIN <b>Access-Control-Allow-Origin:</b> * <b>Timing-Allow-Origin:</b> * <b>x-ms-content-source:</b> DiskPersistentContentCache</p>	



- Pagina que al entrar por nuestra cuenta y ver más a fondo se ve que es un cuestionario relacionado con el tema fitness y la misma empresa.

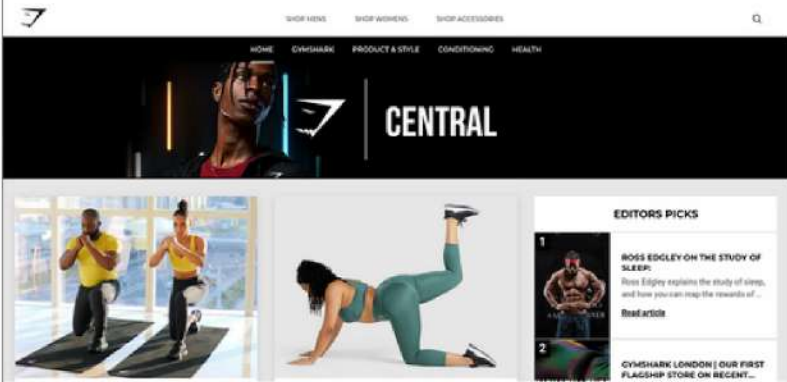
<p><a href="http://tours.gymshark.com">http://tours.gymshark.com</a> Resolved to: 13.33.232.104</p> <p><b>Page Title:</b> The Gymshark Experience <b>Content-Type:</b> text/html <b>Content-Length:</b> 32139 <b>Connection:</b> close <b>Date:</b> Tue, 31 Jan 2023 19:09:02 GMT <b>Last-Modified:</b> Tue, 01 Jun 2021 14:13:50 GMT <b>ETag:</b> "d1b207b8420a057e14ee85ffc10fb3e6" <b>Accept-Ranges:</b> bytes <b>Server:</b> AmazonS3 <b>X-Cache:</b> Hit from cloudfront <b>Via:</b> 1.1 54b7a6e04e496eb001a345a89b73b306.cloudfront.net (CloudFront) <b>X-Amz-Cf-Pop:</b> MAD51-C1 <b>X-Amz-Cf-Id:</b> BaODV4Ex2qTTVb2i8VUJ5YnwCUrvZwg1kX4gWeuFMoo0BDDuh7Kliw== <b>Age:</b> 922 <b>Response Code:</b> 200</p> <p><a href="#">Source Code</a></p>	
--	--

Al ingresar :



- Varias IP hacia la misma pagina

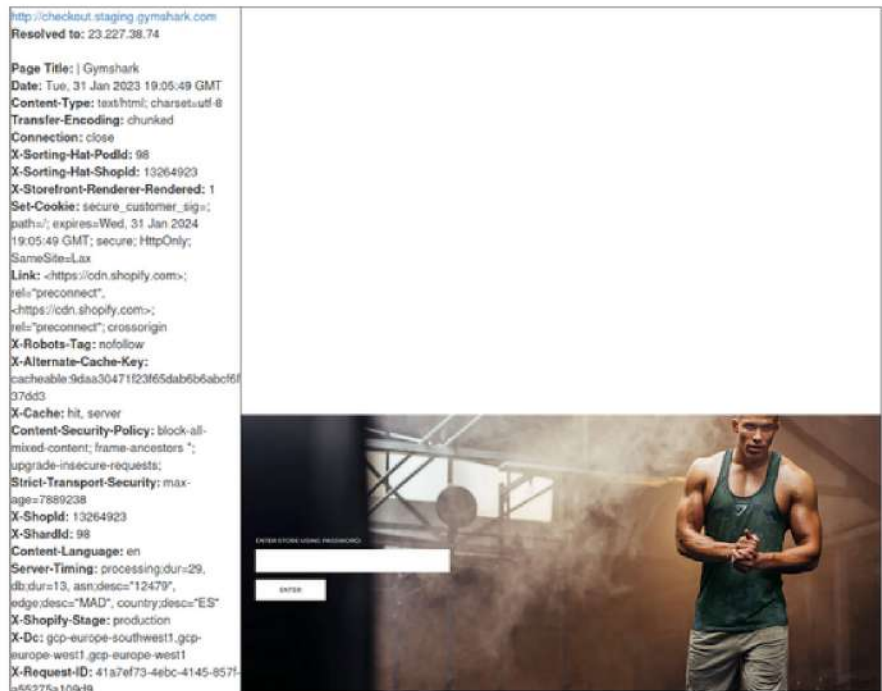
<p><a href="http://www.central.gymshark.com">http://www.central.gymshark.com</a> Resolved to: 18.67.240.88</p> <p><b>Page Title:</b> Gymshark's Official Blog   Gymshark Central <b>Content-Type:</b> text/html; charset=utf-8 <b>Transfer-Encoding:</b> chunked <b>Connection:</b> close <b>Content-Security-Policy:</b> default-src * 'unsafe-inline' 'unsafe-eval'; script-src * 'unsafe-inline' 'unsafe-eval'; connect-src * 'unsafe-inline'; img-src * data: blob: 'unsafe-inline'; frame-src *; style-src * 'unsafe-inline'; <b>Date:</b> Tue, 31 Jan 2023 19:00:40 GMT <b>ETag:</b> "4a061-aNZZ5wZJkP0q7Ulp43FSJMQJ0gc" <b>Permissions-Policy:</b> accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=() <b>Referrer-Policy:</b> same-origin <b>Strict-Transport-Security:</b> max-age=31536000; includeSubDomains; preload <b>X-Content-Type-Options:</b> nosniff <b>X-Frame-Options:</b> DENY <b>X-Powered-By:</b> Next.js <b>X-Xss-Protection:</b> 1; mode=block <b>Vary:</b> Accept-Encoding, Accept-Encoding <b>X-Cache:</b> Hit from cloudfront <b>Via:</b> 1.1</p>	<p><a href="http://central.gymshark.com">http://central.gymshark.com</a> Resolved to: 18.67.240.48</p> <p><b>Page Title:</b> Gymshark's Official Blog   Gymshark Central</p>	<p><a href="http://www.central.gymshark.com">http://www.central.gymshark.com</a> Resolved to: 18.67.240.88</p> <p><b>Page Title:</b> Gymshark's Official Blog   Gymshark Central</p>
--	--	--



