CONFIDENCIAL.

Andrés Jesús Ricaurte Valera
KEEPCODING | RED TEAM

Fecha: 25/05/2025

Informe entregado para:
KeepCoding

ÍNDICE.

CONFIDENCIALIDAD.

Este documento es de exclusiva propiedad de mi persona Andres Jesus Ricaurte Valera y de KeepCoding. Este documento contiene información propietaria y confidencial.

CONTACTO.

Nombre	Cargo	Contacto
Pablo Andres Jesus Ricaurte Valera	Profesor Alumno	Pablo@correo.com Andresricv@outlook.es

1. OBJETIVO.

El objetivo de este ejercicio es realizar una planificación y un reconocimiento inicial de la organización remitly.com con el fin de identificar su superficie de exposición pública en internet. A través de técnicas de recolección de información pasiva y activa no intrusiva, se busca:

- Obtener una visión general de los activos digitales visibles públicamente.
- Establecer un alcance preliminar para futuros análisis de seguridad.
- Identificar dominios, subdominios, sistemas autónomos y rangos de red asociados a la empresa.
- Priorizar dichos activos según su relevancia y posible exposición a vectores de ataque.

Este reconocimiento se desarrolla con fines académicos y bajo un enfoque ético, sin realizar pruebas agresivas ni intentos de explotación de vulnerabilidades.

2. ALCANCE.

El presente ejercicio se limita a realizar un reconocimiento externo de la empresa remitly.com mediante técnicas de enumeración pasiva y activa no intrusiva. El análisis se enfocará exclusivamente en activos públicos, sin interactuar directamente con los sistemas ni realizar escaneos agresivos.

Este subdominio expone los endpoints de la API pública y privada, utilizada por aplicaciones móviles/web para interactuar con la plataforma.

Importancia:

- Facilita el envío de dinero, validación de usuarios, y seguimiento de transacciones.
- Posiblemente expone endpoints como:
- /v1/transactions

- /v1/users/login
- /v1/rates

Riesgos potenciales:

- Enumeración de endpoints (si no hay buena documentación controlada).
- Falta de autenticación en alguna ruta.
- Malas prácticas CORS o políticas laxas de origen.
- Ataques de tipo API abuse, rate-limiting bypass o data scraping.

Herramientas útiles para análisis:

curl, httpx, whatweb, Burp Suite (modo pasivo).

1- auth.remitly.com – (Sistema de autenticación de usuarios).

Función:

- Módulo central para la autenticación y autorización. Puede implementar:
- Inicio de sesión
- Recuperación de contraseña
- Tokens de sesión
- MFA (multi-factor authentication)

Importancia:

- Punto crítico de entrada para usuarios y administradores.
- Malas configuraciones podrían comprometer credenciales, tokens o sesiones.

Riesgos potenciales:

- Redirecciones abiertas.
- Autenticación débil o sin MFA.
- Fugas de tokens JWT en headers.
- Sesiones que no expiran correctamente.

Herramientas útiles para análisis:

curl -I, wappalyzer, nmap --script http*, jwt.io

2- kyc.remitly.com – (Know Your Customer - Verificación de identidad).

Función:

Este subdominio está orientado al proceso KYC: subida de documentos, selfies, comprobantes de identidad. Podría estar integrado con servicios como Jumio, Onfido o Sumsub.

Importancia:

- Procesa documentación sensible: pasaportes, DNIs, selfies.
- Obligatorio por regulaciones internacionales (AML, FATF, etc.)

Riesgos potenciales:

- Fugas de archivos o almacenamiento inseguro.
- Falta de cifrado en tránsito o almacenamiento.
- Formulario vulnerable a ataques de tipo CSRF o XSS.

Herramientas útiles para análisis:

curl, Burp, revisión de headers de seguridad (Content-Security-Policy, X-Frame-Options).

3- support.remitly.com – (Plataforma de soporte a clientes).

