# Information Gathering

## José Benito Ibarria Topete

## Profesor Martín Martín

### Bootcamp de ciberseguridad KeepCoding

Introducción:

En el contexto de un mundo financiero en constante evolución, la ciberseguridad se ha convertido en un pilar fundamental para asegurar la integridad, confidencialidad y disponibilidad de los sistemas informáticos, especialmente para aquellas entidades que operan dentro de la economía criptográfica. Coinbase, como líder en la construcción de la criptoeconomía – un sistema financiero más justo, accesible, eficiente y transparente habilitado por la criptomoneda – se destaca por su compromiso hacia la seguridad y la confianza de sus usuarios desde su fundación en 2012. Con la idea radical de que cualquiera, en cualquier lugar, debería poder enviar y recibir Bitcoin de manera fácil y segura, Coinbase ha evolucionado para ofrecer una plataforma confiable y fácil de usar para acceder a la criptoeconomía más amplia.

Este reporte se centra en evaluar las prácticas de seguridad cibernética de la organización Coinbase, con el objetivo de identificar y analizar cualquier vulnerabilidad potencial que pudiera afectar la seguridad de sus operaciones y, por extensión, la confianza de sus usuarios. A través de una serie de técnicas de recopilación de información y análisis de vulnerabilidades autorizadas y éticas, se busca proporcionar una visión integral del estado actual de la seguridad de Coinbase, enfocándose en la infraestructura digital, las aplicaciones web, y los servicios en línea que forman el núcleo de sus operaciones.

Con el permiso expreso de Coinbase a través de HackerOne, este ejercicio de ciberseguridad se llevó a cabo siguiendo las mejores prácticas y metodologías establecidas en la industria, asegurando un proceso transparente y responsable. La intención de este reporte es servir como una herramienta educativa y de referencia practica para la comunidad de ciberseguridad, promoviendo así la mejora continua y el fortalecimiento de las defensas en el dinámico entorno de la criptoeconomía.

Metodología:

Enumeración de Subdominios con Shuffledns:

Proceso y Ejecución: Para realizar una exploración exhaustiva de la superficie de ataque asociada con coinbase.com, empleamos shuffledns, una herramienta avanzada de enumeración de subdominios. El proceso comenzó con la recopilación de un amplio conjunto de datos de fuentes pasivas, complementado posteriormente con un ataque de fuerza bruta para descubrir subdominios potencialmente no listados y ocultos. Utilizamos el siguiente comando para ejecutar shuffledns:

***Shuffledns –d coinbase.com –w wordlist.txt –r resolvers.txt***

Donde wordlist.txt contiene una lista de posibles nombres de subdominios a probar, y resolvers.txt una lista de servidores DNS para la resolución de nombres, ambas listas provistas por nuestro docente y que a su vez provienen de listas que se encuentran en github.

Hallazgos:

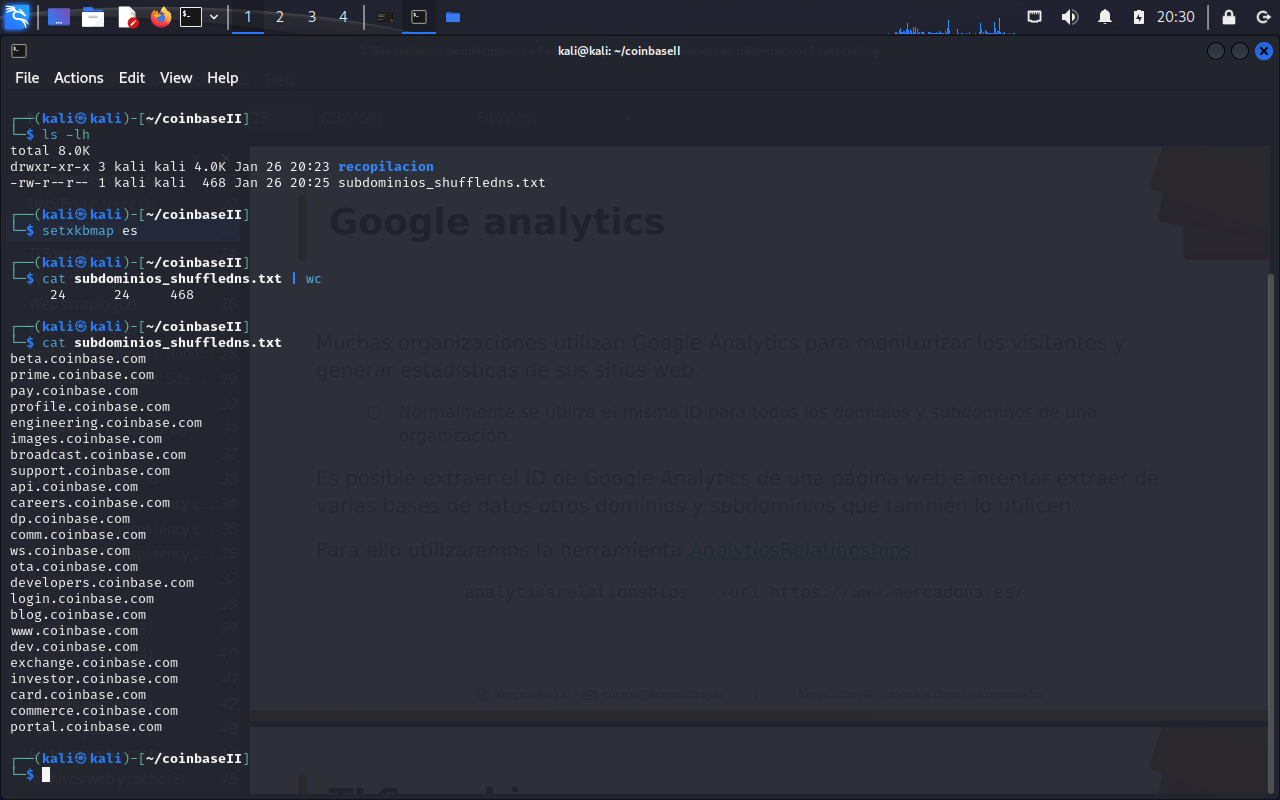
La ejecución de shuffledns permitió identificar varios subdominios relacionados con coinbase.com, destacando aquellos que podrían ser de interés por su potencial exposición a riesgos de seguridad o su relevancia para futuras fases de prueba de penetración. Entre los subdominios encontrados, algunos de los más notables incluyen:

***api.coinbase.com:*** Punto de acceso para las interfaces de programación de aplicaciones, relevante para entender la exposición de servicios internos.

***login.coinbase.com:*** Subdominio asociado al proceso de autenticación de usuarios, crítico para evaluar la seguridad en la gestión de sesiones y credenciales.

***engineering.coinbase.com*** ***y developers.coinbase.com:*** Portales que podrían contener información técnica detallada, documentación de APIs, o datos sobre el entorno de desarrollo.

Estos subdominios representan áreas de interés clave para una evaluación de seguridad más detallada, ya que podrían alojar servicios internos, interfaces de usuario para la autenticación, o documentación técnica que, si se manejan incorrectamente, podrían ser vectores de ataque potenciales.



Análisis TLS con cero:

Proceso y Ejecución:

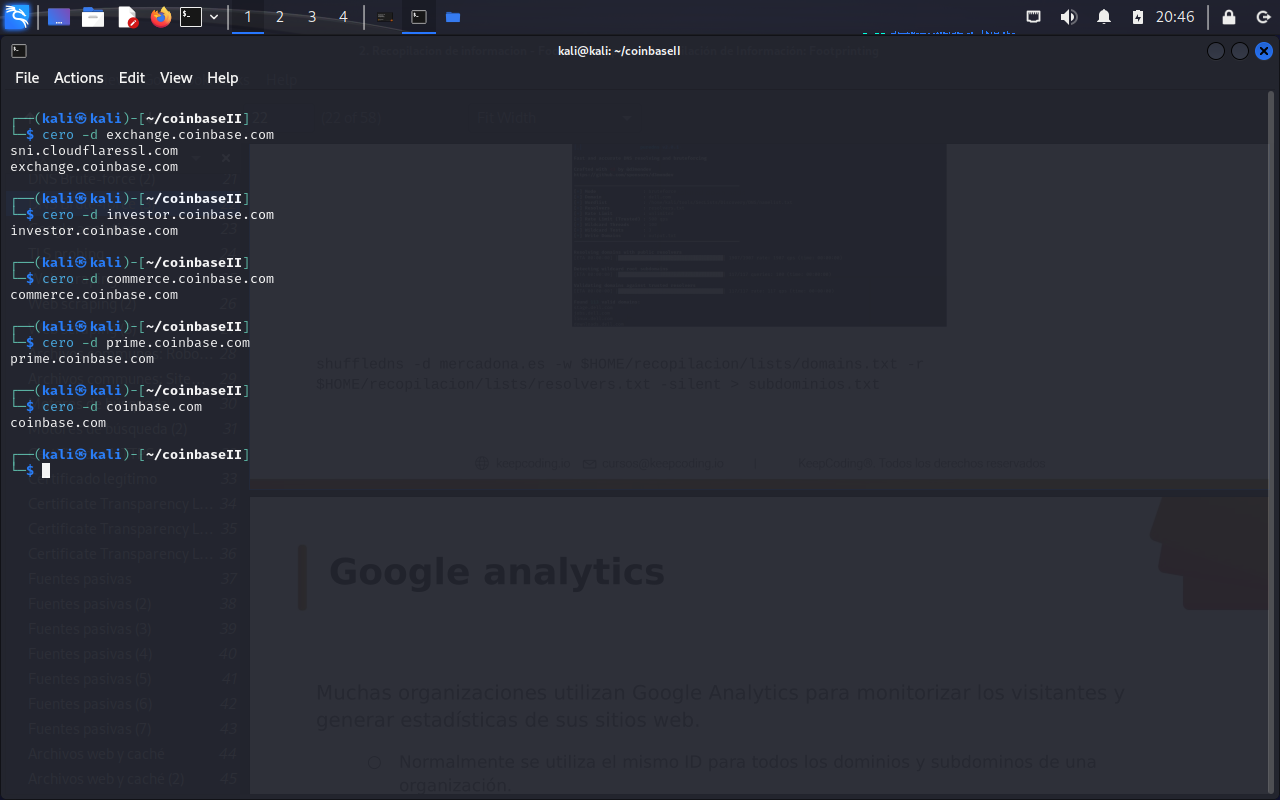
Para evaluar las configuraciones TLS/SSL de coinbase.com, utilizamos la herramienta cero, enfocada en el probing de TLS. A través de esta herramienta, buscamos identificar la implementación de seguridad en las comunicaciones encriptadas del dominio. El comando utilizado fue simple, apuntando directamente al dominio sin especificaciones adicionales para mantener el análisis dentro de un marco ético y autorizado.

Hallazgos:

El análisis realizado con cero resultó en un único registro TLS para coinbase.com, lo cual indica que el dominio emplea configuraciones de seguridad robustas que no exponen detalles innecesarios. Aunque el resultado fue limitado, este hallazgo subraya la eficacia de las medidas de protección implementadas por Coinbase, asegurando que la información sobre sus configuraciones TLS/SSL permanezca segura y no fácilmente accesible a través de herramientas de escaneo público. El comando utilizado fue:

***cero –d coinbase.com, cero –d Exchange.coinbase.com, cero –d investor.coinbase.com y cero –d prime.coinbase.com***

Este resultado refleja positivamente la postura de seguridad de coinbase.com, demostrando un compromiso sólido con la protección de las comunicaciones de sus usuarios a través de prácticas de encriptación fuertes y actualizadas.



