

INFORME SMULE.COM

Versión: 1.0

Fecha: 09/03/2025

Autor: Rafael Figueroa

Índice

1. Introducción	3
2. Footprinting	4
3. Fingerprinting	12
4. Análisis de vulnerabilidades	19
5. OSINT	26

1.- Introducción

Smule, Inc. es una empresa estadounidense especializada en el desarrollo de aplicaciones móviles centradas en la creación y colaboración musical. Fundada en 2008 por Jeff Smith y Ge Wang, profesor asistente en la Universidad de Stanford, la compañía tiene su sede en Salt Lake City, Utah. Su misión es facilitar la expresión musical y fomentar la interacción social a través de experiencias digitales innovadoras.

Smule ha desarrollado diversas aplicaciones que permiten a los usuarios interactuar con la música de manera creativa. Entre las más destacadas se encuentran:

- **Smule** (anteriormente Sing! Karaoke): Lanzada en 2012, esta aplicación permite a los usuarios interpretar canciones en solitario o en colaboración con otros, incluidos artistas internacionales. Ofrece herramientas de mejora vocal y efectos audiovisuales para enriquecer la experiencia del usuario.
- **Magic Piano**: Una aplicación que simula la ejecución de un piano virtual, facilitando la interpretación de piezas musicales con una interfaz intuitiva.
- **AutoRap**: Permite transformar frases habladas en raps sincronizados con bases musicales preestablecidas.

En 2018, Smule introdujo LiveJam, una funcionalidad que posibilita la interpretación en tiempo real con otros usuarios a nivel global. Asimismo, en 2020 lanzó Styles, una herramienta de personalización que combina filtros de audio y video para optimizar las presentaciones.

Desde su fundación, Smule ha experimentado un crecimiento sostenido. En 2018, recaudó 74 millones de dólares en una ronda de financiamiento liderada por Tencent y Times Bridge, lo que fortaleció su expansión internacional. La empresa ha establecido colaboraciones con reconocidas marcas y franquicias, como Disney, permitiendo a los usuarios participar en duetos con personajes animados en canciones icónicas.

Smule ha sido reconocida por su capacidad de conectar a personas a través de la música, contando con más de 50 millones de usuarios activos mensuales. Su plataforma ha sido elogiada por su accesibilidad y por brindar una oportunidad para que músicos y aficionados expresen su creatividad en un entorno digital colaborativo.

Smule, Inc. se ha consolidado como un referente en la industria de las aplicaciones musicales, combinando tecnología e innovación para transformar la manera en que las personas interactúan con la música. Gracias a su enfoque en la colaboración social y la mejora continua de sus herramientas, la empresa continúa expandiendo su presencia global y fortaleciendo su comunidad de usuarios.

2.- FOOTPRINTING

2.1 DNS Brute-Force

```
(kali㉿kali)-[~]
$ cd recopilacion

(kali㉿kali)-[~/recopilacion]
$ cd lists

(kali㉿kali)-[~/recopilacion/lists]
$ resolvlist -o resolvers.txt
No DNS server source file or URL provided. Using default public DNS list.
Checking 474 of 62790 DNS servers. Results: 138 valid - 336 non-valid DNS servers. 0.75% completed.

Home
```

```
(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ shuffledns -mode brute-force -d smule.com -w /home/kali/recopilacion/lists/domains.txt -r /home/kali/recopilacion/lists/resolvers.txt -silent > shuffledns.txt

(kali㉿kali)-[~/recopilacion/smule.com/0218]
```

Tras realizar esta técnica se comprueba el archivo shuffledns.txt, en el mismo aparecen 66 subdominios, a continuación se enumeran los más destacados:

- **api.smule.com**: Endpoint principal de la API de Smule, utilizado por la web y la aplicación para interactuar con la plataforma (autenticación, carga de datos, etc.).
- **app.smule.com**: Este dominio podría ser el acceso para las aplicaciones móviles o interacciones relacionadas con la app de Smule.
- **email.smule.com**: Se utiliza para gestionar correos electrónicos enviados desde la plataforma Smule (como notificaciones o confirmaciones).
- **static1.smule.com / static2.smule.com / static3.smule.com**: Estos son subdominios probablemente destinados a alojar contenido estático, como imágenes, videos o archivos JavaScript utilizados por el sitio web.
- **status.smule.com**: Subdominio utilizado para mostrar el estado de la plataforma, si está funcionando correctamente o si hay interrupciones en el servicio.
- **forum.smule.com**: Es probable que sea la sección del foro de Smule, donde los usuarios pueden interactuar, discutir y resolver problemas.
- **dev.smule.com / developers.smule.com**: Subdominios relacionados con los desarrolladores, probablemente proporcionando documentación sobre cómo interactuar con la API de Smule o herramientas para crear aplicaciones compatibles.

- **jira.smule.com**: Usado para gestión de proyectos internos y seguimiento de incidencias (probablemente relacionado con el sistema de tickets y gestión de bugs).
- **care.smule.com**: Posiblemente dedicado al soporte al cliente o asistencia técnica.
- **blog.smule.com**: Para acceder a contenido de blog oficial de Smule, como novedades, tutoriales y actualizaciones.

2.2 Google Analytics



```
(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ analyticsrelationships --url https://www.smule.com > analytics.txt
/usr/bin/analyticsrelationships:34: SyntaxWarning: invalid escape sequence '\d'
    pattern = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:47: SyntaxWarning: invalid escape sequence '\.'
    pattern = "(www\.googletagmanager\.com/ns\.html\?id=[A-Z0-9\-\_]+)"
/usr/bin/analyticsrelationships:49: SyntaxWarning: invalid escape sequence '\d'
    pattern3 = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:78: SyntaxWarning: invalid escape sequence '\-'
    pattern = "/relationships/[a-z0-9\-\_\.]+\.[a-z]+"

> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar

[+] Analyzing url: https://www.smule.com
[-] Tagmanager URL not found
```

The terminal window shows the output of the 'analyticsrelationships' tool. It lists several syntax warnings related to regular expression patterns. Below this, it provides instructions for using the tool, its Python version, and credits to the author (@JosueEncinar). At the bottom, it shows the analysis of the URL 'https://www.smule.com' and notes that a Tagmanager URL was not found.

Tras ejecutar la herramienta `analyticsrelationships` no se obtienen resultados sobre el uso de Google Analytics

2.3 TLS Probing

```
(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ cero -d smule.com > cero.txt
```

Tras ejecutar la herramienta `cero` se comprueba el archivo `cero.txt`, el cual está en blanco, lo que indica que `smule.com` no tienen subdominios asociados en el certificado SSL/TLS