- Dos paginas de un mismo juego



- Más formularios donde directamente piden contraseña



- Más de una página con errores internos en el servidor según el texto. Estas de apis

Web Request Info	Web Screenshot
<p><a href="http://api.gymshark.com">http://api.gymshark.com</a> Resolved to: 54.192.95.29</p> <p>Page Title: Unknown Content-Type: application/json Content-Length: 36 Connection: close Date: Tue, 31 Jan 2023 19:20:19 GMT x-amzn-RequestId: 40f050a1-a9c0-40c9-8cc6-147fb2b93be6 Access-Control-Allow-Headers: * x-amzn-ErrorType: InternalServerErrorException x-amzn-arn-id: fn1-RGvYIAMFWRA=</p>	<p>{"message": "Internal server error"}</p>

Los resultados de EyeWitness serán guardados en la carpeta : eyewitnessresults



# WEB APPLICATION FIREWALL — — — — —

## WAFW00F

A continuación se va a intentar detectar firewalls de aplicaciones web, el cual es un tipo específico de cortafuegos que protege contra ataques a aplicaciones web. Esto se hace con la herramienta de WAF00F ya integrada en Kali. Hacemos uso del siguiente comando, ingresando la lista ya hecha de subdominios y pidiendo un output en el archivo txt de "wafresults.txt"

```
(kali@kali)~[~/Desktop/herramientas]
$ wafw00f -i subdomains -o wafresults.txt
```

Se puede ver como las páginas son protegidas con WAFs CloudFront de Amazon y Cloudflare

```
RROR:wafw00f:Site pos.gymshark.com appears to be down
*) Checking https://eu.gymshark.com
+) The site https://eu.gymshark.com is behind Cloudflare (Cloudflare Inc.) WAF.
~) Number of requests: 2
*) Checking https://cdn.gymshark.com
+) The site https://cdn.gymshark.com is behind Cloudfront (Amazon) WAF.
~) Number of requests: 2
*) Checking https://no.gymshark.com
+) The site https://no.gymshark.com is behind Cloudflare (Cloudflare Inc.) WAF.
~) Number of requests: 2
*) Checking https://dev.gymshark.com
+) The site https://dev.gymshark.com is behind Cloudflare (Cloudflare Inc.) WAF.
~) Number of requests: 2
*) Checking https://app.gymshark.com
+) The site https://app.gymshark.com is behind Cloudfront (Amazon) WAF.
~) Number of requests: 2
*) Checking https://dk.gymshark.com
+) The site https://dk.gymshark.com is behind Cloudflare (Cloudflare Inc.) WAF.
~) Number of requests: 2
*) Checking https://ch.gymshark.com
+) The site https://ch.gymshark.com is behind Cloudflare (Cloudflare Inc.) WAF.
~) Number of requests: 2
*) Checking https://u.gymshark.com
+) The site https://u.gymshark.com is behind Cloudfront (Amazon) WAF.
~) Number of requests: 2
*) Checking https://m.gymshark.com
+) The site https://m.gymshark.com is behind Cloudflare (Cloudflare Inc.) WAF.
~) Number of requests: 2
*) Checking https://central.gymshark.com
+) The site https://central.gymshark.com is behind Cloudfront (Amazon) WAF.
~) Number of requests: 2
*) Checking https://info.gymshark.com
RROR:wafw00f:Something went wrong HTTPSConnectionPool(host='info.gymshark.com', port=
```

Los resultados de WAFW00F serán guardados en la carpeta : WAF

## DESCUBRIMIENTO DE TECNOLOGIAS

### WHATWEB

Con esta herramienta y haciendo uso de la segunda lista de subdominios hecha a raíz de las páginas destacadas con EyeWitness podremos obtener información sobre las tecnologías usadas en estas.

```
(kali@kali)-[~/Desktop/herramientas]
$ whatweb -i /home/kali/Desktop/practica/subdomains2.txt > whatweb.txt
```

De aquí se puede sacar información como que los lenguajes utilizados por las aplicaciones son Javascript y Json.

Esto nos servirá para emplearlo en la siguiente herramienta

**Los resultados de WhatWeb serán guardados en la carpeta : whatweb**

## DESCUBRIMIENTO DE DIRECTORIOS

### DIRSEARCH

Para esto se hará uso de **dirsearch**. Las direcciones enseñadas anteriormente en la parte de la herramienta Eyewitness han sido recogidas en una lista aparte para ser mas concretos y usar dirsearch con esta .

Este comando nos ayuda con -l a pasarle un archivo con una lista de dominios. Con -e podemos especificar que extensiones queremos tomando de ayuda el output de whatweb y con -x podemos excluir aquello que no nos interesa en absoluto

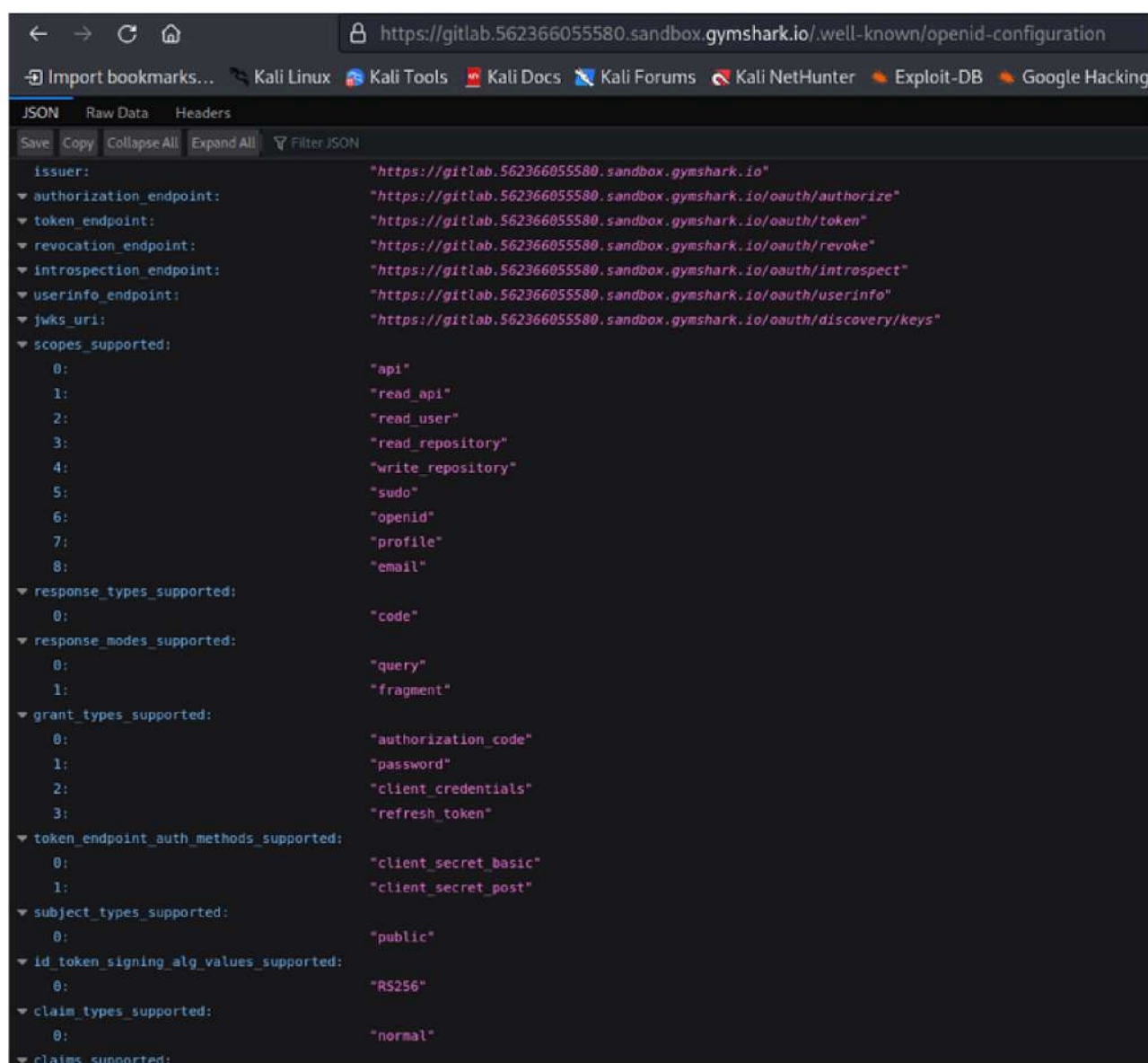
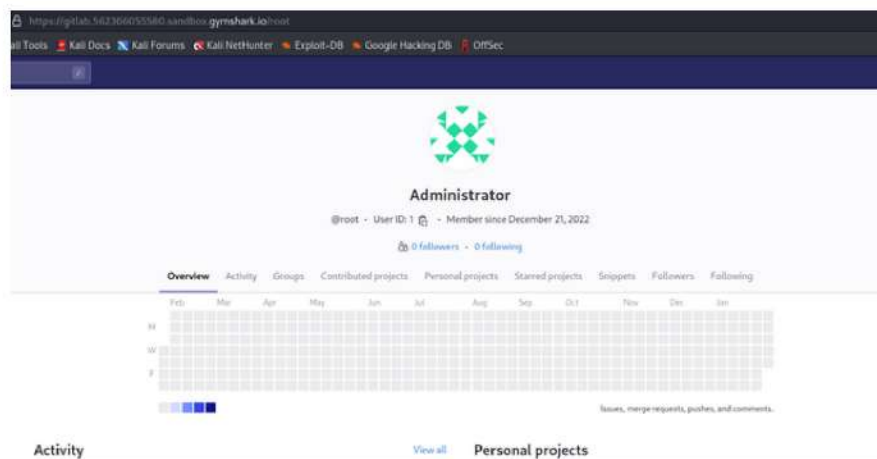
```
(kali@kali)-[~/Desktop/herramientas/dirsearch]
$ python3 dirsearch.py -l /home/kali/Desktop/herramientas/subdomains2.txt -e html,php,json,js,txt -x 301,302,400-499,500-599 -o /home/kali/Desktop/practica/dirsearchresults/dirsearch.txt --full-url
```