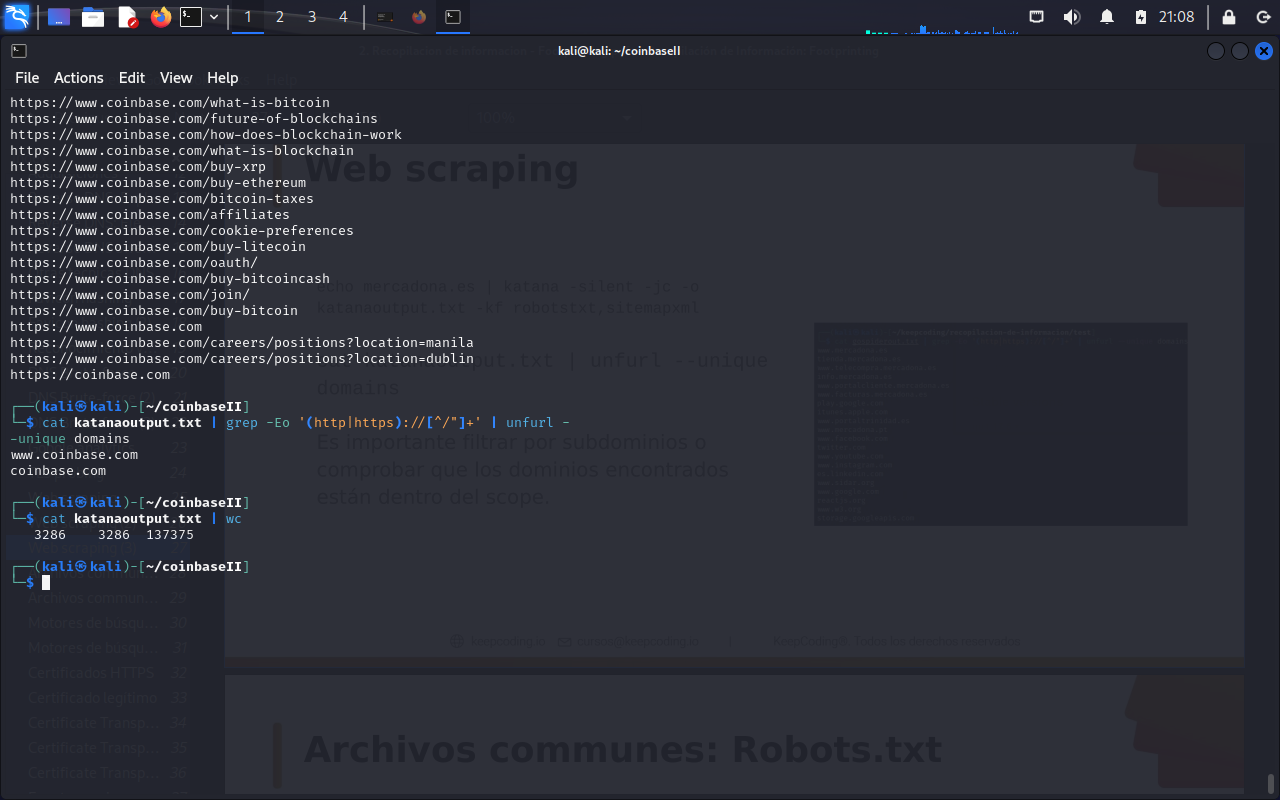
Análisis de WEB Scrapping y extracción de subdominios únicos con Katana

Proceso y Ejecución:

Para identificar dominios únicos asociados con coinbase.com, empleamos la herramienta Katana. La estrategia consistió en extraer todas las URLs encontradas en el sitio web y luego filtrarlas para obtener una lista de dominios únicos. El proceso se llevó a cabo con el siguiente comando en Katana, que incluye filtros y herramientas como unfurl para destilar solo los dominios únicos:

***katana -silent -jc -o katanaoutput.txt -kf robotstxt,sitemapxml www.coinbase.com | unfurl -u domains***

Hallazgos:

El resultado fue una lista “limpia” de dominios y subdominios, proporcionando una perspectiva valiosa sobre la estructura del sitio web de Coinbase. Entre los dominios encontrados, se destacan aquellos que apuntan a funciones críticas del negocio, como las páginas de transacción de criptomonedas, plataformas de usuario y carreras profesionales. Esta información es crucial para entender la exposición y la potencial superficie de ataque del sitio web.

Análisis de Registro de ecrtificados SSL con ctfr

Proceso y Ejecución:

Para profundizar en la infraestructura de coinbase.com, utilizamos la herramienta ctfr, que permite buscar en el registro de certificados SSL/TLS. La metodología se basó en identificar subdominios a través de los certificados emitidos, lo cual es una táctica efectiva para descubrir nombres de host que no se encuentran fácilmente a través de métodos tradicionales. Se ejecutó ctfr con el siguiente comando:

***ctfr –d coinbase.com***

Hallazgos:

El análisis con ctfr reveló una serie de subdominios interesantes, algunos de los cuales podrían ser críticos desde una perspectiva de seguridad:

* Subdominios de entornos de desarrollo y pruebas como sandbox.coinbase.com y staging.coinbase.com, que podrían ser más susceptibles a vulnerabilidades.
* Subdominios relacionados con servicios específicos como api.coinbase.com y support.coinbase.com, esenciales para la operación del negocio y, por lo tanto, importantes para asegurar adecuadamente.
* Subdominios que apuntan a servicios de infraestructura interna, como cloud.coinbase.com, que pueden ofrecer una visión de la arquitectura de la red de la empresa.

Estos subdominios, identificados a través de los registros de certificados SSL/TLS, proporcionan una comprensión más profunda de la superficie de ataque potencial y ayudan a formular estrategias de defensa más efectivas.

Análisis de caché con gau

Proceso y Ejecución:

La herramienta gau fue utilizada para examinar el caché y las referencias históricas de los contenidos asociados con coinbase.com. El propósito de este análisis fue identificar posibles exposiciones pasadas y entender mejor la estructura histórica de los recursos web de la empresa. Se implementó gau con el siguiente comando para recopilar una amplia gama de URLs que han sido indexadas o almacenadas en caché:

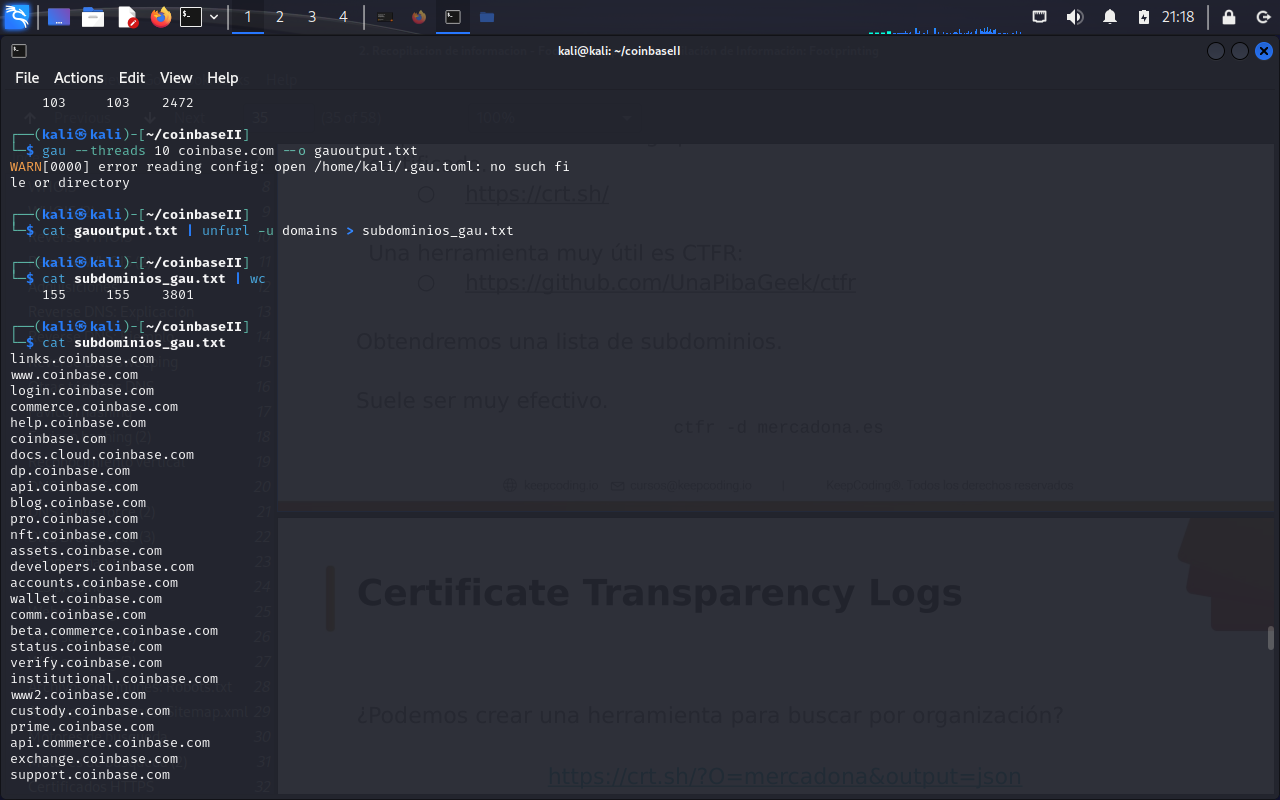
***gau –threads 5 coinbase.com –0 gauoutput.txt***

Hallazgos:

* La ejecución de gau generó una lista comprensiva de URLs que han estado asociadas con coinbase.com en el pasado. Entre los elementos más destacados encontrados se incluyen:
* Subdominios relacionados con áreas específicas de negocio como api.coinbase.com y support.coinbase.com.
* URLs de entornos de prueba y desarrollo, tales como sandbox.coinbase.com y staging.coinbase.com, que pueden contener versiones no finales y potencialmente menos seguras de la plataforma.
* Dominios con prefijos de "api", "developers" y "assets" que sugieren puntos de acceso para desarrolladores o recursos digitales críticos.

Varias URLs que contienen cadenas de texto aleatorias o nombres de proyectos que podrían corresponder a desarrollos internos o infraestructura no destinada al acceso público.

Estos hallazgos indican posibles vectores de información que podrían ser de interés para auditorías de seguridad y análisis de vulnerabilidades más detallados.



Después de lo anterior hicimos un único archivo para que al juntarlos todos tener todo en un mismo lugar y poder pasar a la fase de *Fingerprinting lo más organizados posible*, lo realizamos mediante el comando:

***Cat subdominios\_\* | unfurl –d domains > subdominios\_a\_revisar.txt***

## Fase de FingerPrinting

Fingerprinting con httpx

Proceso y Ejecución:

El fingerprinting de subdominios fue realizado utilizando la herramienta httpx, que permite inspeccionar los subdominios para identificar servicios web activos y sus tecnologías asociadas. El comando utilizado para esta operación fue:

***cat subdominios\_a\_revisar.txt | httpx -silent > objetivos\_limpios.txt***

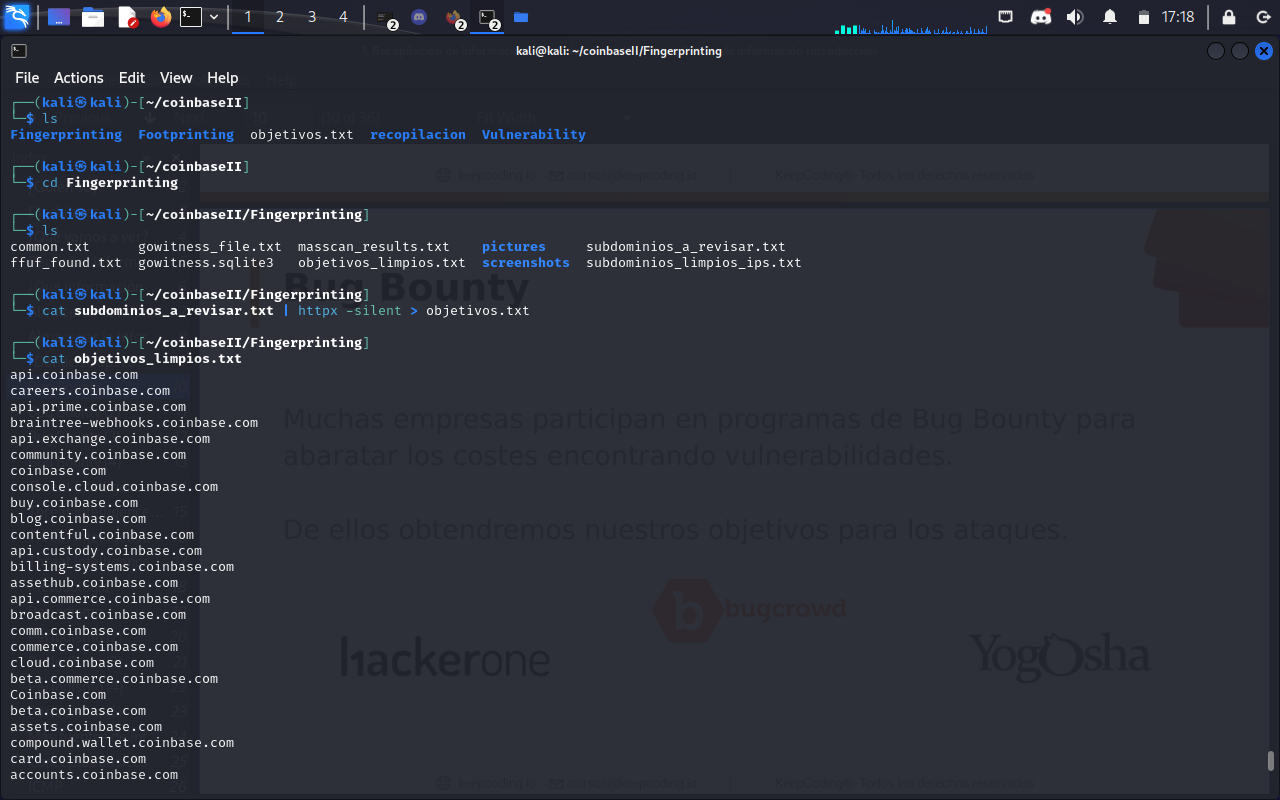
Esto nos permitió pasar una lista de subdominios a través de httpx y obtener detalles técnicos de los servicios activos y sus encabezados HTTP.

Hallazgos:

* Los resultados obtenidos con httpx proporcionaron una amplia visión de los subdominios activos bajo coinbase.com. Se identificaron varios subdominios que son de particular interés para el análisis de seguridad:
* Subdominios que indican entornos de desarrollo y pruebas (como sandbox.coinbase.com y dev.coinbase.com), que podrían ser vectores de ataque si no se gestionan adecuadamente.
* Puntos de acceso de APIs (como api.coinbase.com y api.exchange.coinbase.com), cruciales para la integración de servicios y posibles objetivos para la explotación de vulnerabilidades.

Subdominios asociados con servicios de atención al cliente y soporte técnico (como support.coinbase.com y help.coinbase.com), que contienen interfaces de usuario críticas.

Estos hallazgos son esenciales para la etapa de modelado de amenazas y planeación de pruebas de penetración, ya que resaltan componentes específicos de la infraestructura web que requieren un escrutinio de seguridad adicional.



Análisis de puertos con masscan:

Proceso y Ejecución:

Para descubrir puertos abiertos que podrían ser potenciales puntos de entrada para ataques, se utilizó Masscan, un escáner de puertos masivamente paralelo. Se configuró para escanear los rangos de puertos más comunes asociados con servicios conocidos y administrativos:

Análisis de Puertos con Masscan

Proceso y Ejecución:

Para descubrir puertos abiertos que podrían ser potenciales puntos de entrada para ataques, se utilizó Masscan, un escáner de puertos masivamente paralelo. Se configuró para escanear los rangos de puertos más comunes asociados con servicios conocidos y administrativos:

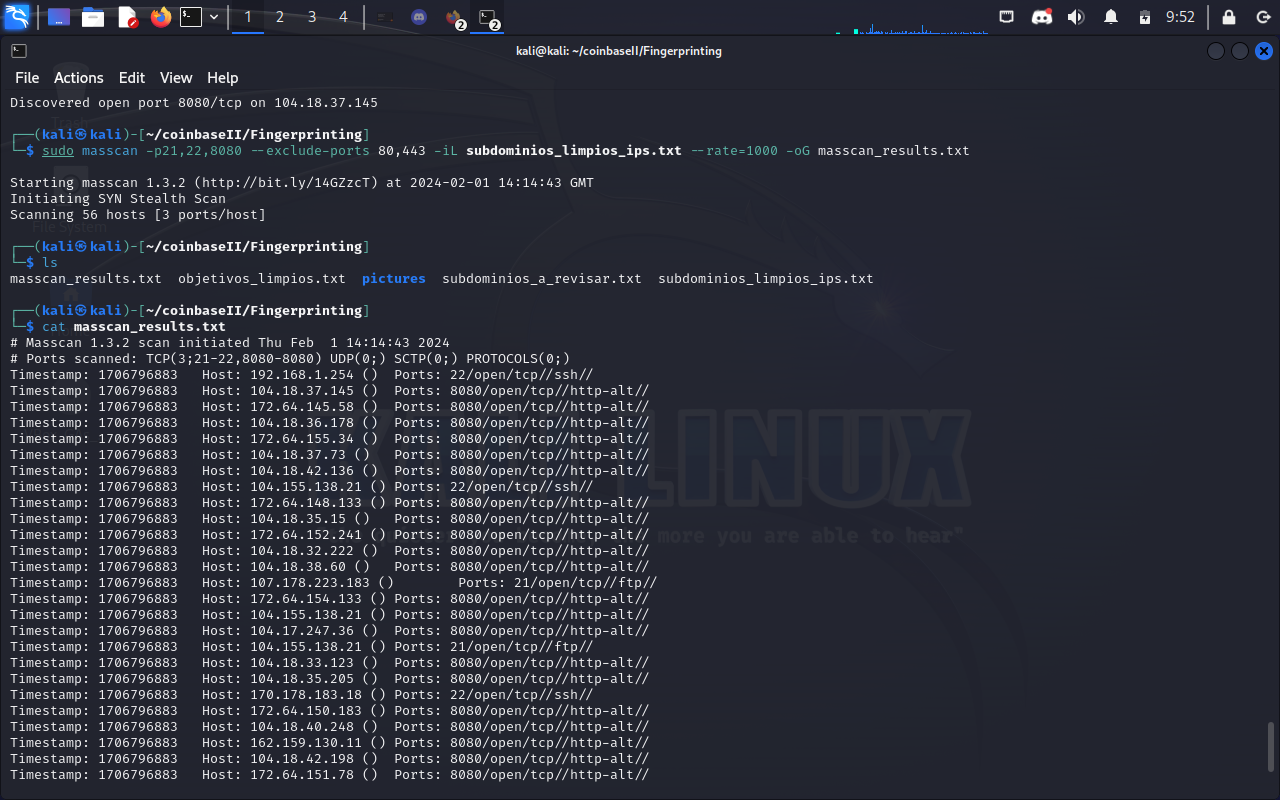
***sudo masscan -p21,22,8080 –exclude-ports 80,443 –iL subdominios\_limpios.txt –rate=1000 oG masscan\_results.txt***

Hallazgos:

La ejecución de Masscan permitió identificar varios puertos abiertos en distintas direcciones IP dentro del rango de la red de coinbase.com. Los puertos más significativos incluyen:

* Puerto 22 (SSH): Encontrado abierto en múltiples hosts, sugiriendo puntos de administración remota.
* Puerto 8080 (HTTP alternativo): Comúnmente utilizado para pruebas de aplicaciones web o servicios proxy, fue identificado en varios hosts.
* Puerto 21 (FTP): Un protocolo menos seguro para la transferencia de archivos, presente en una minoría de hosts.

La presencia de estos puertos abiertos es un hallazgo relevante para la evaluación de seguridad, ya que cada uno presenta diferentes perfiles de riesgo y requiere una gestión de seguridad adecuada.



Análisis visual con gowitness

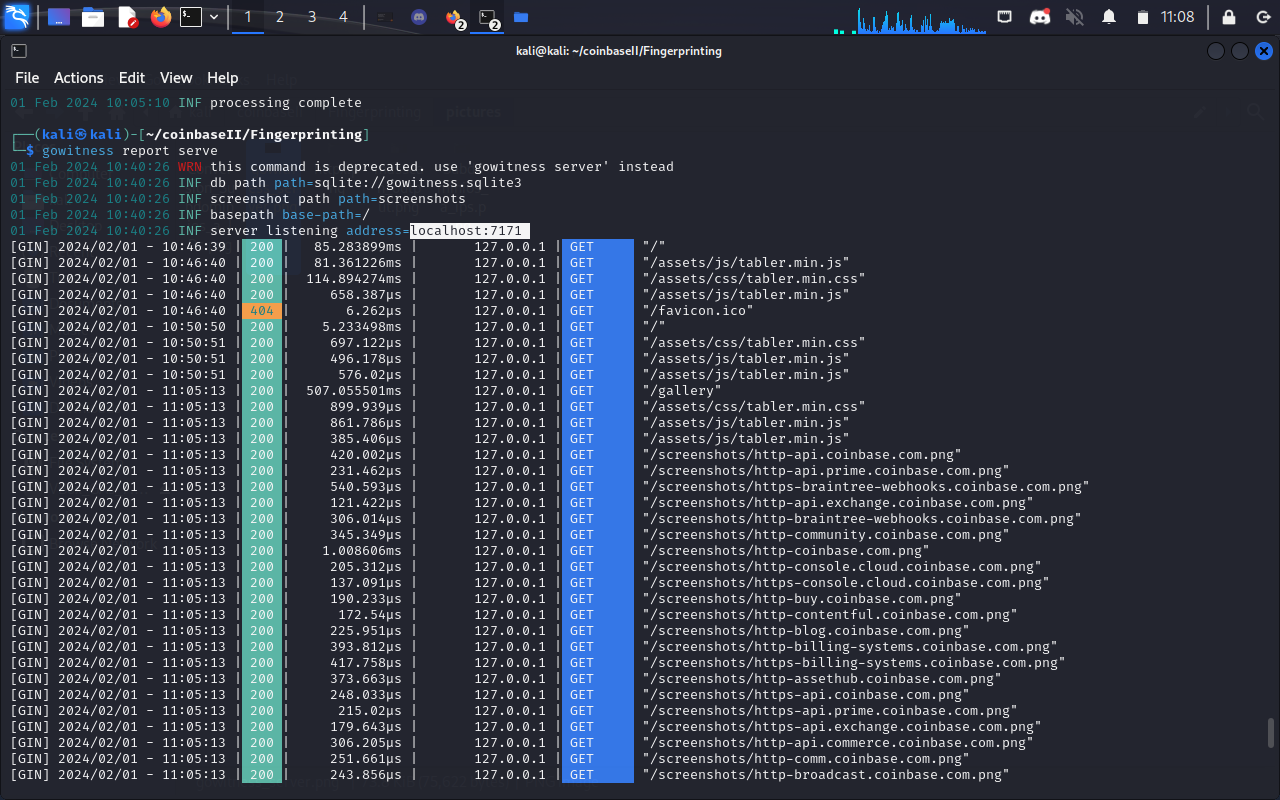
Proceso y Ejecución:

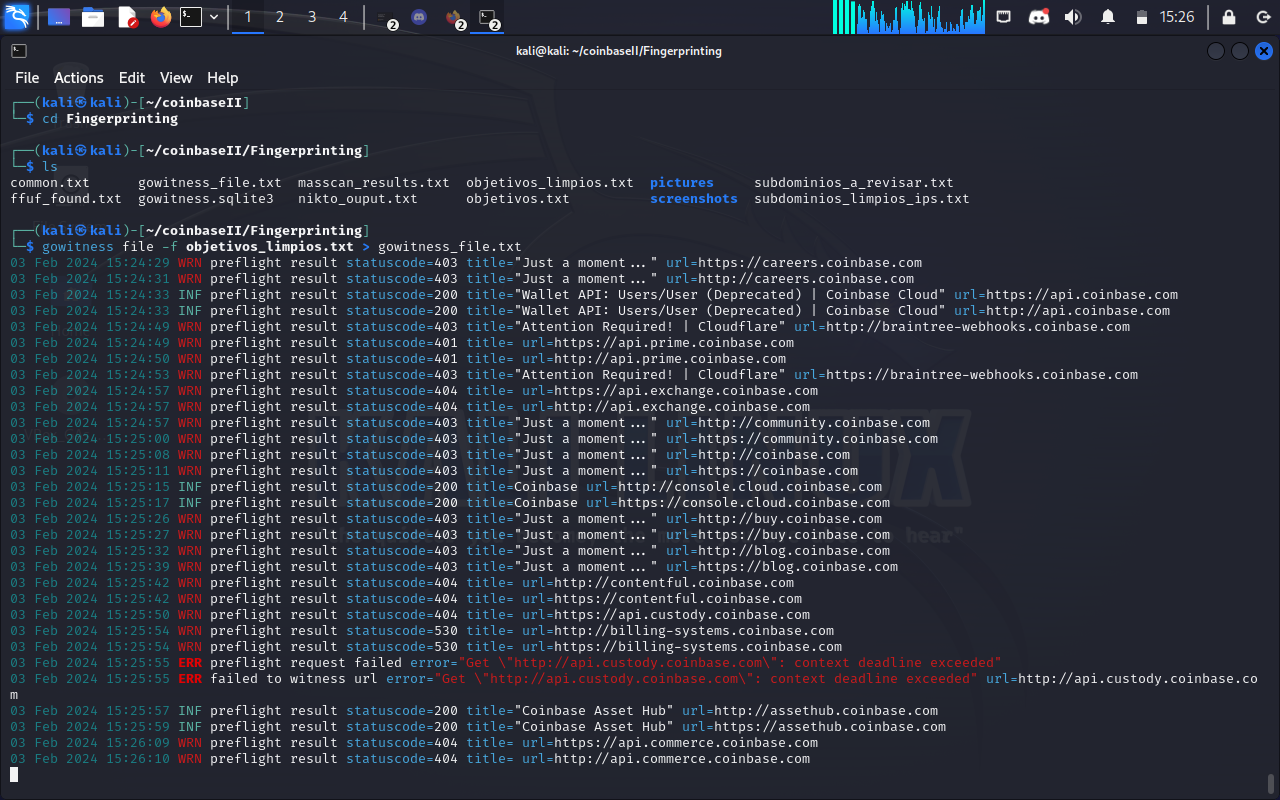
Para realizar un análisis visual de coinbase.com, se empleó GoWitness, una herramienta que toma capturas de pantalla de sitios web. Este proceso se llevó a cabo ejecutando GoWitness en un rango de direcciones IP y subdominios relevantes para obtener una representación visual de los servicios web en ejecución.

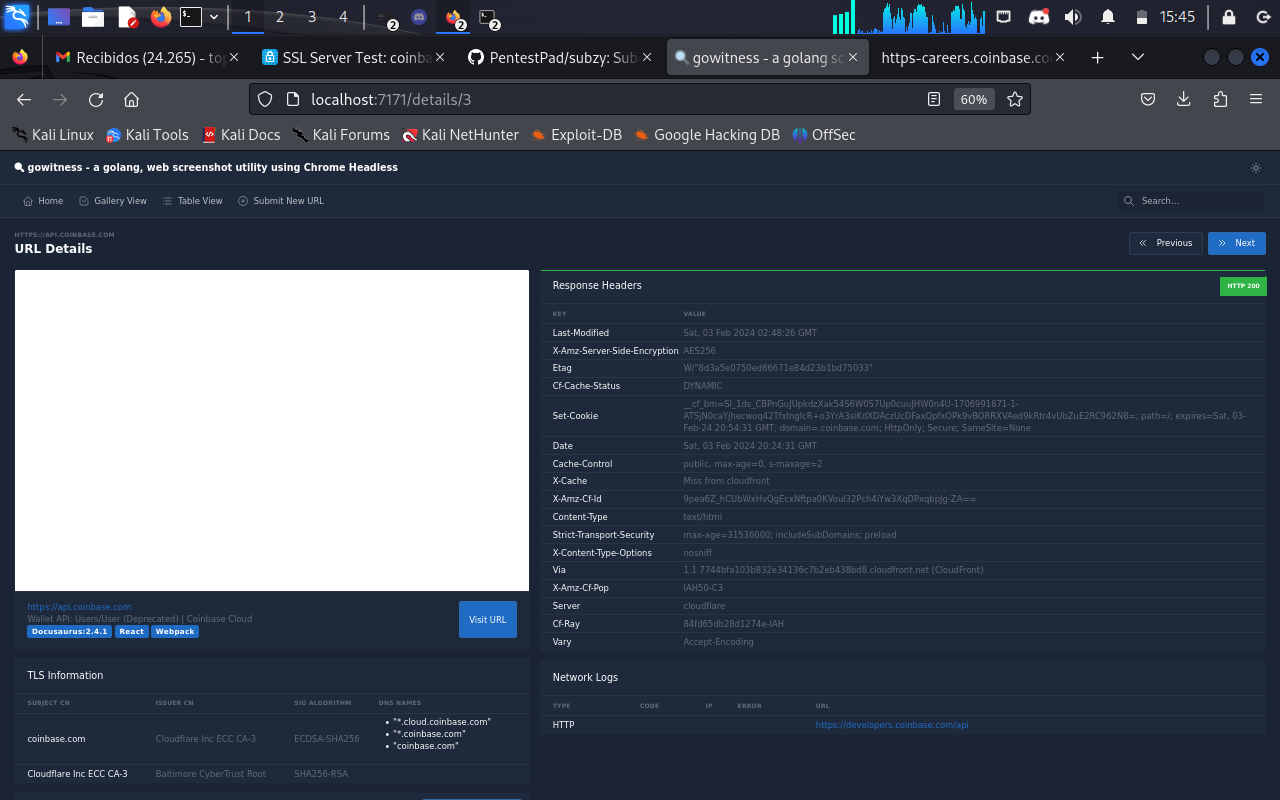
Hallazgos:

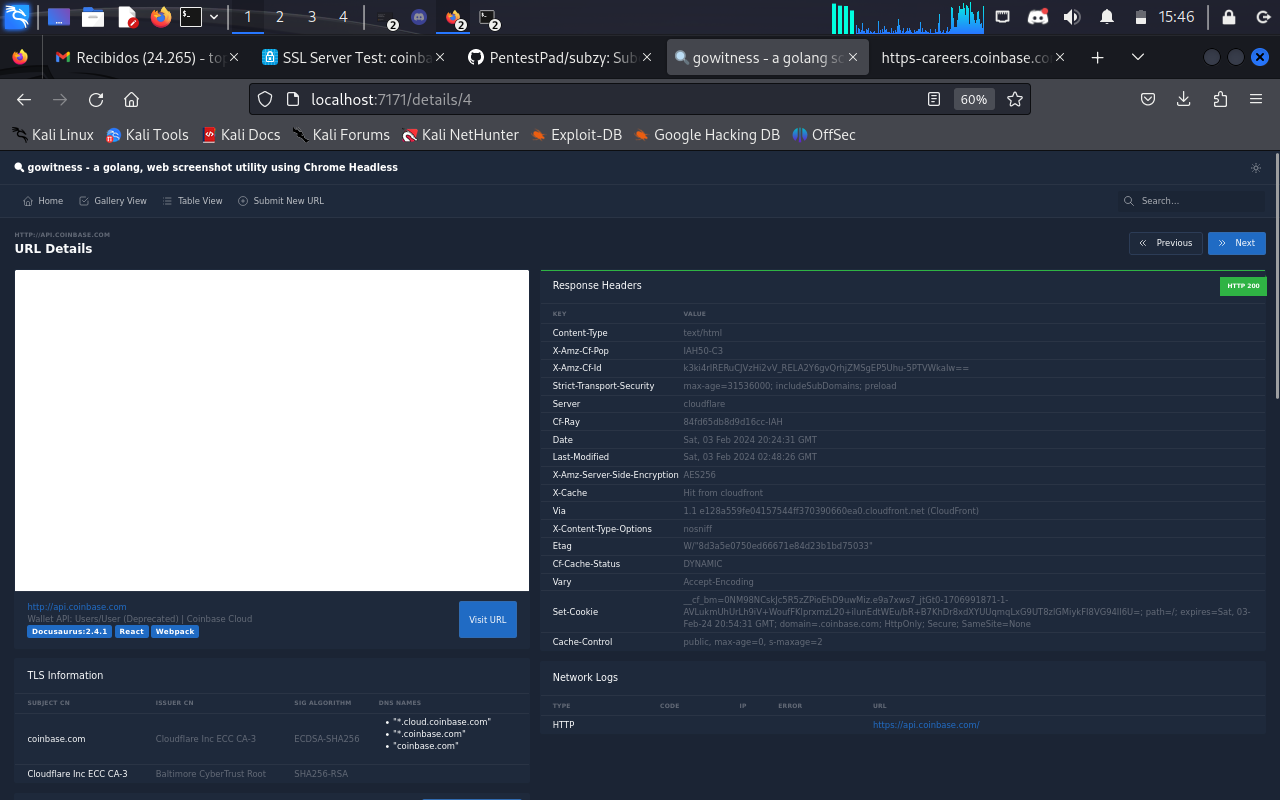
* La herramienta GoWitness permitió la captura de numerosas interfaces web asociadas a los subdominios de coinbase.com. Algunas de las capturas revelaron:
* Interfaces de usuario estándar, como portales de inicio de sesión y paneles de control.
* Páginas de error y redirecciones que podrían indicar configuraciones incorrectas o áreas olvidadas en la web.
* Páginas de servicios API que ofrecen una mirada más cercana a los puntos de integración y consumo de datos.

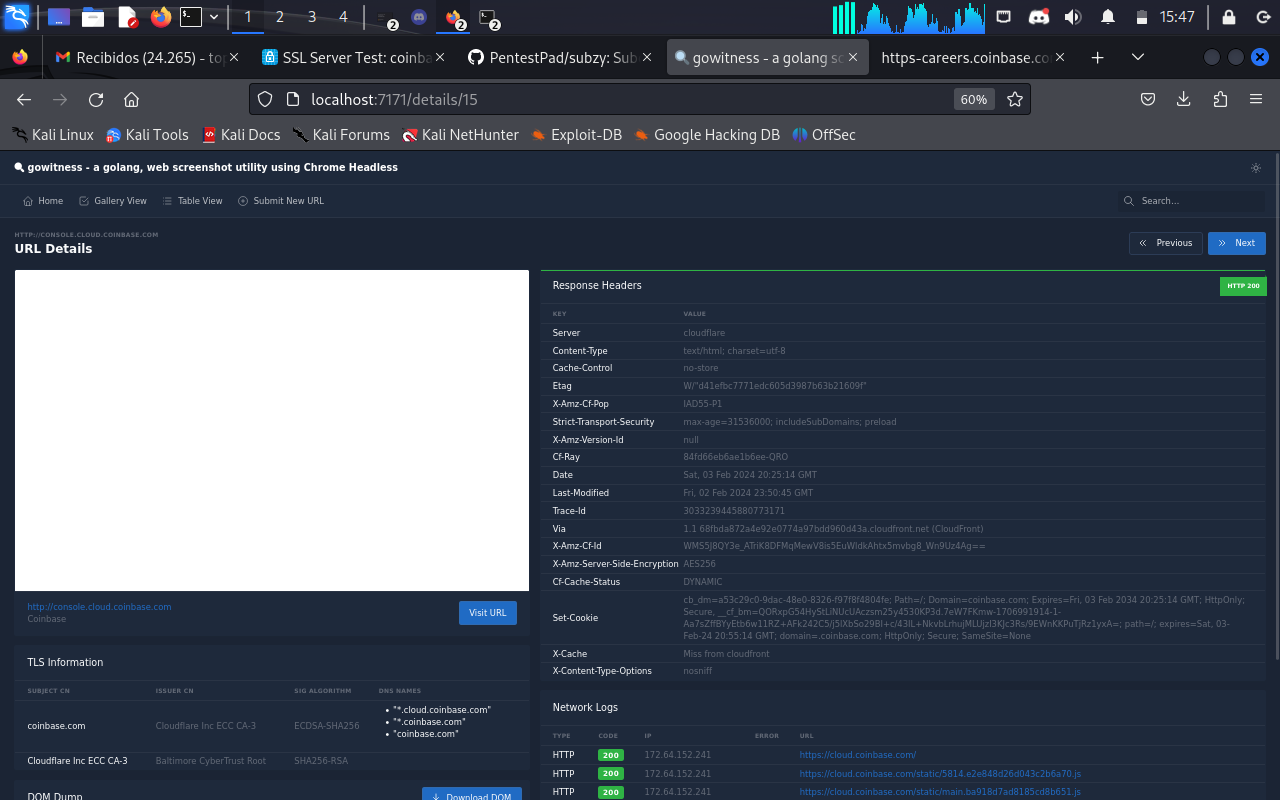
Estas capturas visuales son valiosas para identificar posibles vectores de ataque basados en la interfaz de usuario y para complementar la información recopilada durante el análisis de puertos y servicios.