2.4 Web Scraping

```
(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ echo smule.com | katana -jc -o katanaoutput.txt -kf robotstxt,sitemapxml

projectdiscovery.io

[INF] Started standard crawling for ⇒ https://smule.com
https://www.smule.com/profile/unblock
https://www.smule.com/s/performance/
https://www.smule.com/password_reset
https://www.smule.com/s/playlist_json
https://www.smule.com/profile/block
https://www.smule.com/s/js-log
https://www.smule.com/profile/is_blocked
https://www.smule.com/
https://www.smule.com/user/
https://www.smule.com/activate
https://w1-fa.cdn.smule.com/assets/react/not_found-e2928451f3666a45ffd92a4d4161fd88.js
https://w1-fa.cdn.smule.com/assets/react/9544-cc6100663fea0739fe29a38c9bbedb4b.js
https://w1-fa.cdn.smule.com/assets/react/1530-5ddaf0b3bb08566c9f772c158dc16ff5.js
https://w1-fa.cdn.smule.com/assets/react/main-7a482466061c24001f021f7291ba6a56.js
https://w1-fa.cdn.smule.com/assets/react/632-65ff3b9725cbdae5878da1cda0ddf382.js
https://w1-fa.cdn.smule.com/assets/react/server_error-3cafaef2cde98f27b09cad6f91305533.js
http://www.smule.com/jobs
https://www.smule.com/forum/
https://w1-fa.cdn.smule.com/assets/main-react/main-af48bfa94a6001d4b1df138fc70b3e84.js
https://w1-fa.cdn.smule.com/assets/main-react/9544-cc6100663fea0739fe29a38c9bbedb4b.js
https://w1-fa.cdn.smule.com/assets/main-react/632-65ff3b9725cbdae5878da1cda0ddf382.js
https://w1-fa.cdn.smule.com/assets/main-react/1530-5ddaf0b3bb08566c9f772c158dc16ff5.js
https://w1-fa.cdn.smule.com/assets/main-react/4979-7bcc918553bb190b22ac6c999a76da2f.js
https://w1-fa.cdn.smule.com/assets/react/5061-e12dae8b49aab60f71d7e405666e764e.js
https://w1-fa.cdn.smule.com/assets/react/3915-55508f9839931d71c3a9f1ddab0d6a68.js
https://www.smule.com/jobs
https://w1-fa.cdn.smule.com/assets/react/4979-7bcc918553bb190b22ac6c999a76da2f.js
https://www.smule.com/recording/faouzia-john-legend-minefields/2390267296_3953346364
https://www.smule.com/recording/faouzia-john-legend-minefields/2390267296_3953346364/frame/box
https://www.smule.com/search?q=
https://w1-fa.cdn.smule.com/assets/main-react/main-af48bfa94a6001d4b1df138fc70b3e84.js
https://www.smule.com/user/register
https://www.smule.com/search?q=[search_term_string]
https://smule.com

(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ cat katanaoutput.txt | unfurl --unique domains > katana.txt
```

Después de ejecutar la herramienta **katana** y depurar el archivo de salida **katana.txt** para eliminar información irrelevante, se identifica un nuevo dominio: **w1-fa.cdn.smule.com**. Este dominio forma parte de la Content Delivery Network (CDN) de Smule, una red de servidores distribuidos geográficamente diseñada para optimizar la entrega de contenido estático, como imágenes, audios, videos y otros archivos esenciales para la aplicación.

Las CDN mejoran el rendimiento y la experiencia del usuario al reducir la latencia y distribuir el contenido desde servidores cercanos al usuario. Esto agiliza la carga de archivos, disminuye la presión sobre los servidores principales y ofrece beneficios adicionales como mayor disponibilidad, mitigación de ataques DDoS y optimización del ancho de banda, aspectos clave para aplicaciones con alto tráfico como Smule.

2.5 Certificate Transparency Logs

```
[kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ ctfr -d smule.com > ctfr.txt
/usr/bin/ctfr:27: SyntaxWarning: invalid escape sequence '\\ '
  b = ''
/usr/bin/ctfr:40: SyntaxWarning: invalid escape sequence '\\.'
  return re.sub('.*www\\.', '', target, 1).split('/')[0].strip()
/usr/bin/ctfr:40: DeprecationWarning: 'count' is passed as positional argument
  return re.sub('.*www\\.', '', target, 1).split('/')[0].strip()

[kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ ctfr-org -d smule > ctfr_org.txt
/usr/bin/ctfr-org:27: SyntaxWarning: invalid escape sequence '\\ '
  b = ''
/usr/bin/ctfr-org:40: SyntaxWarning: invalid escape sequence '\\.'
  return re.sub('.*www\\.', '', target, 1).split('/')[0].strip()
/usr/bin/ctfr-org:40: DeprecationWarning: 'count' is passed as positional argument
  return re.sub('.*www\\.', '', target, 1).split('/')[0].strip()

[kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ cat ctfr.txt | unfurl --unique domains > ctfr_limpio.txt
0218
[kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ cat ctfr_org.txt | unfurl --unique domains > ctfr_org_limpio.txt

[kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ █
0219
```

Después de ejecutar la herramienta **ctfr** en ambas modalidades y depurar los archivos generados, se han obtenido un total de 14 resultados. A continuación, se enumeran y describen aquellos que no habían aparecido previamente y que se consideran relevantes:

- **registry.smule.com**: Relacionado con el registro y autenticación de usuarios, almacenamiento de perfiles o administración de datos en la plataforma.
- **j-int.smule.com**: Dominio interno para pruebas o integración interna de sistemas de Smule.
- **registry-test.smule.com**: Dominio interno para pruebas del sistema de registro, utilizada en entornos de desarrollo o control de calidad.
- **c-t1.cdn.gcp.smule.com / c-t2.cdn.gcp.smule.com / c-t3.cdn.gcp.smule.com / c-t4.cdn.gcp.smule.com**: Subdominios de una CDN alojada en Google Cloud Platform (GCP), usados para la distribución de contenido multimedia o archivos estáticos con balanceo de carga.
- **c-int.cdn.gg.smule.com**: Nodo interno de CDN en Google Cloud específico para ciertas regiones o propósitos internos.
- **c-stg.cdn.gg.smule.com**: "stg" suele referirse a "staging", lo que indica que este dominio es para pruebas antes de implementar cambios en producción.

2.6 Archivos web y caché

```
[kali㉿kali)-[~/recopilacion/smule.com/0218]
$ gau --threads 5 smule.com --o gauoutput.txt
WARN[0000] error reading config: Config file /home/kali/.gau.toml not found, using default config
[kali㉿kali)-[~/recopilacion/smule.com/0218]
$ cat gauoutput.txt | unfurl --unique domains > gau.txt
[kali㉿kali)-[~/recopilacion/smule.com/0218]
$
```

Tras ejecutar la herramienta **gau** y depurar el archivo correspondiente, se obtienen 46 subdominios, se procede a enumerar los más destacados:

- **web.smule.com**: Subdominio alternativo a la versión principal de www.smule.com.
- **link.smule.com**: Utilizado para redireccionamiento de enlaces dentro de Smule (ej. compartir canciones o perfiles).
- **tracking.smule.com**: Utilizado para seguimiento y análisis de usuarios (ej. interacciones, métricas de uso, publicidad).
- **sing.oauth.smule.com**: Relacionado con el sistema de autenticación OAuth de Smule para inicios de sesión en su aplicación.
- **api-sing.smule.com / api-autorap.smule.com / api-piano.smule.com / api-iris.smule.com / api-beta.smule.com**: Son versiones específicas de la API para diferentes aplicaciones o pruebas (por ejemplo, Sing! Karaoke, AutoRap, Piano, Iris).
- **m.smule.com**: versión móvil o ligera del sitio web de Smule.
- **khush.smule.com**: Khush fue una startup de música adquirida por Smule en 2011, por lo que este dominio podría estar relacionado con su integración.
- **ocarina.smule.com / glee.smule.com / tpain.smule.com / iamtpain.smule.com**: Relacionados con antiguas aplicaciones de Smule, como Ocarina, Glee Karaoke y T-Pain's Auto-Tune app.
- Subdominios de **prueba, desarrollo o promociones** como: www-beta.smule.com / www-int.smule.com / www-staging.smule.com / blog-test.smule.com / blog-new.smule.com / link-test.smule.com / superbowl.smule.com

2.7 Permutaciones

```
[kali㉿kali)-[~/recopilacion/smule.com/0218]
$ cat analytics.txt cero.txt katana.txt shuffledns.txt gau.txt ctfr_org_limpio.txt ctfr_limpio.txt > subdominios.txt

[kali㉿kali)-[~/recopilacion/smule.com/0218]
$
```

Una vez generadas las permutaciones de los resultados de las anteriores herramientas unidos, obtenemos 45 subdominios validados por **alterx**, que volvemos a unir a los obtenidos anteriormente, **para llegar a un total de 96 subdominios**, e iniciar la fase de **fingerprinting** con la herramienta **httpx**, se procede a enumerar la relación final de subdominios destacados activos a fecha de **24 de febrero de 2025** con una breve explicación de su función.

```
[kali㉿kali)-[~/recopilacion/smule.com/0224]
$ cat subdominios.txt alterx.txt > subdominios_def.txt

[kali㉿kali)-[~/recopilacion/smule.com/0224]
$ cat subdominios_def.txt | httpx -silent > subdominios_vivos.txt

[kali㉿kali)-[~/recopilacion/smule.com/0224]
$ cat subdominios_vivos.txt | unfurl --unique domains > subdominiosfinal.txt

[kali㉿kali)-[~/recopilacion/smule.com/0224]
$ for subdominio in $(cat subdominiosfinal.txt); do dig +short $subdominio | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}'; done > subdominiosfinal_ips.txt

[kali㉿kali)-[~/recopilacion/smule.com/0224]
$ █
```

Subdominios de API y Backend

- **api.smule.com / api1.smule.com / api2.smule.com / api4.smule.com / api5.smule.com:** APIs principales utilizadas por la plataforma para interactuar con la aplicación y los servicios.
- **api-iris.smule.com / api-piano.smule.com / api-autorap.smule.com:** APIs específicas para ciertas aplicaciones o características dentro de Smule.
- **api-staging.smule.com / api-beta.smule.com:** Versiones de prueba o preproducción de la API antes de implementarse en producción.

Subdominios de Contenidos y CDN

- **c-fa.cdn.smule.com / c-sf.smule.com / c-sg.smule.com:** Subdominios CDN (Content Delivery Network) para la distribución de contenido multimedia.
- **c-t1.cdn.gcp.smule.com / c-t2.cdn.gcp.smule.com / c-t3.cdn.gcp.smule.com / c-t4.cdn.gcp.smule.com:** Servidores en la nube de Google Cloud Platform utilizados para la entrega de contenido.
- **legacy.cdn.smule.com:** Posiblemente una versión anterior del CDN utilizada para archivos antiguos.

Subdominios Administrativos y de Desarrollo

- **admin.smule.com / admin-test.smule.com:** Portal de administración interna.
- **git.smule.com:** Servidor de control de versiones para desarrollo de software.
- **ftp.smule.com:** Posible servidor FTP para transferencias de archivos.
- **tracking.smule.com:** Seguimiento de datos analíticos y métricas de uso.

Subdominios de Aplicaciones y Servicios Específicos

- **ocarina.smule.com / ocarina-app.smule.com:** Relacionados con la app Ocarina de Smule.
- **iamtpain.smule.com / iamtpain-test.smule.com / iamtpain-staging.smule.com:** Vinculados a la aplicación "I Am T-Pain".
- **glee.smule.com / glee-test.smule.com / glee-staging.smule.com / glee-app.smule.com:** Conectados con la aplicación de "Glee Karaoke".
- **tpain.smule.com:** Otro dominio posiblemente relacionado con la app de T-Pain.

Subdominios Web y de Marketing

- **www.smule.com:** Página principal de Smule.
- **blog.smule.com:** Blog oficial de Smule.
- **forum.smule.com:** Foro de la comunidad.
- **links.marketing.smule.com / link.smule.com / link-test.smule.com:** Enlaces de marketing y promoción.
- **corp.smule.com:** Posible sitio corporativo o institucional.

Subdominios de Testing y Desarrollo

- **test.cdn.smule.com / w1-beta.smule.com / w1-fa-beta.cdn.smule.com:** Servidores de prueba y desarrollo.
- **www-test.smule.com / www-beta.smule.com / www-staging.smule.com:** Versiones en prueba de la página principal.

Subdominios Relacionados con Infraestructura

- **status.smule.com:** Posiblemente un panel de estado del servicio.
- **s.smule.com / s1.smule.com / s2.smule.com / s3.smule.com / s4.smule.com:** Servidores de recursos o almacenamiento.
- **s-beta.smule.com:** Versión beta de los servidores de almacenamiento.
- **w1.smule.com / w2.smule.com:** Servidores web principales.

2.8 Shodan

www.smule.com

IP Address	205.143.41.226
Hostname(s)	smule.com api2.oak.smle.co
Tags	eol-product
Vulnerabilities	CVE-2023-44487, CVE-2021-23017, CVE-2021-3618

Open Ports

80 443

Mediante esta extensión se localiza el dominio **api2.oak.smle.co**, este subdominio parece ser parte de la infraestructura de API de Smule, encargada de gestionar solicitudes entre la aplicación y sus servidores.

Possible Function

- api2 indica que puede ser una segunda versión de la API o una instancia específica para ciertas funciones.
- oak podría referirse a una ubicación geográfica (como Oakland) o a un nodo dentro de la red de servidores de Smule.
- smle.co es una variante del dominio principal, usada posiblemente para servicios internos o distribución de contenido.

3.- FINGERPRINTING

3.1 Escaneo de puertos y servicios

```
(kali㉿kali)-[~/recopilacion/smule.com/0224]
$ sudo masscan --top-ports 1000 -il subdominiosfinal_ips.txt
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-02-24 13:14:01 GMT
Initiating SYN Stealth Scan
Scanning 58 hosts [1000 ports/host]
Discovered open port 80/tcp on 52.51.23.169
Discovered open port 443/tcp on 167.89.115.56
Discovered open port 80/tcp on 151.101.194.132
Discovered open port 80/tcp on 205.143.41.229
Discovered open port 443/tcp on 167.89.115.78
Discovered open port 5280/tcp on 205.143.41.223
Discovered open port 443/tcp on 167.89.115.61
Discovered open port 80/tcp on 167.89.123.90
```

Tras ejecutar la herramienta **masscan** se comprueba que los siguientes puertos se encuentran abiertos:

- **80 (HTTP)**: Se usa para la comunicación web sin cifrar. Si está abierto, probablemente haya un servidor web en ejecución (como Apache o Nginx).
- **443 (HTTPS)**: Se usa para la comunicación web cifrada con SSL/TLS. Indica que un servidor web seguro está activo.
- **5280 (XMPP HTTP Binding - BOSH)**: Este puerto está asociado con servidores de mensajería instantánea que usan el protocolo XMPP (Jabber). Se usa para conexiones HTTP a un servidor XMPP.
- **5222 (XMPP Client Connection)**: Es el puerto estándar para conexiones de clientes XMPP a servidores de mensajería instantánea.
- **10002**: Este no es un puerto estándar, pero es comúnmente usado por aplicaciones personalizadas o servicios específicos. Puede estar relacionado con juegos en línea, cámaras de seguridad, servicios IoT o software interno.

3.2 Identificación tecnologías web

En la siguiente captura de **Wappalyzer** se muestran todas las tecnologías utilizadas por smule, como se aprecia si utiliza Google Analytics. El resultado negativo por parte de la herramienta **analyticsrelationships**, utilizada anteriormente, puede ser debido al uso en modo ofuscado de Google Analytics.

The screenshot shows the Wappalyzer interface with the following detected technologies:

- Analytics**: Facebook Pixel, Google Analytics GA4, Adjust
- Web servers**: Nginx 1.18.0
- Programming languages**: Ruby 50% sure
- JavaScript frameworks**: styled-components 5.3.5, React
- Payment processors**: PayPal
- Tag managers**: Google Tag Manager
- Development**: styled-components 5.3.5
- Web frameworks**: Ruby on Rails
- JavaScript libraries**: core-js 3.8.0
- Miscellaneous**: HTTP/2, Open Graph
- Reverse proxies**: Nginx 1.18.0
- Authentication**: Facebook Login

Mediante la herramienta **gowitness** se adjuntan capturas de múltiples subdominios de Smule (archivo gowitness.zip). Lamentablemente no se ha podido hacer uso del servidor local generado por la herramienta para el análisis de las capturas.

Mediante la herramienta **whatweb** se procede a examinar la configuración de seguridad

```
(kali㉿kali)-[~/recopilacion/smule.com/0224]
$ whatweb -i subdominiosfinal.txt
http://api-iris.smule.com/ [403 Forbidden] Country[RESERVED][ZZ], IP[205.143.41.225]
http://c-sg.smule.com/ [403 Forbidden] Country[RESERVED][ZZ], IP[205.143.41.232], Title[403 Forbidden]
http://app.smule.com [404 Not Found] Country[RESERVED][ZZ], IP[205.143.41.226], Title[404]
http://api-sing.smule.com/ [418 Unassigned] Country[RESERVED][ZZ], IP[205.143.41.225], Teapot[I'm a teapot]
http://c-t2.cdn.gcp.smule.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Google-Edge-Cache]
http://c-t1.cdn.gcp.smule.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Google-Edge-Cache]
http://c-ash.smule.com/ [403 Forbidden] Country[RESERVED][ZZ], IP[205.143.41.232], Title[403 Forbidden]
http://admin.smule.com [403 Forbidden] Country[RESERVED][ZZ], IP[205.143.41.213]
http://api-beta.smule.com/ [418 Unassigned] Country[RESERVED][ZZ], IP[205.143.41.226], Teapot[I'm a teapot]
http://api-piano.smule.com/ [418 Unassigned] Country[RESERVED][ZZ], IP[205.143.41.226], Teapot[I'm a teapot]
http://c-fa.cdn.smule.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[199.232.34.
-served-by,x-cache-hits,x-timer], Varnish, Via-Proxy[1.1 varnish]
```

1. Estados de los servidores:

- Muchos dominios redirigen a una versión HTTPS con un código **301 (Moved Permanently)**, lo que indica que los servicios han migrado a conexiones seguras.
- Algunos servidores responden con **403 Forbidden**, lo que significa que el acceso está restringido (posiblemente por configuración del servidor o firewall).
- Otros devuelven **404 Not Found**, lo que sugiere que las rutas pueden estar deshabilitadas o que no hay contenido en esas direcciones.

2. Ubicaciones e infraestructura:

- Se identifican direcciones IP principalmente en **Estados Unidos** y algunas en regiones reservadas (**ZZ**), lo que podría significar que los servidores están en una infraestructura privada o en la nube.
- Hay presencia de servidores **Google-Edge-Cache**, **nginx**, **Apache**, y **Varnish**, lo que sugiere una infraestructura con balanceo de carga y caché de contenido.

3. Seguridad:

- Algunos servidores tienen configuraciones de seguridad como **Strict-Transport-Security (HSTS)**, que obliga a usar HTTPS en futuras conexiones.
- También se detectan encabezados como **X-Frame-Options[SAMEORIGIN]** y **X-XSS-Protection**, que ayudan a mitigar ataques de clickjacking y XSS (Cross-Site Scripting).

4. Servicios específicos:

- Se han identificado diferentes entornos como **staging**, **beta**, y **integration**, lo que indica que hay servidores dedicados a pruebas y desarrollo.
- Se menciona el uso de **Ruby on Rails** y **Bootstrap**, lo que sugiere que algunas partes de Smule están desarrolladas con estos frameworks.

El análisis muestra que Smule tiene una infraestructura distribuida con varias capas de seguridad y caché. Algunos servidores están abiertos al público, mientras que otros están restringidos o en desuso.

3.3 Análisis posibles WAFs

```
[kali㉿kali)-[~/recopilacion/smule.com/0224]
$ wafw00f -i subdominiosfinal.txt -o wafw00f.txt

File System
Woof!
Home ~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://c-fa.cdn.smule.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
[*] Checking https://ds.smule.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
[*] Checking https://c-sf.smule.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
[*] Checking https://api-iris.smule.com
[+] The site https://api-iris.smule.com is behind Shadow Daemon (Zecure) WAF.
[~] Number of requests: 2
[*] Checking https://api-piano.smule.com
[+] The site https://api-piano.smule.com is behind Shadow Daemon (Zecure) WAF.
[~] Number of requests: 2
[*] Checking https://ftp.smule.com
[+] The site https://ftp.smule.com is behind Shadow Daemon (Zecure) WAF.
[~] Number of requests: 2
```

Tras ejecutar la herramienta **wafw00f** el archivo generado **wafw00f.txt** muestra los resultados de un escaneo en los subdominios de **Smule** para detectar la presencia de **firewalls de aplicaciones web (WAFs)**. Aquí está la interpretación de los resultados clave:

1. Detección de WAFs

- **Shadow Daemon:** Es un WAF que se detectó en múltiples subdominios, incluyendo:
 - <https://api-iris.smule.com>
 - <https://api-piano.smule.com>
 - <https://ftp.smule.com>
 - <https://admin.smule.com>
 - <https://forum.smule.com>
 - <https://app.smule.com>
 - <https://glee.smule.com>
 - <https://api.smule.com>
 - <https://www.smule.com>

Shadow Daemon es un WAF diseñado para detectar y bloquear ataques de inyección SQL, XSS y accesos no autorizados a archivos del sistema.

- **Wordfence:** Detectado en <https://blog.smule.com>, lo que indica que este subdominio podría estar basado en **WordPress**, ya que Wordfence es un plugin de seguridad para esta plataforma.
- **CloudFront:** Aparece en <https://static1.smule.com>, <https://static2.smule.com> y <https://static3.smule.com>, lo que sugiere que estos dominios están protegidos o gestionados a través de la red de distribución de contenido (**CDN**) de Amazon.

2. Subdominios sin WAF detectado

Algunos subdominios no muestran un WAF detectado, lo que no necesariamente significa que no haya protección, sino que **wafw00f** no pudo identificarlo. Estos incluyen:

- <https://c-fa.cdn.smule.com>
- <https://ds.smule.com>
- <https://c-sf.smule.com>
- <https://c-t1.cdn.gcp.smule.com>
- <https://tracking.smule.com>
- <https://www-int.smule.com>
- <https://y-sg.smule.com>
- <https://test.cdn.smule.com>

3. Pruebas realizadas

Se utilizaron payloads para probar vulnerabilidades en cada subdominio, incluyendo:

- **XSS (Cross-Site Scripting):** <script>alert("XSS");</script>
- **SQL Injection:** UNION SELECT ALL FROM information_schema AND " or SLEEP(5) or "
- **Directory Traversal:** ../../etc/passwd

Los subdominios protegidos por **Shadow Daemon** bloquearon estos intentos, lo que indica que el WAF está activo.

Conclusión

- Smule tiene protección activa en muchos de sus subdominios con Shadow Daemon, Wordfence y CloudFront.
- Algunos subdominios no muestran WAF detectado, lo que podría significar que están menos protegidos o usan un sistema que wafw00f no pudo identificar.
- Las pruebas de inyección SQL, XSS y directory traversal fueron bloqueadas en los subdominios con WAF.
- Los subdominios que carecen de WAF detectable podrían ser puntos potencialmente vulnerables.

3.4 Descubrimiento de contenido

Mediante la herramienta **ffuf** se procede a chequear el contenido de smule.com y a continuación se analiza el contenido del archivo ffuf.txt

```
(kali㉿kali)-[~/recopilacion/smule.com/0224]
$ ffuf -w ~/recopilacion/lists/common.txt -t 10 -mc 200,401,403 -u https://smule.com/FUZZ -o ffuf.txt

File Sync v2.1.0-dev

:: Method      : GET
:: URL         : https://smule.com/FUZZ
:: Wordlist    : FUZZ: /home/kali/recopilacion/lists/common.txt
:: Output file : ffuf.txt
:: File format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 10
:: Matcher     : Response status: 200,401,403

.git/HEAD          [Status: 403, Size: 93, Words: 6, Lines: 4, Duration: 140ms]
.git/config        [Status: 403, Size: 93, Words: 6, Lines: 4, Duration: 140ms]
.git/logs/         [Status: 403, Size: 93, Words: 6, Lines: 4, Duration: 141ms]
.git/index         [Status: 403, Size: 93, Words: 6, Lines: 4, Duration: 141ms]
.svn/entries       [Status: 403, Size: 93, Words: 6, Lines: 4, Duration: 140ms]
.well-known/apple-app-site-association [Status: 200, Size: 434, Words: 199, Lines: 23, Duration: 141ms]
.well-known/assetlinks.json [Status: 200, Size: 597, Words: 57, Lines: 19, Duration: 140ms]
.well-known/security.txt [Status: 200, Size: 205, Words: 7, Lines: 7, Duration: 140ms]
._stats            [Status: 403, Size: 93, Words: 6, Lines: 4, Duration: 140ms]
about              [Status: 200, Size: 5868, Words: 654, Lines: 85, Duration: 142ms]
apple-app-site-association [Status: 200, Size: 434, Words: 199, Lines: 23, Duration: 139ms]
channel            [Status: 200, Size: 257, Words: 35, Lines: 8, Duration: 161ms]
```

Resultados principales

Se encontraron **rutas interesantes**, clasificadas según su código de estado:

Directarios y archivos restringidos (403 - Forbidden)

Estos archivos pueden contener información sensible si estuvieran accesibles:

- .git/HEAD, .git/config, .git/logs/, .git/index
- .svn/entries
- _stats

Implicación: Smule tiene **repositorios Git y SVN restringidos**, lo que sugiere que hay control de versiones en el servidor. Sin embargo, la presencia de estas carpetas puede ser una **mala práctica de seguridad**, ya que si en algún momento quedan accesibles, podrían exponer el código fuente o credenciales.

Archivos y páginas accesibles (200 - OK)

Se encontraron archivos públicos:

- **Archivos en .well-known/** (usados para configuraciones de seguridad y aplicaciones):
 - .well-known/apple-app-site-association (434 bytes, JSON)
 - .well-known/assetlinks.json (597 bytes, JSON)
 - .well-known/security.txt (205 bytes, TXT)

Implicación: Estos archivos permiten la integración con **Apple** y **Android** para apps móviles y proporcionan información de seguridad.

- **Páginas informativas:**
 - /about
 - /copyright, /copyright-policy
 - /privacy, /privacy-policy, /privacy_policy, /privacypolicy
 - /jobs (página de ofertas de trabajo)
 - /patents (posiblemente sobre propiedad intelectual)
 - /press (sección de prensa)
 - /explore (posible sección de exploración de contenido)
 - /songs (página de canciones)

Implicación: Estas páginas no presentan riesgos, pero muestran información útil sobre la empresa.

- **Otros archivos:**
 - /crossdomain.xml (configuración de acceso de dominios externos)
 - /favicon.ico (ícono del sitio web)

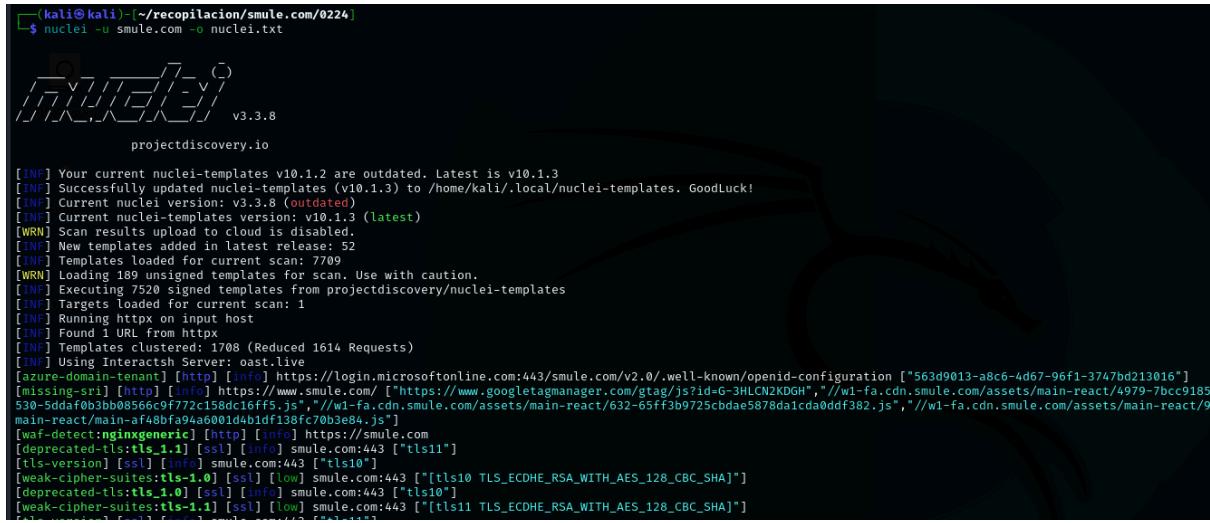
Implicación: crossdomain.xml podría ser analizado para verificar si permite accesos indebidos desde otros dominios.

Conclusión

- **Se identificaron archivos potencialmente sensibles (.git, .svn) con acceso restringido (403).** Aunque están protegidos, es una buena práctica **eliminarlos** del servidor de producción.
- **Se detectaron archivos de configuración en .well-known/**, lo que sugiere que Smule tiene integración con dispositivos móviles y prácticas de seguridad documentadas.
- **Las páginas públicas revelan información sobre la empresa, políticas y exploración de contenido,** pero no representan riesgos inmediatos.
- **No se encontraron archivos que filtren datos confidenciales.**

4.- Análisis de vulnerabilidades

4.1 Análisis Estándar



```
(kali㉿kali)-[~/recopilacion/smule.com/0224
$ nuclei -u smule.com -o nuclei.txt
v3.3.8
projectdiscovery.io

[INF] Your current nuclei-templates v10.1.2 are outdated. Latest is v10.1.3
[INF] Successfully updated nuclei-templates (v10.1.3) to /home/kali/.local/nuclei-templates. GoodLuck!
[INF] Current nuclei version: v3.3.8 (outdated)
[INF] Current nuclei-templates version: v10.1.3 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 52
[INF] Templates loaded for current scan: 7709
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INF] Executing 7520 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from https://
[INF] Templates clustered: 1708 (Reduced 1614 Requests)
[INF] Using Interactsh Server: oast.live
[azure-domain-tenant] [http] [info] https://login.microsoftonline.com:443/smule.com/v2.0/.well-known/openid-configuration ["563d9013-a8c6-4d67-96f1-3747bd213016"]
[missing-sri] [http] [info] https://www.smule.com/ ["https://www.googletagmanager.com/gtag/js?id=G-3HLCN2KDGH", "//w1-fa.cdn.smule.com/assets/main-react/4979-7bcc9185530-5ddaf03bb08566c9f772c158dc16ff5.js", "//w1-fa.cdn.smule.com/assets/main-react/632-65ff3b9725chdae5878da1cd0ddf382.js", "//w1-fa.cdn.smule.com/assets/main-react/9main-react/main-a48bf94a6001db41df138fc70b3e84.js"]
[waf-detect:nginxgeneric] [http] [info] https://smule.com
[deprecated-tls:tls_1.1] [ssl] [info] smule.com:443 [*tls11*]
[tls-version] [ssl] [info] smule.com:443 [*tls10*]
[weak-cipher-suites:tls-1.0] [ssl] [low] smule.com:443 [*["tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA"]*]
[deprecated-tls:tls_1.0] [ssl] [info] smule.com:443 [*tls10*]
[weak-cipher-suites:tls-1.1] [ssl] [low] smule.com:443 [*["tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA"]*]
```

El escaneo realizado con **Nuclei** ha identificado varias configuraciones de seguridad en **smule.com**.

1. Autenticación y Seguridad

- **Azure Tenant Detection:** Uso de **Azure AD** para autenticación.
- **Archivo security.txt:** Indica un programa de seguridad en **HackerOne** y el correo **security@smule.com** para reportes.
- **Apple App Site Association:** Confirma integración con aplicaciones iOS (**Sing!** y **AutoRap**).

2. Seguridad Web

- **Web Application Firewall (WAF):** Uso de **Nginx** con posible WAF genérico.
- **Falta de SRI en Scripts Externos:** Algunos scripts en **smule.com** no cuentan con **Subresource Integrity (SRI)**, lo que podría permitir modificaciones maliciosas.

Recomendación: Agregar los atributos **integrity** y **crossorigin="anonymous"** en las etiquetas `<script>`.

3. Seguridad en SSL/TLS

- **Versiones de TLS:**
 - **TLS 1.0 y 1.1 detectados**, ambos obsoletos.
 - **TLS 1.2 soportado**, pero **TLS 1.3 no habilitado**.

Recomendación: Deshabilitar **TLS 1.0 y 1.1** y habilitar **TLS 1.3**.

- **Cifrados Débiles:**
 - Uso de **CBC** en **TLS 1.0 y 1.1**, vulnerable a **LUCKY13**.

Recomendación: Utilizar cifrados más seguros como **AEAD (AES-GCM)**.

- **Certificados SSL:**
 - Uso de **certificado wildcard (*.smule.com)**. Posible riesgo, si el certificado se ve comprometido, todos los subdominios quedarían expuestos.

Recomendación: Considerar el uso de certificados específicos por subdominio.

4. Seguridad en el Correo (DNS y SPF)

- **SPF Record:** Correctamente configurado con -all para evitar suplantación de identidad.
- **DMARC Policy:** Configurado en "quarantine", pero la opción **p=reject** ofrecería mayor seguridad contra intentos de phishing.

5. Información de Dominio

- **DNSSEC no habilitado (secureDNS: false).**

Recomendación: Activar **DNSSEC** para prevenir ataques de **spoofing**.

- **MX (Mail Exchange):** Uso de **Google Apps (Gmail/Google Workspace)** para la gestión del correo electrónico.

Conclusiones

Hallazgos Críticos (Alta Prioridad)

- Deshabilitar **TLS 1.0 y 1.1**.
- Reemplazar los cifrados **CBC** con **AEAD (AES-GCM)**.
- Habilitar **TLS 1.3** para mejorar la seguridad y el rendimiento.

Hallazgos de Riesgo Medio

- Implementar **HSTS (Strict-Transport-Security)** para evitar ataques de **SSL Stripping**.
- Revisar el uso del **certificado wildcard** y considerar certificados individuales para subdominios críticos.
- Añadir **SRI en scripts externos** para prevenir modificaciones maliciosas.

Hallazgos de Riesgo Bajo

- Cambiar **DMARC a "p=reject"** para mejorar la protección contra phishing.
- Habilitar **DNSSEC** para prevenir ataques de spoofing.

El análisis sugiere que **smule.com** debe fortalecer su seguridad, especialmente en la configuración de **TLS/SSL**, la protección de scripts externos y la autenticación de correos electrónicos.

4.2 Análisis web

Como muestra la siguiente captura, smule.com no usa la tecnología **Wordpress**.

4.3 Análisis SSL/TLS

```
(kali㉿kali)-[~/recopilacion/testssl.sh]
$ ./testssl.sh smule.com

#####
# testssl.sh version 3.2rc4 from https://testssl.sh/dev/
# (74209e0 2025-02-17 15:39:26)

This program is free software. Distribution and modification under
GPLv2 permitted. USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/

#####

Using OpenSSL 1.0.2-bad  [~183 ciphers]
on kali:./bin/openssl.Linux.x86_64

Testing all IPv4 addresses (port 443): 205.143.41.213 205.143.41.225 205.143.41.228 205.143.41.226 205.143.41.227
Start 2025-02-24 15:11:58          → 205.143.41.213:443 (smule.com) ←
Further IP addresses: 205.143.41.227 205.143.41.226 205.143.41.228 205.143.41.225
rDNS (205.143.41.213): api5.oak.smle.co.
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2    not offered (OK)
SSLv3    not offered (OK)
TLS 1     offered (deprecated)
TLS 1.1   offered (deprecated)
TLS 1.2   offered (OK)
TLS 1.3   not offered and downgraded to a weaker protocol
NPN/SPDY h2, http/1.1 (advertised)
ALPN/HTTP2 h2, http/1.1 (offered)
```

El análisis de seguridad realizado con la herramienta **testssl.sh** a los servidores de **smule.com** revela varias áreas de interés en términos de seguridad TLS/SSL. A continuación, se presenta un resumen con hallazgos clave y posibles recomendaciones.

1. Protocolos soportados

- **SSLv2 y SSLv3:** No están ofrecidos.
- **TLS 1.0 y 1.1:** Están habilitados.
- **TLS 1.2:** Está habilitado.
- **TLS 1.3:** No está soportado y se hace downgrade a una versión más débil.

Riesgo: TLS 1.0 y 1.1 están obsoletos y presentan riesgos de seguridad, lo que baja la calificación de seguridad.

Recomendación: Deshabilitar **TLS 1.0 y TLS 1.1** y habilitar **TLS 1.3** para mejorar la seguridad y compatibilidad futura.

2. Cifrado soportado

- **Cifrado débil (NULL, RC4, DES, 3DES, etc.):** No está soportado.
- **Cifrado fuerte (AEAD con Forward Secrecy):** Está soportado.
- **Cifrado obsoleto CBC (AES, ARIA, etc.):** Está habilitado.

Riesgo: Se soportan cifrados en modo **CBC**, los cuales pueden ser vulnerables a ataques como **LUCKY13**.

Recomendación: Eliminar cifrados **CBC** y priorizar **GCM** (AES-GCM-SHA256 o superior).

3. Orden de cifrados del servidor

- **El servidor tiene preferencia en el orden de cifrados:** Sí.

Impacto: Permite evitar ataques en los que un cliente pueda forzar cifrados más débiles.

4. Forward Secrecy (FS)

- **Está habilitado para los cifrados modernos:** Sí.

Impacto: Protege sesiones pasadas en caso de que la clave privada del servidor se vea comprometida.

5. Certificado y cadena de confianza

- **Certificado wildcard para *.smule.com.**
- **Cadena de confianza válida y bien configurada.**
- **Tiempo de expiración: hasta octubre de 2025.**

Possible problema: Los certificados **wildcard** pueden ser un riesgo si se compromete una subdominio.

Recomendación: Evaluar la posibilidad de emitir certificados específicos para cada subdominio crítico.

6. HTTP Headers y configuraciones adicionales

- **Strict Transport Security (HSTS):** No está configurado.
- **Public Key Pinning (HPKP):** No ofrecido.
- **OCSP Stapling:** No ofrecido.
- **Redirección HTTP 301:** Correcta.

Recomendaciones:

- **Habilitar HSTS** para evitar ataques tipo **SSL Stripping**.
- **Activar OCSP Stapling** para mejorar la validación del certificado sin depender de terceros.

7. Pruebas de vulnerabilidades

- **Heartbleed, POODLE, DROWN, ROBOT, CRIME, etc.:** No vulnerables.
- **LUCKY13:** Potencialmente vulnerable.
- **BEAST:** Vulnerable en TLS 1.0 (pero mitigado en TLS 1.1/1.2).

Recomendaciones:

- **Eliminar TLS 1.0/1.1** para mitigar BEAST.
- **Eliminar CBC y usar AES-GCM** para mitigar LUCKY13.

8. Calificación de seguridad

- **Puntuación final: 91/100** (Calificación: **B**).
- **Razones por las que no obtiene "A":**
 - Se ofrece **TLS 1.0 y 1.1**.
 - No se ha implementado **HSTS**.

Cómo mejorar la calificación a "A":

1. **Eliminar TLS 1.0 y 1.1.**
2. **Habilitar TLS 1.3.**
3. **Implementar HSTS.**
4. **Desactivar cifrados CBC y usar solo AES-GCM.**

Conclusión

El servidor de **smule.com** tiene una configuración **moderadamente segura**, pero hay **mejoras críticas necesarias**:

1. **Deshabilitar TLS 1.0 y 1.1.**
2. **Habilitar TLS 1.3.**
3. **Habilitar HSTS.**
4. **Eliminar cifrados CBC.**

4.4 Análisis de servidores de correo electrónico

```
[kali㉿kali] -[~/recopilacion/spoofcheck]
$ python spoofcheck.py smule.com
[*] Found SPF record:
[*] v=spf1 mx ip4:104.254.204.1/22 ip4:65.222.153.33 ip4:205.139.25.0/24 ip4:54.251.142.61 ip4:205.143.40.0/22 include:_spf.google.com
include:email-smtp.outlook.com include:spf.mandrillapp.com include:_spf.atlassian.net include:mail.zendesk.com -all
[*] SPF record contains an All item: -all
[*] Found DMARC record:
[*] v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarc-reports@smule.com
[-] DMARC policy set to quarantine
[*] Aggregate reports will be sent: mailto:dmarc-reports@smule.com
[-] Spoofing not possible for smule.com

[kali㉿kali] -[~/recopilacion/spoofcheck]
$
```

La herramienta **SpoofCheck** se utilizó para verificar si **smule.com** es vulnerable a ataques de **email spoofing**. A continuación, se analiza el resultado:

1. Registro SPF (Sender Policy Framework)

- Se permite el envío de correos solo desde los servidores especificados.
- El uso de **-all** **bloquea el spoofing**, evitando que servidores no autorizados envíen correos en nombre de smule.com.
- Incluye proveedores como **Google, Atlassian, Mandrill y Zendesk**.

Conclusión: SPF está bien configurado y ayuda a prevenir spoofing.

4.5 Detección de Subdomain Takeover

```
[kali㉿kali] -[~/recopilacion/smule.com/0224]
$ subzy run --targets subdominios_vivos.txt
[*] Fingerprints found; checking integrity with an upstream
[*] Loaded 94 targets
[*] Loaded 76 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] - https://c-fa.cdn.smule.com
[NOT VULNERABLE] - https://ds.smule.com
[NOT VULNERABLE] - https://blog.smule.com (outdated, Latest is v10.1.3)
[NOT VULNERABLE] - https://c-sf.smule.com (10.1.3) to /home/kali/.local/nuclei-templates. GoodLuck!
[NOT VULNERABLE] - https://api-iris.smule.com
[NOT VULNERABLE] - https://api-beta.smule.com (test)
[NOT VULNERABLE] - https://api-piano.smule.com
[NOT VULNERABLE] - https://admin.smule.com
[NOT VULNERABLE] - https://ftp.smule.com
[NOT VULNERABLE] - https://c-sg.smule.com (Use with caution.)
[NOT VULNERABLE] - https://c-int-ash.smule.com/discovery/nuclei-templates
[NOT VULNERABLE] - https://api-sing.smule.com
[NOT VULNERABLE] - https://c-int-sf.smule.com
[NOT VULNERABLE] - https://c-ash.smule.com
[NOT VULNERABLE] - https://api4.smule.com (Requests)
[NOT VULNERABLE] - https://api5.smule.com
[ ] https://login.microsoftonline.com:443/smule.com/v2.0/.well-known/openid-configuration
[VULNERABLE] - https://api-staging.smule.com [Cargo Collective] (tagmanager.com/gtag/js?id=G-3HLCN2KDI)
[DISCUSSION] - [Issue #152](https://github.com/EdOverflow/can-i-take-over-xyz/issues/152) (smule.com)
[DOCUMENTATION] - [Cargo Support Page](https://support.2.cargocollective.com/Using-a-Third-Party-Domain)
```

El escaneo realizado con la herramienta **Subzy** sobre los subdominios de **smule.com** detectó que la mayoría de los subdominios no son vulnerables a **Subdomain Takeover**. Sin embargo, **8 subdominios fueron identificados como vulnerables** debido a configuraciones erróneas con el servicio **Cargo Collective**.

Subdominios vulnerables:

1. <https://api-staging.smule.com>
2. <https://admin-test.smule.com>
3. <https://email.smule.com>
4. <https://j-int.smule.com>
5. <https://links.marketing.smule.com>
6. <https://w1-beta.smule.com>
7. <https://w1-fa-beta.cdn.smule.com>
8. <https://w2-beta.smule.com>

Cada uno de estos subdominios presenta una vulnerabilidad documentada en el siguiente enlace <https://github.com/EdOverflow/can-i-take-over-xyz/issues/152>

Recomendaciones

- **Eliminar registros DNS huérfanos:** Si los subdominios ya no están en uso, eliminarlos de la configuración DNS.
- **Reclamar los subdominios en Cargo Collective:** Si estos subdominios aún son necesarios, deben ser reclamados en la plataforma correspondiente
- **Implementar reglas de seguridad** en el servidor DNS para evitar la toma de control de subdominios huérfanos.

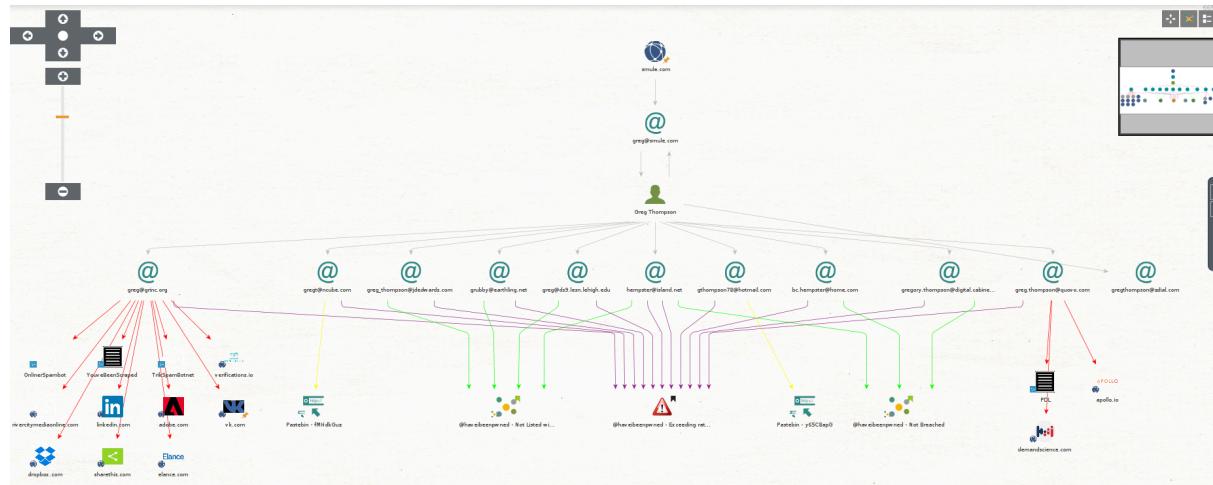
4.6 Shodam

Tal y como se mostraba en la captura de esta extensión web (ver página...) aparecen las siguientes vulnerabilidades

1. **CVE-2023-44487:**
Es una vulnerabilidad en HTTP/2 que permite ataques de **denegación de servicio (DoS)** explotando el mecanismo de "**Rapid Reset**", donde un atacante puede sobrecargar un servidor con múltiples solicitudes y cancelaciones rápidas, agotando sus recursos.
2. **CVE-2021-23017:**
Afecta a **NGINX** y permite **ejecución remota de código (RCE)** debido a un error en la función de resolución de nombres DNS. Un atacante podría enviar respuestas DNS maliciosas para ejecutar código arbitrario en el servidor afectado.
3. **CVE-2021-3618:**
Es una vulnerabilidad en **libgcrypt**, una biblioteca de criptografía utilizada en varias aplicaciones. Un fallo en la gestión de memoria podría permitir a un atacante ejecutar código arbitrario o causar una corrupción de memoria, afectando la seguridad del sistema.

5.- OSINT

5.1 Maltego



Tras ejecutar la aplicación Maltego sobre el dominio smule.com y aplicar las transformaciones necesarias, se identificó a un empleado de Smule, Greg Thompson, junto con varias direcciones de correo personal. Al analizar estas direcciones mediante la extensión de haveibeenpwned.com, se descubrió que la cuenta greg@grinc.org ha estado involucrada en múltiples brechas de seguridad, entre ellas las de Adobe en 2013, LinkedIn en 2016 y Dropbox en 2012.

A continuación se muestra una captura del perfil de Linkedin de Greg Thompson, donde se puede comprobar que fue empleado de Smule entre los años 2012 y 2014.