Los resultados mostraron unicamente informacion sobre las siguientes direcciones :

```
2
3 200      1KB  http://gitlab.562366055580.sandbox.gymshark.io/.well-known/openid-configuration
4 200      54KB http://gitlab.562366055580.sandbox.gymshark.io/cc
5 200      55KB http://gitlab.562366055580.sandbox.gymshark.io/explore
6 200      70KB http://gitlab.562366055580.sandbox.gymshark.io/help
7 200      70KB http://gitlab.562366055580.sandbox.gymshark.io/help.htm
8 200      70KB http://gitlab.562366055580.sandbox.gymshark.io/help/
9 200     663B http://gitlab.562366055580.sandbox.gymshark.io/public.json
10 200     55KB http://gitlab.562366055580.sandbox.gymshark.io/public/
11 200     55KB http://gitlab.562366055580.sandbox.gymshark.io/public
12 200     57KB http://gitlab.562366055580.sandbox.gymshark.io/public.html
13 200      2KB  http://gitlab.562366055580.sandbox.gymshark.io/robots.txt
14 200     60KB http://gitlab.562366055580.sandbox.gymshark.io/root
15 200     60KB http://gitlab.562366055580.sandbox.gymshark.io/root/
16 200     52KB http://gitlab.562366055580.sandbox.gymshark.io/search.php
17 200    295B http://gitlab.562366055580.sandbox.gymshark.io/search.js
18 200     54KB http://gitlab.562366055580.sandbox.gymshark.io/search.html
19 200     52KB http://gitlab.562366055580.sandbox.gymshark.io/search
20 307     88B  http://preview.staging.gymshark.com/_src → REDIRECTS TO: https://vercel.com/deployments/preview.staging.gymshark.com/source
21
```



Algunos de estos resultados buscados por cuenta propia muestran este tipo de páginas que seguramente deberían ser borradas u ocultas de mejor forma



Los resultados de diresearch serán guardados en la carpeta : dirsearchresults



## ESCANEO DE VULNERABILIDADES

### NUCLEI

Esta herramienta nos ayudará con el escaner de vulnerabilidades. Se empleará contra la segunda lista de subdominios donde estan las paginas que han sido destacadas de eyewitness.