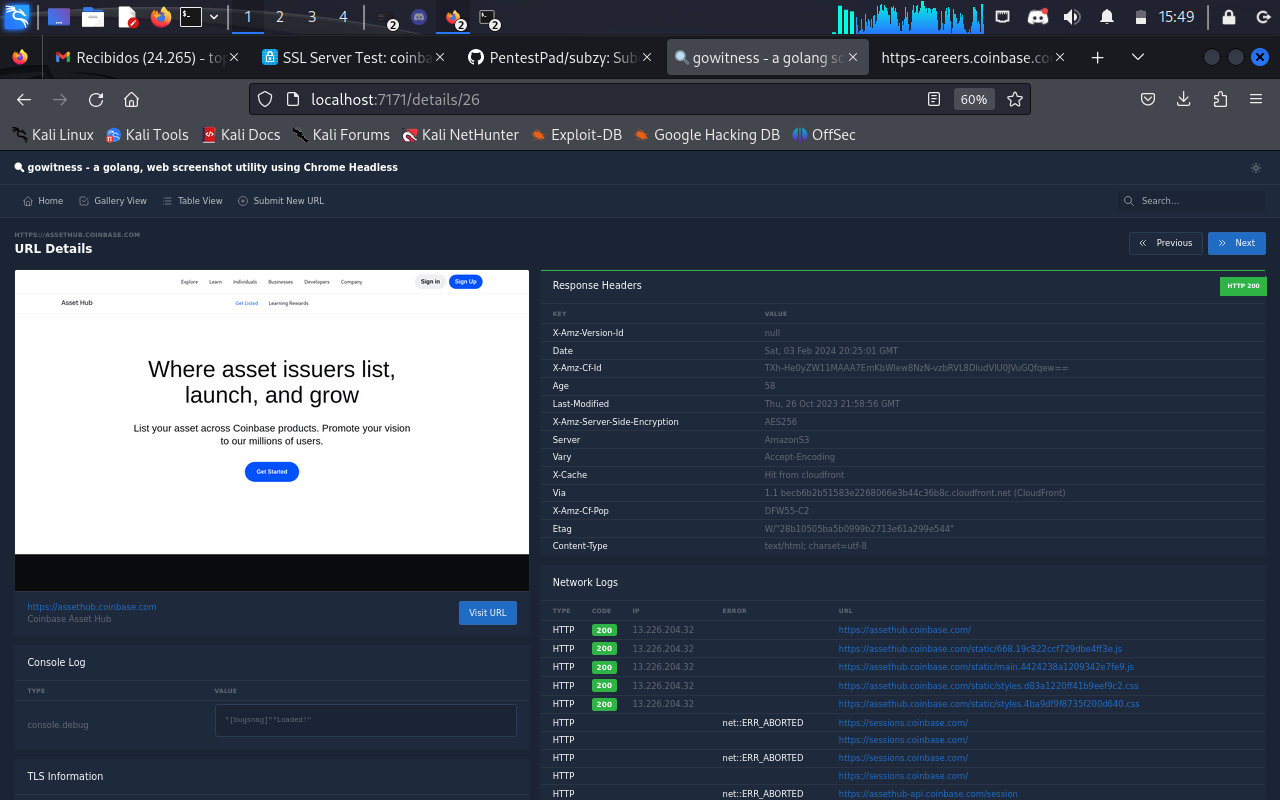


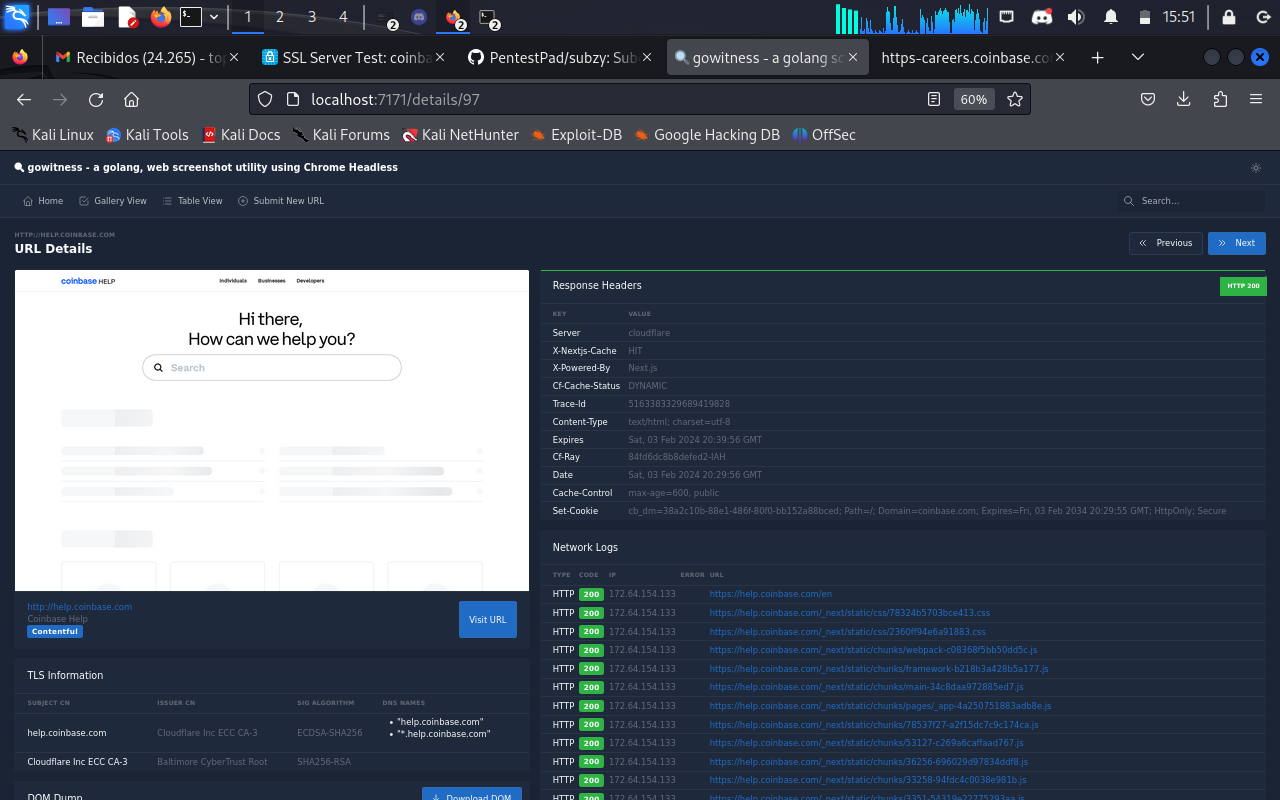


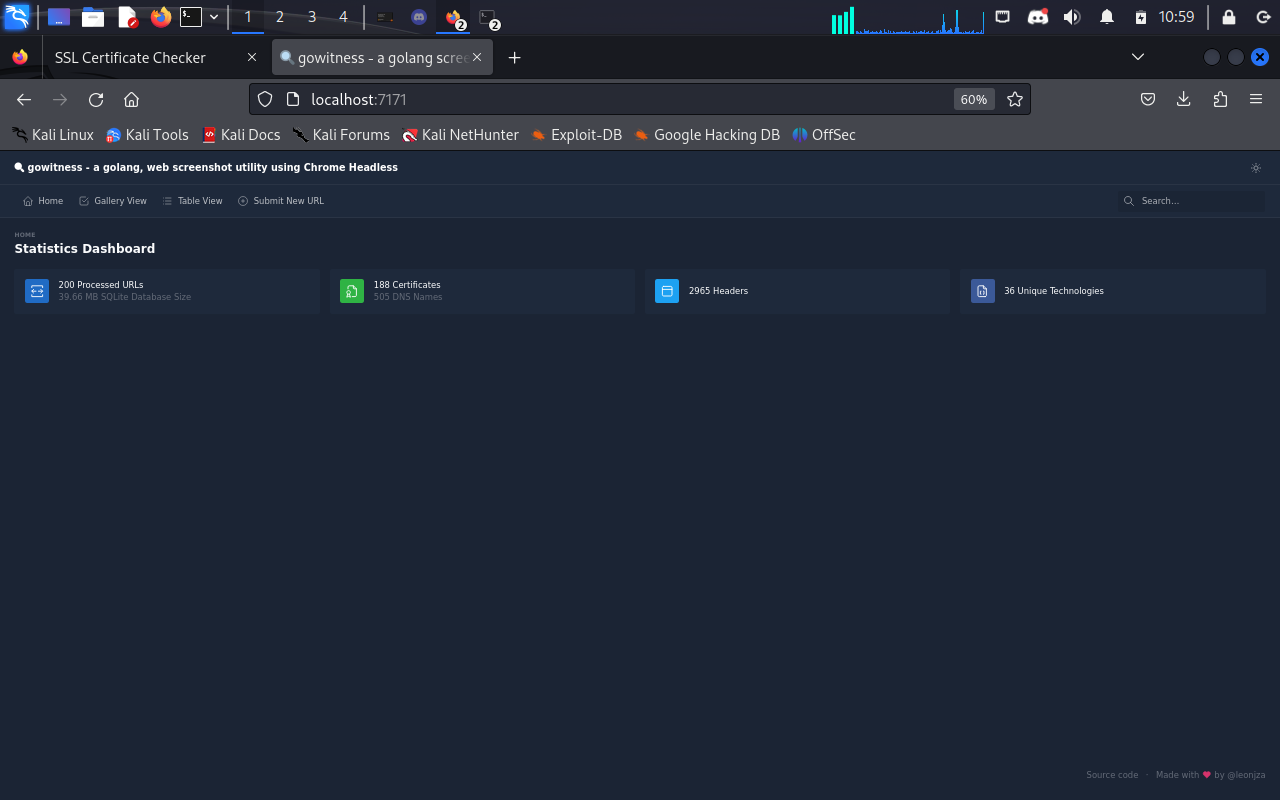












Análisis de firewall con Wafw00f

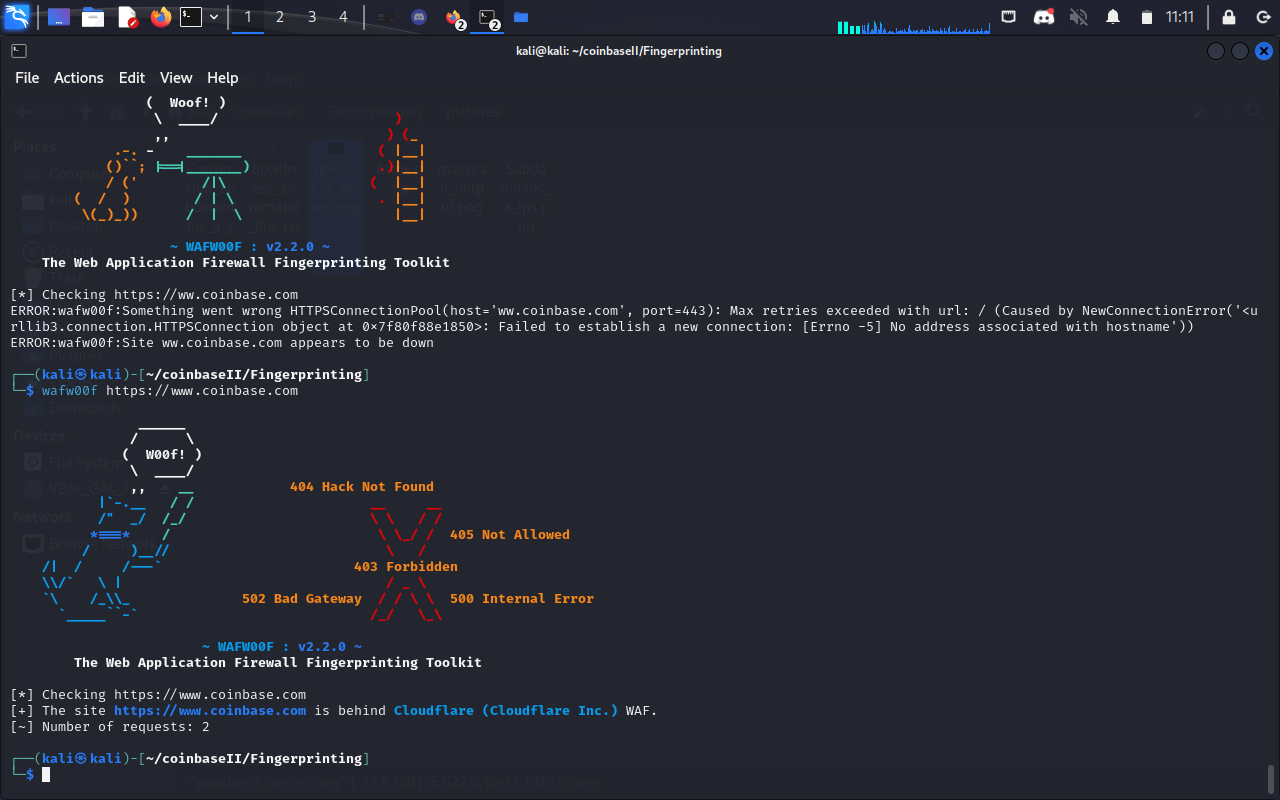
Proceso y Ejecución:

Se utilizó la herramienta WAFW00F para identificar la presencia de firewalls de aplicaciones web (WAF) en coinbase.com. WAFW00F realiza solicitudes a la web y analiza las respuestas para determinar si hay un WAF protegiendo el sitio. El comando ejecutado fue:

***wafw00f*** [***https://www.coinbase.com***](https://www.coinbase.com)

Hallazgos:

El resultado indicó que coinbase.com está protegido por Cloudflare, que es un WAF reconocido por su eficacia en la protección contra amenazas web comunes y ataques DDoS. Además, WAFW00F intentó realizar conexiones a coinbase.com, pero algunas solicitudes no se completaron, lo que sugiere que el WAF está configurado para bloquear ciertas acciones que podrían ser interpretadas como maliciosas o no deseadas.



Enumeración de directorios y ficheros con ffuf

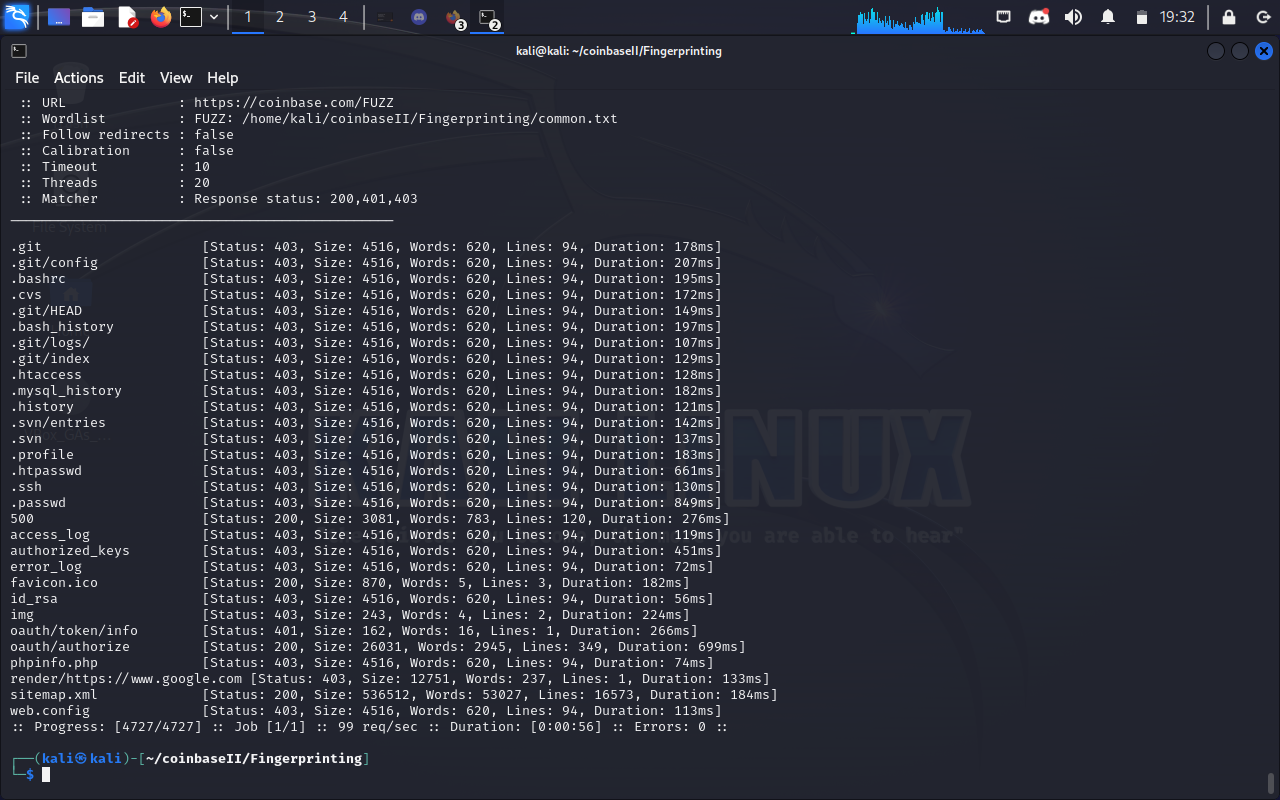
Proceso y Ejecución:

Para identificar directorios y archivos en coinbase.com, se utilizó la herramienta ffuf, que es un fuzzer rápido para la web. Este enfoque nos permite descubrir recursos y rutas ocultos que no están directamente enlazados o visibles. El comando utilizado para el análisis fue:

***ffuf -w wordlist.txt -u*** [***https://coinbase.com/FUZZ***](https://coinbase.com/FUZZ)

Hallazgos:

El escaneo con ffuf reveló múltiples rutas y archivos que devolvieron un estado HTTP 403, indicando que están presentes pero no son accesibles públicamente. Un estado HTTP 401 para ciertos endpoints sugiere la necesidad de autenticación. Se identificaron archivos y rutas específicas como .git, .htaccess, y sitemap.xml con respuestas variadas, incluyendo estados 200 y 403, lo cual puede señalar áreas de interés para la revisión de seguridad más detallada.



Identificación de vulnerabilidades con nuclei

Proceso y Ejecución:

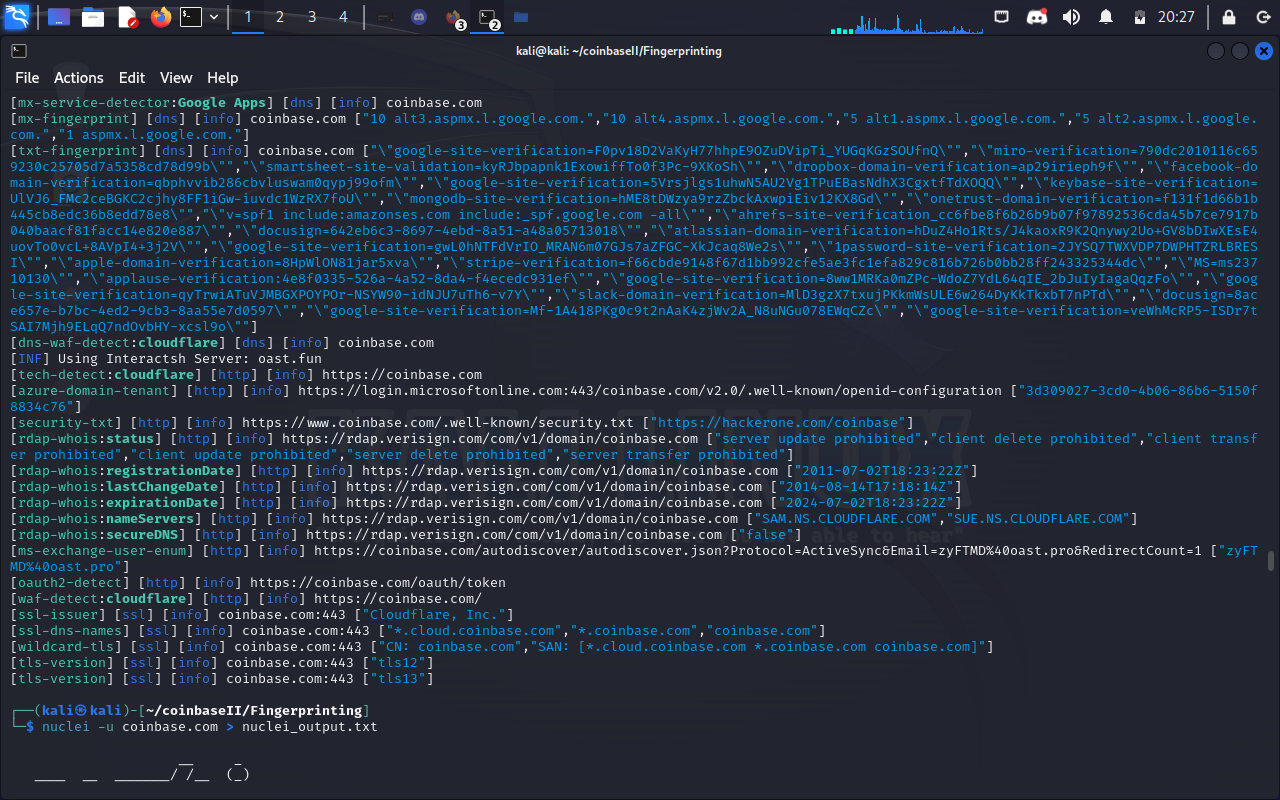
Se implementó Nuclei, una herramienta de escaneo de vulnerabilidades, para realizar un análisis dirigido en coinbase.com. Nuclei utiliza plantillas para buscar problemas de seguridad conocidos y configuraciones erróneas en aplicaciones web.

Hallazgos:

Nuclei identificó varios puntos de información a través de DNS y HTTP que son útiles para el análisis de seguridad:

* Se detectaron servicios de correo electrónico a través de MX records, lo que indica la utilización de servicios de correo de Google.
* La presencia de un Web Application Firewall (WAF) de Cloudflare fue confirmada, lo cual es importante para cualquier consideración de prueba de penetración, ya que Cloudflare puede bloquear o alterar el tráfico malicioso.
* Fueron encontrados registros TXT y CAA que incluyen verificaciones de dominio y políticas de seguridad de correo electrónico.
* Se confirmaron configuraciones de TLS, incluyendo el soporte para TLS 1.2 y TLS 1.3.

Estos descubrimientos ofrecen una comprensión más profunda de la postura de seguridad de coinbase.com, subrayando áreas que podrían necesitar atención o que podrían ser aprovechadas para fortalecer la seguridad general.



Análisis de seguridad con nikto

Proceso y Ejecución:

Se realizó un escaneo de seguridad en coinbase.com utilizando Nikto, una herramienta de evaluación web que busca diversos tipos de vulnerabilidades. Este comando se ejecutó para comenzar el escaneo:

***nikto –h*** [***www.coinbase.com***](http://www.coinbase.com)

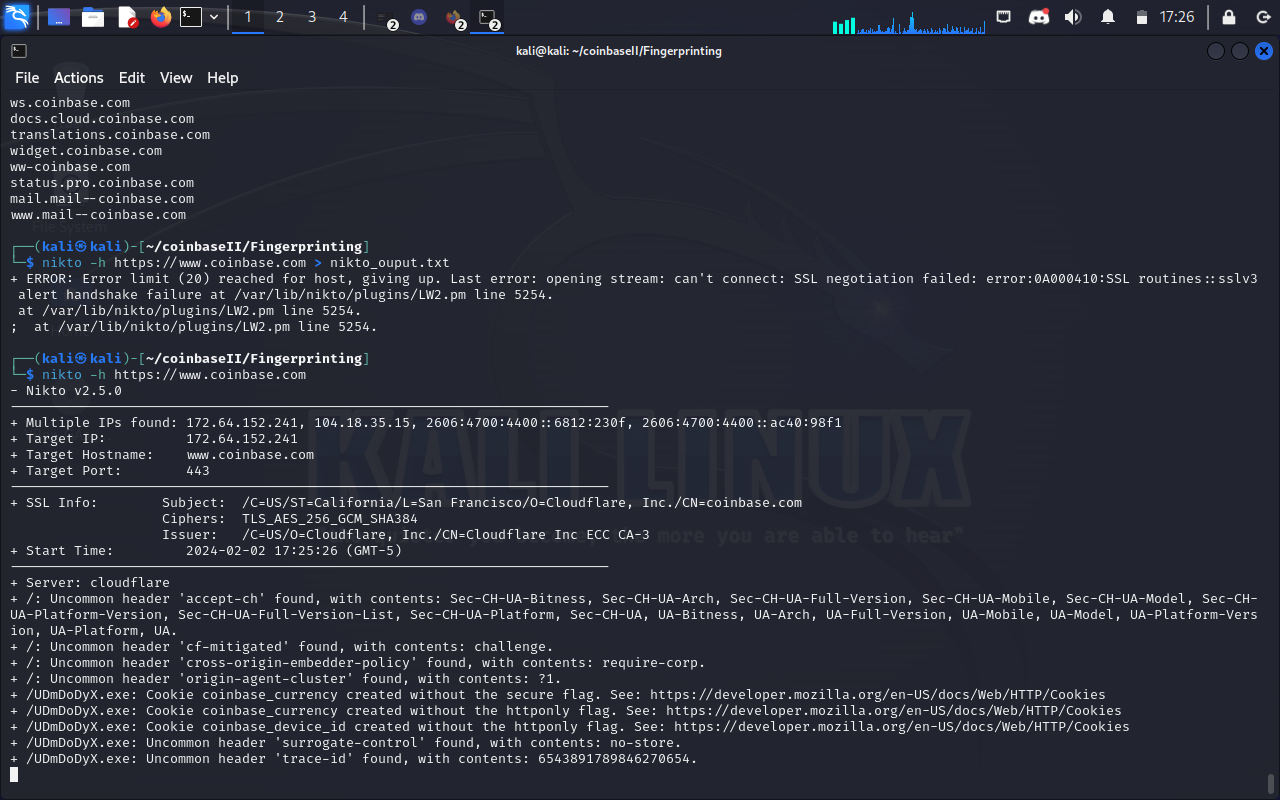
Hallazgos:

El escaneo de Nikto identificó varios aspectos importantes:

Se detectaron múltiples respuestas con estado HTTP 403 en archivos y directorios sensibles, lo que indica que están presentes pero protegidos por restricciones de acceso.

* Se encontraron cookies establecidas sin las banderas Secure ni HttpOnly, lo que podría aumentar el riesgo de ataques como el secuestro de sesión o Cross-Site Scripting (XSS).
* Hubo una discrepancia entre el nombre de host y el nombre en el certificado SSL, lo que podría indicar problemas de configuración o posibles vulnerabilidades.
* Se observaron cabeceras y métodos inusuales que podrían revelar información sobre la infraestructura subyacente del servidor.

Estos hallazgos sugieren áreas donde coinbase.com podría mejorar sus prácticas de seguridad para protegerse mejor contra ataques web.



Evaluación de subdominio takeover con subzy

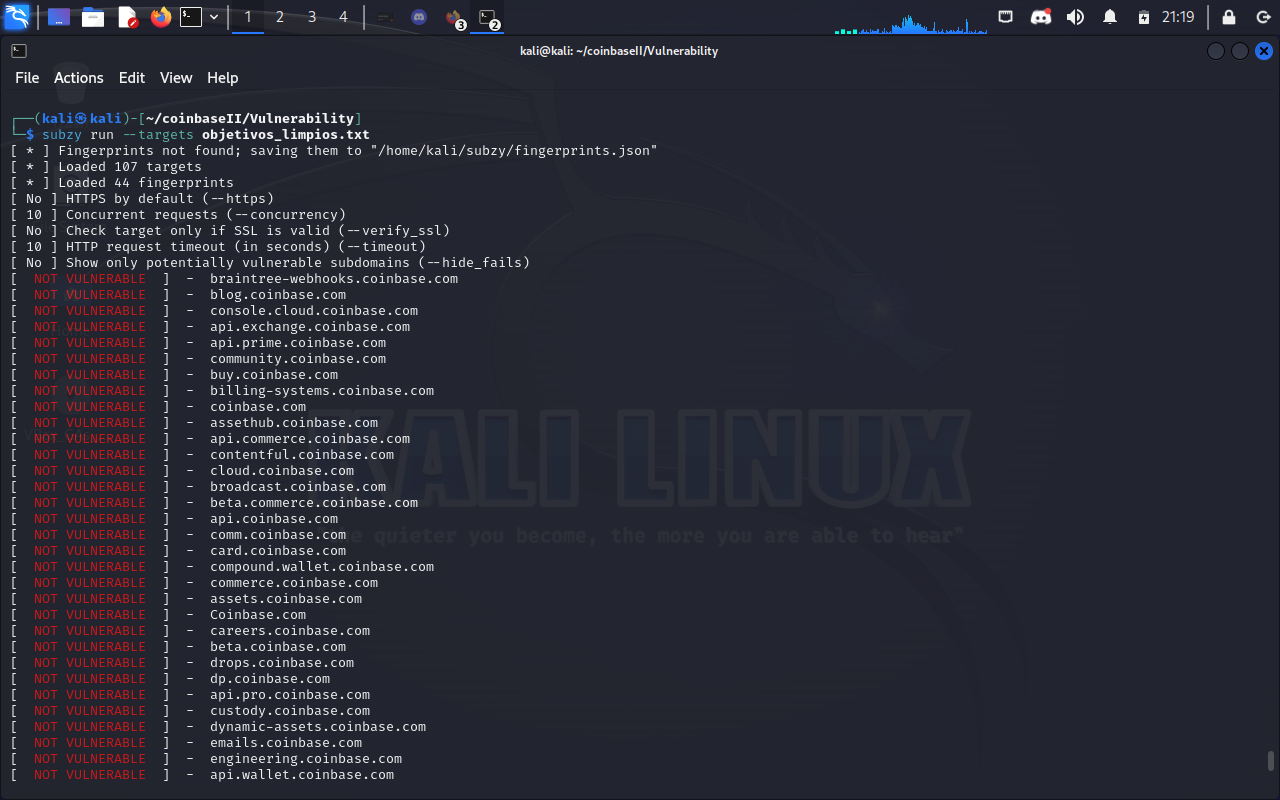
Proceso y Ejecución:

Subzy, una herramienta especializada en la detección de vulnerabilidades de subdominio takeover, fue utilizada para evaluar los subdominios de coinbase.com. Se ejecutó con el objetivo de identificar subdominios que apuntan a servicios en la nube sin la debida configuración, lo que podría permitir que un atacante tome el control de estos subdominios. Se utilizó el comando siguiente:

***Subzy run –targets objetivos\_limpios.txt***

Hallazgos:

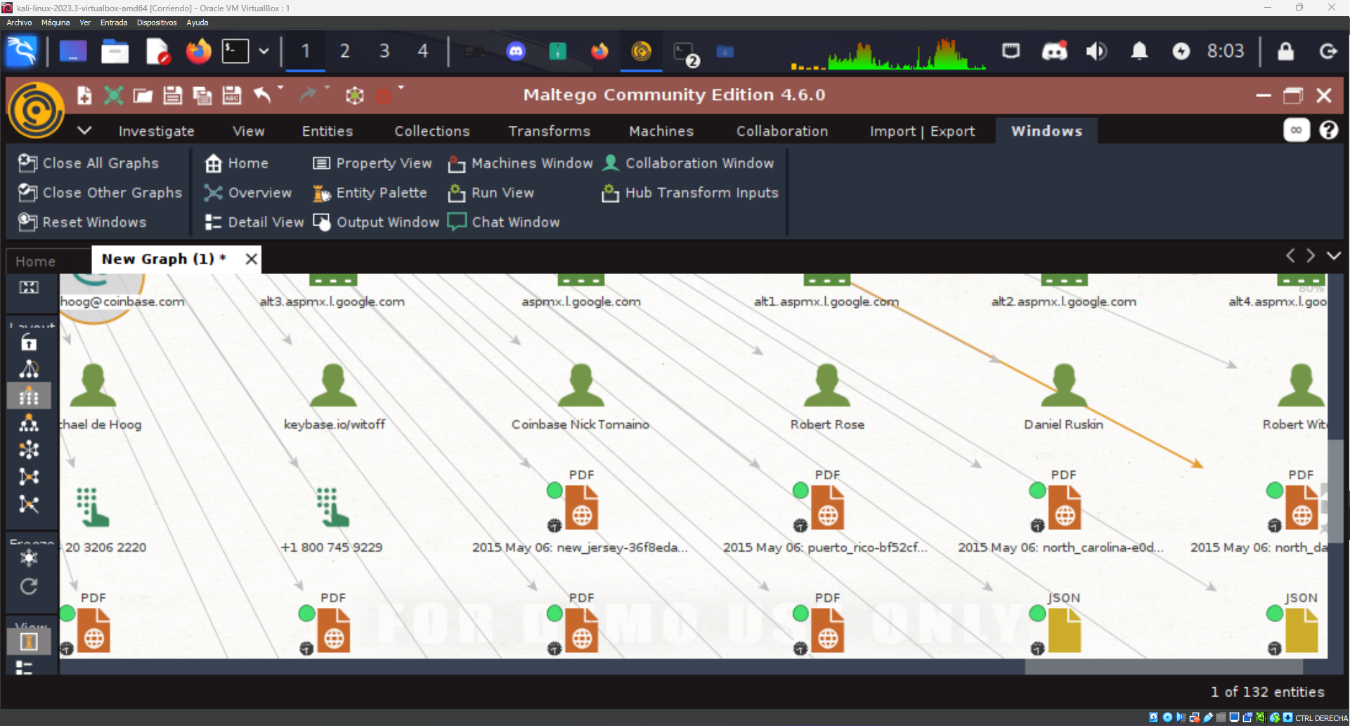
La herramienta Subzy confirmó que todos los subdominios probados no son vulnerables a subdominio takeover. A pesar de varios errores HTTP observados, que podrían necesitar investigación adicional, la ausencia de vulnerabilidades de takeover indica una configuración robusta y una gestión adecuada de los registros DNS y los servicios en la nube asociados con los subdominios de coinbase.com



Open Source Inteligence(OSINT)

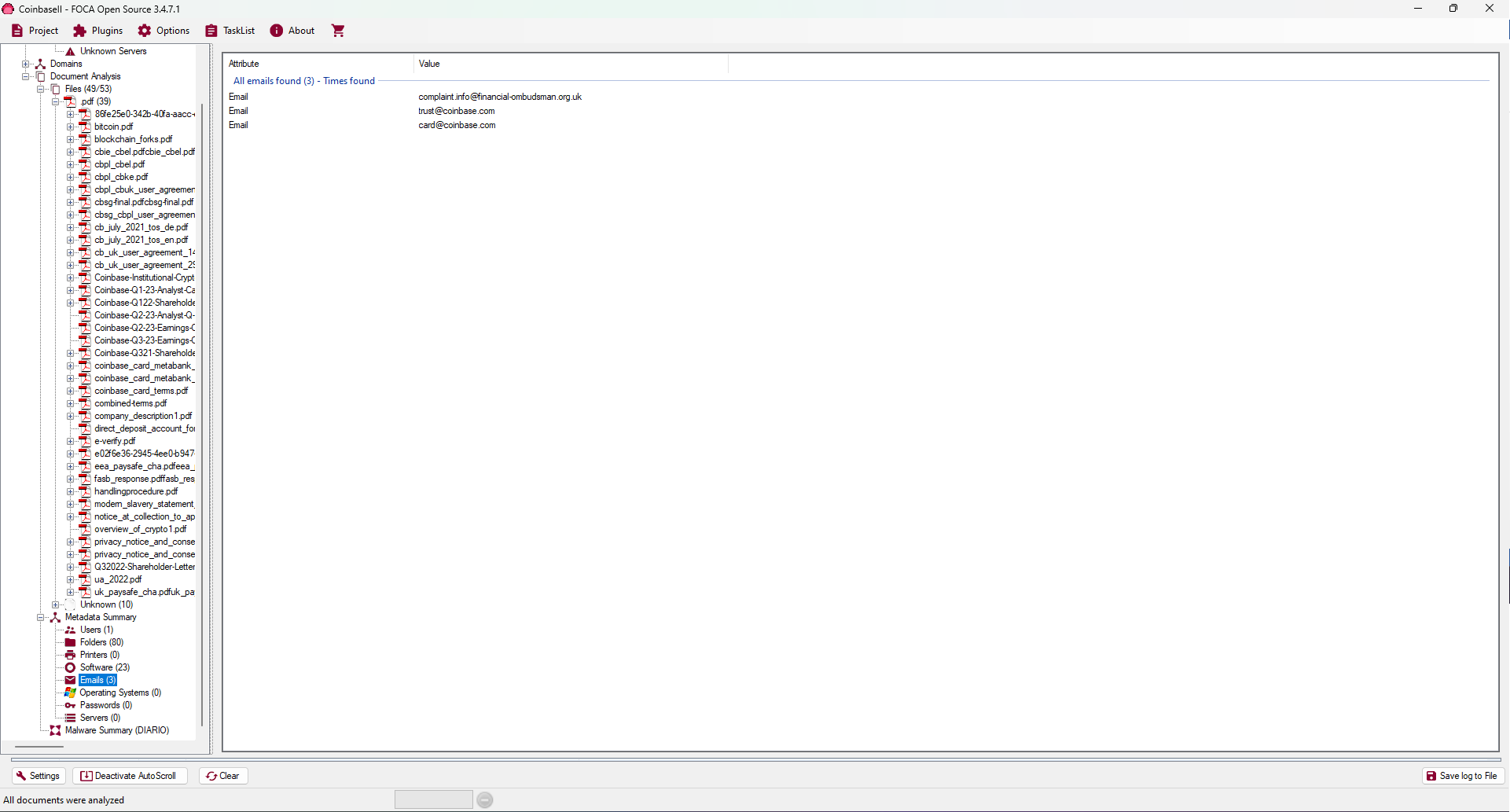
Utilizando la herramienta maltego preinstalada en Kali Linux hemos descubierto que, dentro de los trabajadores “de peso” que laboran para la organización, son los visualizados en la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Puesto | Correo electrónico asociado | Perfil linkedln |
| Brian Armstrong | CEO Cofunder | [Brian@coinbase.com](mailto:Brian@coinbase.com) | [linkedin.com/in/brian-armstron-8a667722](https://www.linkedin.com/in/brian-armstron-8a667722) |
| Michael de Hoog | Software Engineer | [Michel.dehoog@coinbase.com](mailto:Michel.dehoog@coinbase.com) | [linkedin.com/in/michael-de-hoog-a572b171](https://www.linkedin.com/in/michael-de-hoog-a572b171) |
| Hao Xue | Engineering manager | [Hao.su@coinbase.com](mailto:Hao.su@coinbase.com) | [linkedin.com/in/hao-xue-5ba440155](https://www.linkedin.com/in/hao-xue-5ba440155) |
| Ivan Ledyashov | Security Technical Program Management | [Ivan.ledyashov@coinbase.com](mailto:Ivan.ledyashov@coinbase.com) | [linkedin.com/in/ledivan](https://www.linkedin.com/in/ledivan) |
| Roger Bartlet | Institutional Operations Solutions & Coinbase Treasury Head at Coinbase | [Roger.bartlet@coinbase.com](mailto:Roger.bartlet@coinbase.com) | [linkedin.com/in/roger-bartlett-14713020](https://www.linkedin.com/in/roger-bartlett-14713020) |
| Emilie Choi | President and Chief Operation Officer, Coinbase | [emilie.choi@coinbase.com](mailto:emilie.choi@coinbase.com) | [linkedin.com/in/emiliechoi](https://www.linkedin.com/in/emiliechoi) |



Revisión de metadatos en Documentación Pública

Durante la misma fase de OSINT, se realizó un análisis exhaustivo de metadatos en documentos accesibles al público asociados a coinbase.com mediante la herramienta FOCA. Este examen se enfocó en identificar información que pudiera revelar detalles internos de la organización. Sin embargo, los resultados indicaron que los documentos habían sido limpiados de metadatos sensibles, lo que sugiere una práctica consciente de higiene digital por parte de Coinbase. Este procedimiento de limpieza refleja una postura de seguridad informada y reduce significativamente el vector de ataque que los metadatos podrían representar.



Recomendaciones:

* Mantener una vigilancia continua sobre la aparición de nuevos subdominios y revisar regularmente la seguridad de los mismos.
* Continuar con la política de seguridad para la eliminación de metadatos en todos los documentos públicos.
* Reforzar las configuraciones de seguridad donde se identificaron debilidades, especialmente en lo que respecta a cookies y encabezados HTTP.
* Considerar una revisión de la configuración SSL/TLS para garantizar la alineación del nombre del host con el certificado SSL.
* Realizar una auditoría de seguridad interna basada en los hallazgos de este informe para abordar y mitigar cualquier vulnerabilidad potencial.

Conclusiones:

Este ejercicio de recopilación de información ha proporcionado una visión detallada y valiosa de la postura de seguridad de coinbase.com. A pesar de las fuertes medidas de seguridad observadas, como la protección mediante WAF y la limpieza proactiva de metadatos, siempre hay margen de mejora. Las recomendaciones proporcionadas buscan fortalecer aún más la infraestructura de seguridad de Coinbase y prepararla mejor para enfrentar las amenazas en constante evolución del ciberespacio.