Función:

Centro de ayuda, tickets, respuestas automatizadas. Probablemente vinculado a una solución de terceros (Zendesk, Freshdesk o Salesforce).

Importancia:

- Punto de contacto entre usuarios y soporte técnico.
- Puede exponer emails, historial de tickets y problemas técnicos.
- Riesgos potenciales:
- Enumeración de tickets o usuarios.
- Filtración de información personal por errores de permisos.
- Vectores para ingeniería social (usuarios fingiendo ser soporte).

Herramientas útiles para análisis:

whatweb, wayback machine, Burp, Google Dorks.

4- careers.remitly.com – (Portal de empleo).

Función:

Subdominio usado para la publicación de vacantes, envío de CVs, y postulación.

Importancia:

- Aunque no parece técnico, puede revelar:
- Tecnologías internas usadas (en las descripciones)
- Ubicación de oficinas
- Estructura de equipos y líderes
- Peligroso desde el punto de vista de ingeniería social y OSINT laboral.

Riesgos potenciales:

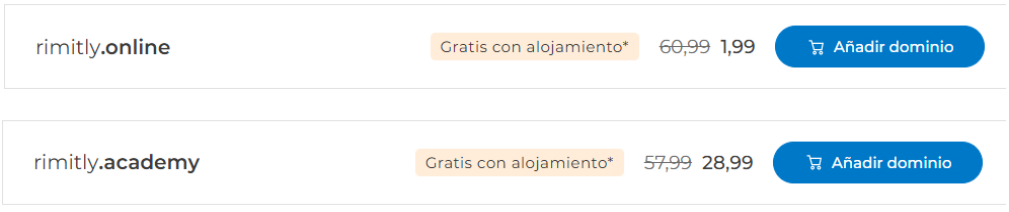
- Uso de subdominios de terceros (como lever.co, greenhouse.io).
- CVs o formularios expuestos públicamente.
- Descripciones que revelan arquitecturas o stacks tecnológicos internos.

Herramientas útiles para análisis:

Revisión manual, curl, Google Dorks, búsqueda en archive.org

2.1.1. DOMINIOS PARA PHISHING.

Se ha hecho una investigación a través de páginas de ventas de dominio, donde podemos conseguir dominios muy interesantes para hacer phishing.



rimitly.bi 94,99 Añadir dominio

3. DIRECCIONES IP.

A continuación se mostrarán las direcciones IP públicas asociadas al dominio principal.

- Los dominios están alojados principalmente en Amazon AWS.
- Resolviendo por dig remitly.com o nslookup da direcciones como:

```
┌──(kali㉿kali)-[~]
└─$ dig remitly.com

; <<>> DiG 9.20.0-Debian <<>> remitly.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42720
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;remitly.com.                   IN      A

;; ANSWER SECTION:
remitly.com.            60      IN      A       13.57.100.64
remitly.com.            60      IN      A       52.9.155.254

;; Query time: 12 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sat May 24 17:28:01 EDT 2025
;; MSG SIZE  rcvd: 72
```

Estas IPs pueden variar por el uso de CDNs y balanceadores de carga.

4. ASN (Autonomous System Numbers).

Usando servicios como bgp.he.net, identificamos que Remitly utiliza:

- AS16509 → Amazon.com, Inc.
- AS13335 → Cloudflare, Inc.

Posiblemente otras ASN a través de proveedores SaaS (Zendesk, Akamai, etc.)

52.9.155.254 > 52.9.0.0/16 > AS16509 > Amazon.com, Inc.
52.9.155.254 > 52.0.0.0/11 > AS16509 > Amazon.com, Inc.
13.57.100.64 > 13.57.0.0/16 > AS16509 > Amazon.com, Inc.
13.57.100.64 > 13.56.0.0/14 > AS16509 > Amazon.com, Inc.