Para formar este comando se ha decidido excluir plantillas de nivel de información esto con **-es**

Con **-pt** se especifica el tipo de templates que se quieren aplicar y pidiendo el output en el archivo nucleireresults

```
(kali@kali)-[~/Desktop/herramientas]
$ nuclei -l subdomains2.txt -es info -pt dns,http,headless,network -o nucleireresults
```

Sólo se ha detectado una cosa y es de categoría desconocida. Aparentemente relacionada con una divulgación de credenciales. En este caso de la página señalada en la imagen.

```
File Edit Search View Document Help
1 [credentials-disclosure] [http] [unknown] https://www.central.gymshark.com/
  ["algoliaApiKey":"0d0ae336234d7b1f9aec8852244f3683",ApiKey":"0d0ae336234d7b1f9aec8852244f3683"]
2
```

**Los resultados de Nuclei serán guardados en la carpeta : Nucleireresults**

### SUBZY

A continuación con Subzy se puede averiguar si alguna de los subdominios de esta segunda lista es vulnerable a un **subdomain takeover**.

Con el siguiente comando

```
(kali@kali)-[~/Desktop/herramientas]
$ subzy run --targets subdomains2.txt
```

```
[ No ] Show only potentially vulnerable subdomains (--hide_fails)
[ NOT VULNERABLE ] - http://careersform.gymshark.com
[ NOT VULNERABLE ] - https://staging1.gymshark.com/password
[ NOT VULNERABLE ] - http://tours.gymshark.com
[ NOT VULNERABLE ] - http://headless.develop.gymshark.com
[ NOT VULNERABLE ] - http://training.staging.gymshark.com
[ NOT VULNERABLE ] - http://enterpriseenrollment.gymshark.com
[ NOT VULNERABLE ] - http://shop.dk.staging.gymshark.com
[ NOT VULNERABLE ] - http://sustainability.gymshark.com
[ NOT VULNERABLE ] - http://features.develop.gymshark.com
[ NOT VULNERABLE ] - http://www.central.gymshark.com
[ NOT VULNERABLE ] - http://teabreak.staging.gymshark.io
[ NOT VULNERABLE ] - http://training.gymshark.com
[ NOT VULNERABLE ] - http://api.gymshark.com
[ NOT VULNERABLE ] - http://2048.develop.gymshark.com
[ NOT VULNERABLE ] - http://gitlab.562366055580.sandbox.gymshark.io
[ NOT VULNERABLE ] - http://preview.staging.gymshark.com
```

Con esto se pudo concluir que ninguno de estos es vulnerable. Sin embargo si quiso hacer la prueba con toda la lista completa subdominios (recordando que hemos estado haciendo esto con los subdominios destacados de eyewitness)

```
[ NOT VULNERABLE ] - events.platform-staging.gymshark.com
[ VULNERABLE ] - link.e-mail.gymshark.com [ Unbounce ]
[ DISCUSSION ] - https://github.com/EdOverflow/can-i-take-over-xyz/issues/11
[ DOCUMENTATION ] - Not available
[ NOT VULNERABLE ] - nsproxy.service.gymshark.io
[ NOT VULNERABLE ] - tableau.gymshark.io
```

```
[ NOT VULNERABLE ] - ablink.e.gymshark.com
[ VULNERABLE ] - link.serviceinfo.gymshark.com [ Unbounce ]
[ DISCUSSION ] - https://github.com/EdOverflow/can-i-take-over-xyz/issues/11
[ DOCUMENTATION ] - Not available
[ NOT VULNERABLE ] - us-sms-opt-in.service.staging.gymshark.com
[ NOT VULNERABLE ] - train.gymshark.com
[ HTTP ERROR ] - testing.gymshark.com
```

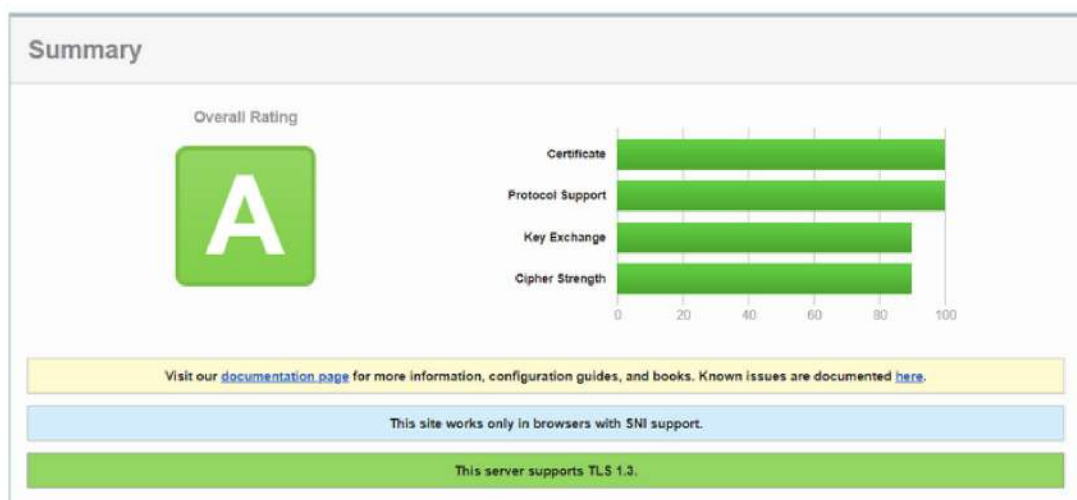
Con esta segunda prueba se pudo ver que **dos subdominios** si son vulnerables a un **subdomain takeover**

Los resultados de Subzy serán guardados en la carpeta : subzyresults

## TESTSSL

Se hace otro análisis pero esta vez respecto a mecanismos de cifrado de aplicaciones . Con esta herramienta y lanzando el siguiente comando se obtiene una calificación A que se puede corroborar en el archivo **testsslresults.csv**

```
(kali@kali)-[~/Desktop/herramientas/testssl.sh]
$ ./testssl.sh --assume-http -iL /home/kali/Desktop/herramientas/subdomains2.txt -oL /home/kali/Desktop/practica/testsslresults2 --csv
#####
```



Los resultados de TESTSSL serán guardados en la carpeta : TESTSSLresults



DESCUBRIMIENTO DE DOCUMENTOS

FOCA

Para este paso, se hará uso del programa FOCA. Se crea un nuevo proyecto indicando los dominios dentro del scope y seleccionaremos el tipo de documentos que queremos sacar y donde queremos que se busque toda esta información:



Se esperaban bastantes resutados pero sorpresivamente han sido pocos. Tratandose los pdf de campañas para los años 2020 , 2021 y 2022. Estos seran adjuntados de igual forma con este documento.

Custom search							Search All
Id	Type	URL	Download	Download Date	Size	Metadata	
0	pdf	https://careers.gymshark.com/Assessment-Centre-Guide...	✗	-	36.9 KB	✗	
1	pdf	https://cdn.gymshark.com/projects/transparency-report/...	✗	02/01/2023 14:58:51	10.84 MB	✗	
2	pdf	https://cdn.gymshark.com/projects/transparency-report/...	✗	-	12.32 MB	✗	
3	pdf	https://cdn.gymshark.com/projects/transparency-report/...	✗	-	109.39 KB	✗	
4		https://www.gymshark.com/	✗	-	-	✗	
5		https://eu.gymshark.com/	✗	-	-	✗	
6		https://www.gymshark.com/pages/about-us	✗	-	-	✗	

En la ultima parte de estos documentos, podemos ver los nombres de sus proveedores, junto a sus direcciones clasificado todo ( suponiendo) por colecciones.

AW20

SUPPLIER NAME	SUPPLIER ADDRESS	FACTORY NAMES	FA
MAS	231, NAWALA ROAD, NUGEGODA	MAS Active (Private) Limited - Sleekline	Plo Col
MAS	231, NAWALA ROAD, NUGEGODA	MAS Active (Private) Limited - Kreedo Intimo	LO1 em
MAS	231, NAWALA ROAD, NUGEGODA	MAS Active (Private) Limited - Contourline Division	BOI
MAS	231, NAWALA ROAD, NUGEGODA	MAS Active (Private) Limited - Asialine Division	THI
MAS	231, NAWALA ROAD, NUGEGODA	MAS Fabrics (PVT) Ltd - Matrix	MA Sri
Prime Source Enterprise Ltd.	Unit 824, Fuxin International Building, #359 Hongwu Rd., Nanjing, China, 210001	Zhejiang Bangjie Digital Knitting Share Co. Ltd	Sou ind
J.M. Fabrics Ltd. (New Asia)	SOUTH NAYA PARA 6 DOGRI, BHAWAL MIRZAPUR, GAZIPUR Bangladesh	J.M. Fabrics Ltd.	Sou pur
RT Knits Ltd	Peupliers Avenue, Pointe aux Sables 11123, Rep of Mauritius.	RT Knits Ltd.	Peu of B
Beachwear Exports Co. Ltd.	ROYAL ROAD, BELLE ETOILE, BEAU BASSIN, MAURITIUS	Beachwear Exports Co. Ltd.	ROF RIT
Sabrina Fashion Industrial Corporation	9F, NO207-5, 3 SECTION BEIXIN ROAD, XINDIAN DIST. NEW TAIPEI CITY, TAIWAN	Top Summit Garment Inc.	Nat Kar
Sintex International Ltd. (Sports City International Inc.)	11F, No.585, Ruiguang Rd., Neihu Dist., Taipei City, Taiwan, R.O.C	Metro Wear Incorporated	Bio Eco Phi
Sintex International Ltd. (Sports City International Inc.)	11492 台北市內湖區瑞光路585號11F	Feeder Apparel Corporation	Bio Eco Phi



FACTORY ADDRESS	COUNTRY
Plot 08 Mepp, Malwatta, Nittabuwa , western, Colombo , Sri Lanka	Sri Lanka
LOT 49, 49A, 58 & 59, B.E.P.Z, WALGAMA, Western, Colombo, Sri Lanka	Sri Lanka
BOI Industrial Park, Pallekale, Kandy, Sri Lanka	Sri Lanka
THORAKOLAYAYA ,MIDDENIYA, SOUTHERN	Sri Lanka
MAS Fabric Park, Kurunegala Road, Thulhiriya, Sri Lanka	Sri Lanka
South section,suxi town,yiwu, Zhejiang province,China	China
South Naya Para 6 Dogri, Bhawal Mirzapur, Gazipur, Dhaka, Bangladesh	Bangladesh
Peupliers Avenue, Pointe aux Sables 11123, Rep. of Mauritius.	Mauritius
ROYAL ROAD, BELLE ETOILE, BEAU BASSIN,MAURITIUS	Mauritius
National Road #4, Phum Trapaing Toul, Khum Kambol, Ang Snoul District	Cambodia
Block C-6, 2nd Avenue Corner 5th Street, Mactan Economic Zone 1, Lapu Lapu City, Cebu, 6015, Philippines	Philippines

Los resultados de FOCA serán guardados en la carpeta : focaresults

## ANÁLISIS DE SERVIDORES DE CORREO

### DMARCIAN

Aquí se a podido realizar un análisis de correo a los ambos dominios dentro del scope. Uno de ellos fue totalmente satisfactorio y el otro no tanto. Se puede ver que no cuentan con SPF en uno de ellos.

**Well done! Your domain is protected against abuse by phishers and spammers**

Receivers are able to reliably separate and block fraudulent emails that mimic your email domain from your authentic emails. We can offer dedicated support to help manage DMARC-related incidents, regular data reviews, monitor ongoing compliance and help embed DMARC into your daily operations.

**DMARC**

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

+ [Details](#)

**SPF**

Your domain has a valid SPF record and the policy is sufficiently strict.

+ [Details](#)

**DKIM**

Your DKIM record is valid.

+ [Details](#)

narcian

SOLUTIONSRESOURCESPRICINGPARTNERSABOUT

SIGN UP / LOGIN

DOMAIN AUDIT

gymshark.io

CHECK DOMAIN

Well done! Your domain is protected against abuse by phishers and spammers

Receivers are able to reliably separate and block fraudulent emails that mimic your email domain from your authentic emails. We can offer dedicated support to help manage DMARC-related incidents, regular data reviews, monitor ongoing compliance and help embed DMARC into your daily operations.

GET STARTED

✓ DMARC

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

+ Details

✗ SPF

Your domain does not have a SPF record.

✗ DKIM

We couldn't find a DKIM record associated with your domain. If you know the correct selector, you can scan for the DKIM record:

Enter selector

## OSINT

### HUNTER.IO

Dentro de esta plataforma se han podido conseguir 9 correos diferentes que sean parte de la empresa. En esta busqueda usando "gymshark.com" . Por parte de "gymshark.io" no han habido resultados


9 results for your search		Export	Find by name
Stephanie Oneill s.oneill@gymshark.com	99%	Save as lead	2 sources
pts@gymshark.com	98%	Save as lead	1 source
s.varma@gymshark.com	98%	Save as lead	1 source
mydata@gymshark.com	97%	Save as lead	20+ sources

support@gymshark.com	Support	Save as lead	20+ sources ▾
workex@gymshark.com		Save as lead	2 sources ▾
corporate@gymshark.com	Management	Save as lead	20+ sources ▾
socialcomps@gymshark.com		Save as lead	20+ sources ▾
affiliates@gymshark.com		Save as lead	1 source ▾


## REDES SOCIALES



Por medio de LinkedIn se hizo una búsqueda en primera instancia de trabajadores en general de Gymshark

Aproximadamente 1.900 resultados




**Miembro de LinkedIn**  
Talent and People Intern at Gymshark | BSc (Hons) Psychology student at University of Leicester  
Reino Unido  
Actual: Talent and People Student Placement en **Gymshark**




**Ben Francis MBE** • 3er y demás   
CEO & Founder of Gymshark.  
Midlands Occidentales  
Habla sobre #fitness, #business y #entrepreneurship  
 448 mil seguidores


[Seguir](#)




**Miembro de LinkedIn**  
Executive Assistant at Gymshark  
Reino Unido  
Actual: Executive Assistant to CPO, CSCO and CCO en **Gymshark**



**Miembro de LinkedIn**  
Engineering Director @ Gymshark  
Solihull  
Actual: Engineering Director en **Gymshark**




**Miembro de LinkedIn**  
Junior Front End Engineer at Gymshark  
Midlands Occidentales  
Actual: Junior Front End Engineer en **Gymshark**




**Miembro de LinkedIn**

Bastantes resultados pero poca información







**Miembro de LinkedIn**  
 Brand Partnerships Executive (Global) at Gymshark  
 Reino Unido  
 Actual: Brand Partnerships Executive (Global) en Gymshark




**Miembro de LinkedIn**  
 Head of Design (brand) at Gymshark  
 Leighton Buzzard  
 Actual: Head Of Design en Gymshark



**Miembro de LinkedIn**  
 Accessories Sourcing at Gymshark  
 Midlands Occidentales  
 Actual: Sourcing Lead - Accessories en Gymshark






**Miembro de LinkedIn**  
 Chief Technology Officer at Gymshark  
 Solihull  
 Actual: Chief Technology Officer en Gymshark



**Miembro de LinkedIn**  
 Creative Producer at Gymshark  
 Londres  
 Actual: Creative Producer en Gymshark


Siendo más específicos, buscando directores, se pudieron recoger dos nombres :





**Ben Francis MBE** • 3er y demás   
 CEO & Founder of Gymshark.  
 Midlands Occidentales  
 Habla sobre #fitness, #business y #entrepreneurship  
 448 mil seguidores

Actual: Engineering Director en Gymshark

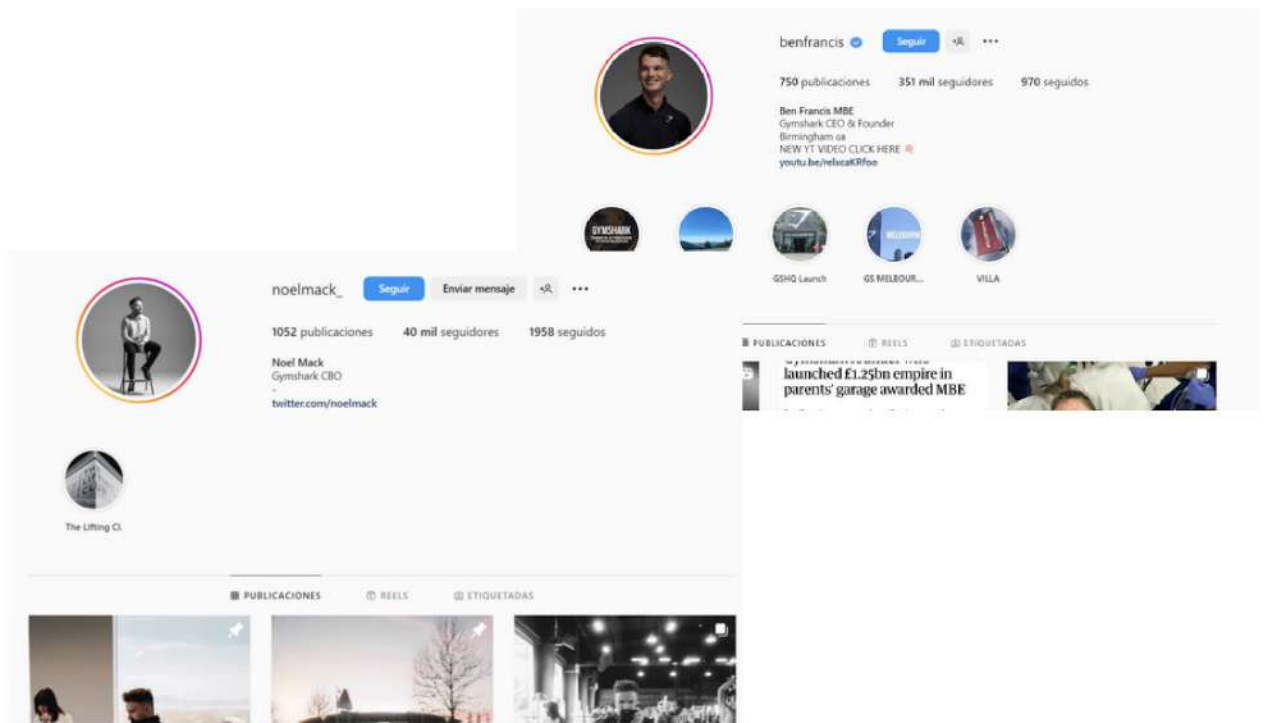
[Seguir](#)



**Noel Mack** • 3er y demás   
 Chief Brand Officer at Gymshark | 2022 Adweek CMO  
 Birmingham  
 Habla sobre #brand, #culture, #community, #ecommerce y #marketing  
 97 mil seguidores

[Seguir](#)

Ambos se buscaron en otras redes sociales como Instagram, Twitter y Facebook. Se encontraron ambas cuentas de Instagram.



Ambas cuentas de twitter y por parte de Facebook unicamente páginas, mas no cuentas personales