Profile picture of Greg Thompson (He/Him)
Senior Engineering Manager at Airbnb



Lead Software Engineer

Smule

feb. 2012 - oct. 2014 · 2 años 9 meses

San Francisco Bay Area

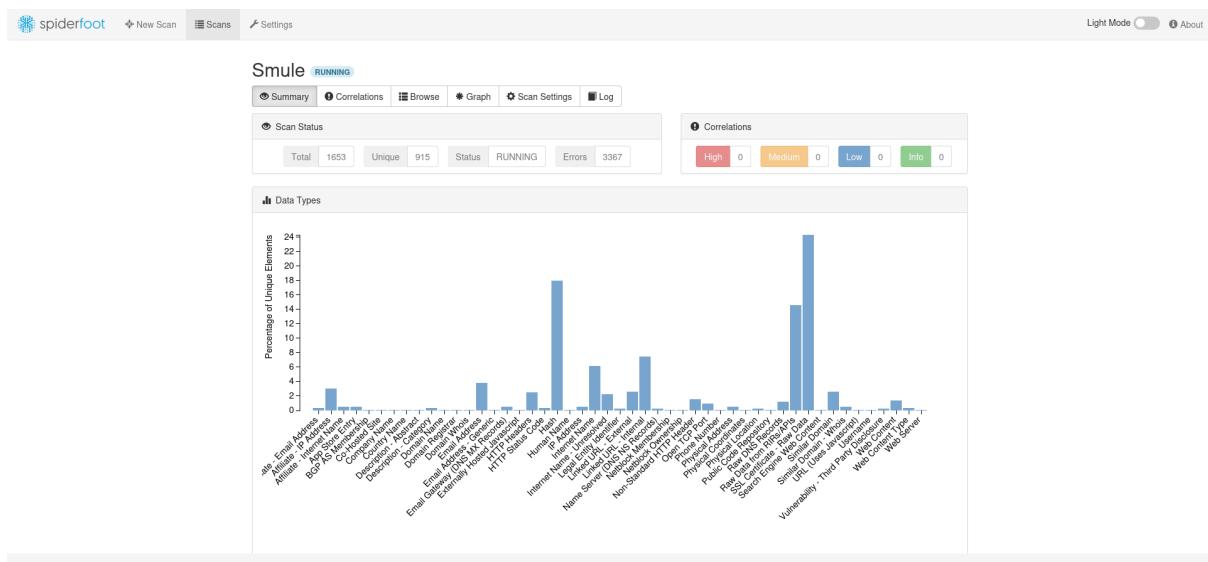
5.2 Spiderfoot

```
[(kali㉿kali)-[~]]$ spiderfoot -l localhost:8082
/usr/lib/python3/dist-packages/adblockparser/parser.py:247: SyntaxWarning: invalid escape sequence '\w'
    rule = rule.replace("^", "(?:[^\\w\\d_\\-.%]|$)")
/usr/lib/python3/dist-packages/adblockparser/parser.py:272: SyntaxWarning: invalid escape sequence '\\|'
    rule = re.sub("(\\|)[^$]", r"\|", rule)

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://localhost:8082/
*****

2025-03-06 18:17:21,864 [INFO] sf : Starting web server at localhost:8082 ...
2025-03-06 18:17:21,870 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

CherryPy Checker:
The use of 'localhost' as a socket host can cause problems on newer systems, since 'localhost' can map to either an I



The screenshot shows the SpiderFoot web interface with the following details:

- Scan Status:** Total 1653, Unique 915, Status RUNNING, Errors 3367.
- Correlations:** High 0, Medium 0, Low 0, Info 0.
- Browse:** Email Address
- Data Table:** A table listing identified email addresses along with their source module and timestamp. All entries are from the 'sfp_skymem' module at 2025-03-06 18:23:26.

Data Element	Source Data Element	Source Module	Identified
android-security@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
appstore@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
assistance@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
autorap-support@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
bill@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
borislav.kolev@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
carla.herrera@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
cheng-i.wang@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
community@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:26
cong.hui@smule.com	smule.com	sfp_skymem	2025-03-06 18:23:27

- Footer:** A note about the SpiderFoot CLI and acinema tutorials.

Mediante la herramienta spiderfoot se han podido encontrar 35 direcciones de correo electrónico asociadas a Smule.com (se recogen todas en el archivo SpiderFoot.csv). De entre todas ellas se han escogido 2 para profundizar sobre las mismas:

- elizabeth.tobey@smule.com



Elizabeth Tobey (She/Her)
Marketing Executive | CX | AI | Digital Transformation



Director of Marketing

Smule, Inc.

feb. 2014 - oct. 2014 · 9 meses

San Francisco Bay Area

Responsible for leadership and management of all marketing activities, including strategy, product marketing, branding, communications, events, and customer service

Rebuilt Marketing department from the ground up, including creating a new community team, overhauling and integrating customer service into the organizational structure, and realigning the communications strategy to focus on consumer and lifestyle angles

Spearheaded company's first brand-focused campaign, aimed at changing the perception of the company from that of an app maker to one that runs a platform powered by over 125 million users

Overhauled the customer lifecycle, including a new email funnel, with extensive A/B testing and metrics tracking to ensure downstream actions are optimized to align with company goals

Oversaw six internal employees as well as an offsite public relations agency

Como muestra la captura de Linkedin, Elisabeth Tobey desempeñó el cargo de Directora de Marketing de Smule durante el año 2014. En la siguiente captura se muestra el resultado de introducir su correo en haveibeenpwned.com.

 **Apollo**: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

 **Covve**: In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles

 **LinkedIn Scraped Data (2021)**: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.

Compromised data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles

- borislav.kolev@smule.com



Borislav Kolev

Engineer at Alkemio. Engineering Manager, Tech Lead, Web Engineer, Creator



Smule, Inc.

5 años 1 mes

- **Engineering Manager**

Jornada completa

2020 - feb. 2024 · 4 años 2 meses

Bulgaria · Híbrido

❖ Cross-functional Team Leadership, Project Management y 2 aptitudes más

- **Web Team Lead**

sept. 2019 - feb. 2024 · 4 años 6 meses

❖ NestJS, React.js y 4 aptitudes más

- **Web Engineer**

feb. 2019 - feb. 2024 · 5 años 1 mes

❖ NestJS, React.js y 4 aptitudes más

Como muestra la captura de Linkedin, Borislav Kolev desempeñó el cargo de Gerente de Ingeniería de Smule desde el año 2020 hasta febrero de 2024. En la siguiente captura se muestra el resultado de introducir su correo en haveibeenpwned.com.

borislav.kolev@smule.com

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

5.3 Empleados destacados en Linkedin

Se adjuntan capturas del perfil de Linkedin tanto del CEO y fundador de Smule Jeffrey Smith, como de su presidente Bill Bradford.

- <https://www.linkedin.com/in/jeffchrsmith/>

The screenshot shows Jeffrey Smith's LinkedIn profile. At the top right is the Smule logo with the tagline "Let's music together". To the left is a circular profile picture of Jeffrey Smith wearing a cap and glasses, standing next to a brown horse. Below the profile picture, his name is listed as "Jeffrey Smith" with a verified checkmark, followed by "3er". His title is "Co-founder and CEO, Smule". His location is "Afton, Wyoming, Estados Unidos" and there is a link to "Información de contacto". It is noted that he has "Más de 500 contactos". At the bottom are three buttons: "Enviar mensaje", "+ Seguir", and "Más". To the right of the profile are two company logos: "Smule, Inc." and "Stanford University".

- <https://www.linkedin.com/in/wnbradford/>

The screenshot shows Bill Bradford's LinkedIn profile. At the top right is the Smule logo with the tagline "Let's music together". To the left is a circular profile picture of Bill Bradford smiling. Below the profile picture, his name is listed as "Bill Bradford" with a verified checkmark, followed by "3er". His title is "President at Smule, Inc.". His location is "San Mateo, California, Estados Unidos" and there is a link to "Información de contacto". It is noted that he has "Más de 500 contactos". At the bottom are three buttons: "Enviar mensaje", "+ Seguir", and "Más". To the right of the profile are two company logos: "Smule, Inc." and "Stanford University".