5. ARCHIVOS PÚBLICOS ACCESIBLES.

Archivo	Ubicación	Información relevante
robots.txt	https://www.remitly.com/robots.txt	Listado de rutas públicas o privadas
security.txt	https://www.remitly.com/.well-known/security.txt	Política de divulgación responsable

Archivo	Ubicación	Información relevante
sitemap.xml	https://www.remitly.com/sitemap.xml	Estructura de URLs públicas

6. CERTIFICADOS DIGITALES.

A través de https://crt.sh se detectan múltiples certificados para:

- *.remitly.com
- remitly.com
- Emitidos por: DigiCert, Let’s Encrypt, GlobalSign

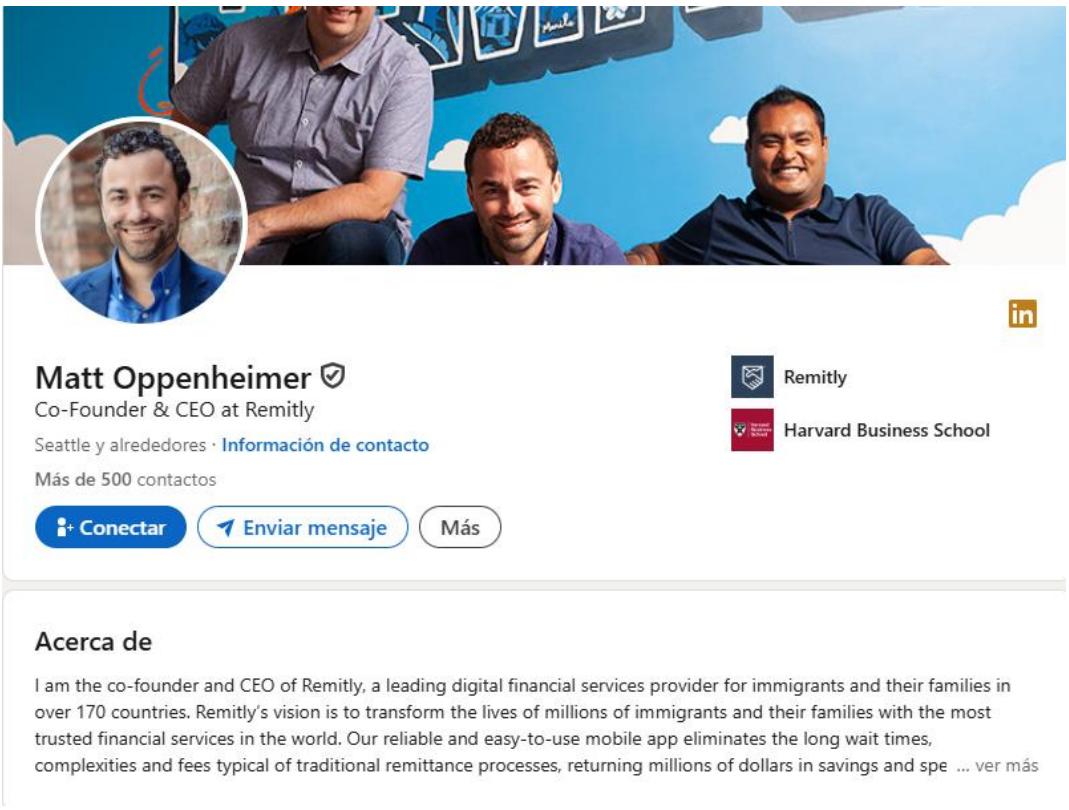
7. INFRAESTRUCTURA EN LA NUBE Y CDN DETECTADAS.

Elemento	Tecnología
Hosting principal	Amazon AWS (EC2, CloudFront, S3)
DNS	Amazon Route 53
CDN / WAF	Akamai, CloudFront
Seguridad y KYC	Sumsub, Jumio (posibles integraciones)

8. ANÁLISIS DE REDES SOCIALES.

Se ha hecho un análisis de redes sociales, utilizando la plataforma LinkedIn, ya que a través de esta podemos tener acceso a personal importante de la empresa, a continuación unos ejemplos:

CEO & Co-Founder de la empresa:



Director de Seguridad: