KeepCoding Bootcamp Ciberseguridad | Edición IX

Módulo Recopilación de Información

Informe de proyecto de auditoria

CONFIDENCIAL

Auditor: Oscar Uriel Tobar Rios
Fecha del Informe: 05/03/2025

Contenido

Declaración de confidencialidad

Este documento es propiedad exclusiva de KeepCoding Y Oscar Tobar. Este documento contiene información confidencial y de propiedad exclusiva. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento de KeepCoding y Oscar Tobar.

KeepCoding puede compartir este documento con auditores bajo acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de prueba de penetración.

Descargo de responsabilidad

Una prueba de penetración se considera una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación y no los cambios o modificaciones realizados fuera de ese período.

Los compromisos con límite de tiempo no permiten una evaluación completa de todos los controles de seguridad. KeepCoding priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. KeepCoding recomienda realizar evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

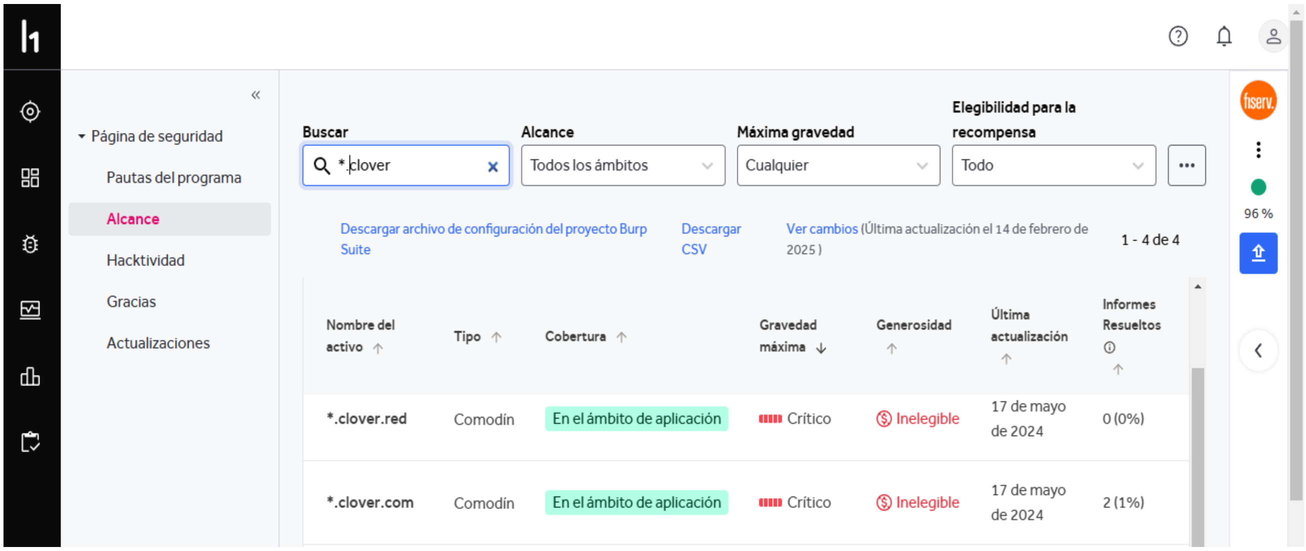
Información de Contacto

Nombre	Cargo	Correo
KeepCoding		
Martín Martín	Global Information Security Manager	Email: hi@mmartin.me
Oscar Tobar		
Oscar Uriel Tobar Rios	Lead Penetration Tester	Email: oscartobar@gmail.com

1 Ámbito y Alcance de la Auditoría

- **Objetivo:** El objetivo de esta auditoria realizar un reconocimiento completo del dominio de una organización y extraer toda la información sensible en el marco de la práctica la materia Recopilación de información del BootCamp de Ciberseguridad IX de Keepcoding

- **Alcance:** La auditoría se realiza sobre el dominio *.clover.com el cual esta en el sitio HackerOne.com dentro de la lista de tipo de programa VDP de Fiserv a quien pertenece este dominio



Buscar: *clover

Alcance: Todos los ámbitos

Máxima gravedad: Cualquier

Elegibilidad para la recompensa: Todo

Descargar archivo de configuración del proyecto Burp Suite · Descargar CSV · Ver cambios (Última actualización el 14 de febrero de 2025) · 1 - 4 de 4

Nombre del activo	Tipo	Cobertura	Gravedad máxima	Generosidad	Última actualización	Informes Resueltos
*.clover.red	Comodín	En el ámbito de aplicación	Crítico	Inelegible	17 de mayo de 2024	0 (0%)
*.clover.com	Comodín	En el ámbito de aplicación	Crítico	Inelegible	17 de mayo de 2024	2 (1%)

Fiserv lleva a cabo sus propias actividades de escaneo e identificación de vulnerabilidades internas. Para minimizar la confusión entre su tráfico y las amenazas legítimas, se utilizó el siguiente encabezado para las solicitudes para que identifiquen mi tráfico según se planean las politicas en HackOne

- X-HackerOne-Research: newsir20k

Las fases de las actividades de pruebas de penetración incluyen las siguientes:

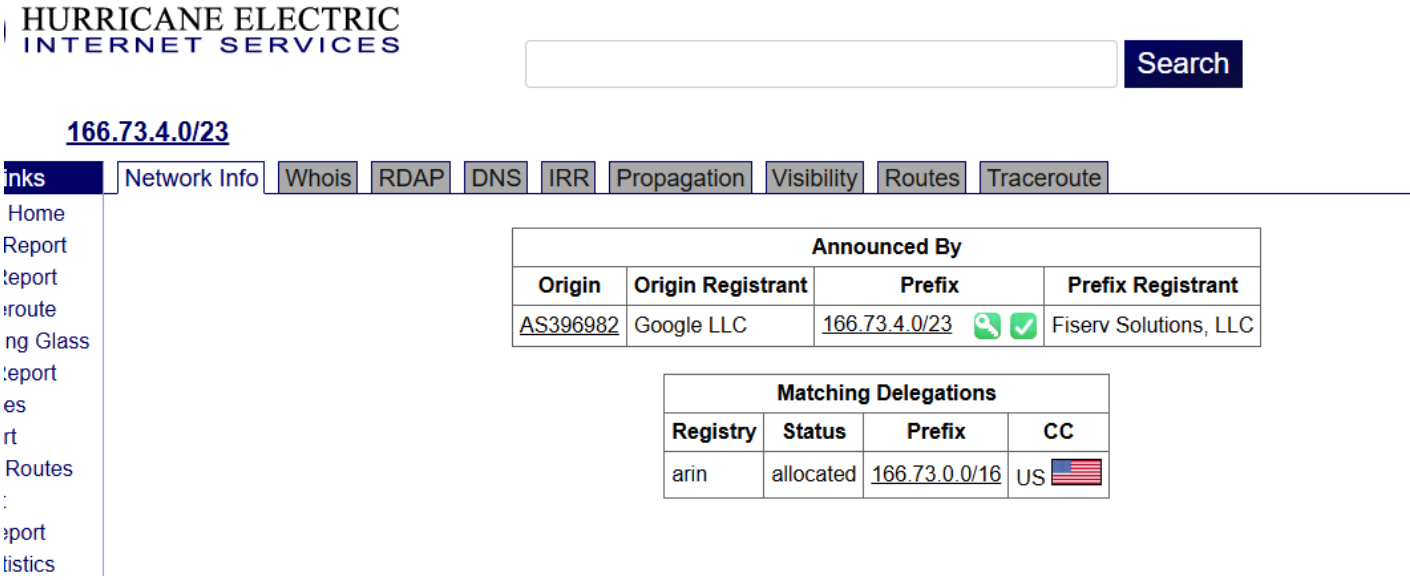
• Planificación: De acuerdo al Caso práctico entregado se debe desarrollar la practica https://github.com/KeepCodingCiber9/recopilacion-de-informacion/blob/main/CasoPractico.pdf

• Descubrimiento: Se realizarón escaneos y enumeraciones para identificar posibles vulnerabilidades, áreas débiles y exploits.

2 Técnicas de Footprinting

2.1 Footprinting Horizontal

2.1.1 Network Info



Announced By			
Origin	Origin Registrant	Prefix	Prefix Registrant
AS396982	Google LLC	166.73.4.0/23	Fiserv Solutions, LLC

Matching Delegations			
Registry	Status	Prefix	CC
arin	allocated	166.73.0.0/16	US

2.1.2 Whois

```
Domain Name: CLOVER.COM
   Registry Domain ID: 5097243_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2023-05-25T05:16:10Z
   Creation Date: 1991-08-27T04:00:00Z
   Registry Expiry Date: 2025-08-26T04:00:00Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: domain.operations@web.com
   Registrar Abuse Contact Phone: +1.8777228662
   Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
   Name Server: DNS1.P07.NSONE.NET
   Name Server: DNS2.P07.NSONE.NET
   Name Server: NS1.P201.DNS.ORACLECLOUD.NET
   Name Server: NS2.P201.DNS.ORACLECLOUD.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form:
https://www.icann.org/wicf/
```

2.2 Footprinting vertical

2.2.1 DNS Brute-force -> shuffledns

Primero traemos una lista de servidores DNS

```
wget -O /tmp/resolvers.txt https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt
```

Luego los validamos

```
resolvalid -u resolvers.txt -o $HOME/recopilacion/lists/resolvers2.txt -to 5s
```

o

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

Ver en

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/resolvers.txt

luego generar una lista aleatoria de dominios

```
shuffledns -mode bruteforce -d clover.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > shuffledns.txt
```

Ver en

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/shuffledns.txt

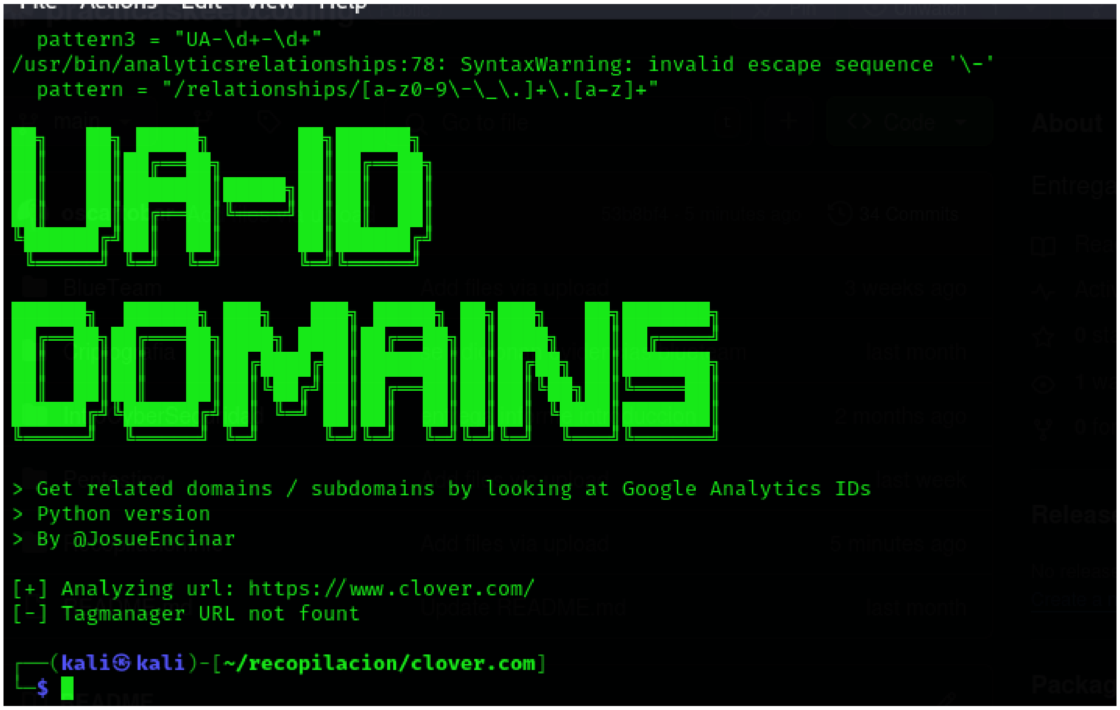
2.2.1.1 Análisis

Utilizando la técnica de generación de dns aleatoros basados en la información existente, de pudieron generar 42 posible dominios

2.2.2 Google analytics -> analyticsrelationships

Para buscar información del dominio en Google analitics se uso analyticsrelationships asi:

```
analyticsrelationships --url https://www.clover.com/
```



```
  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.clover.com/
[-] Tagmanager URL not fount

┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ 
```

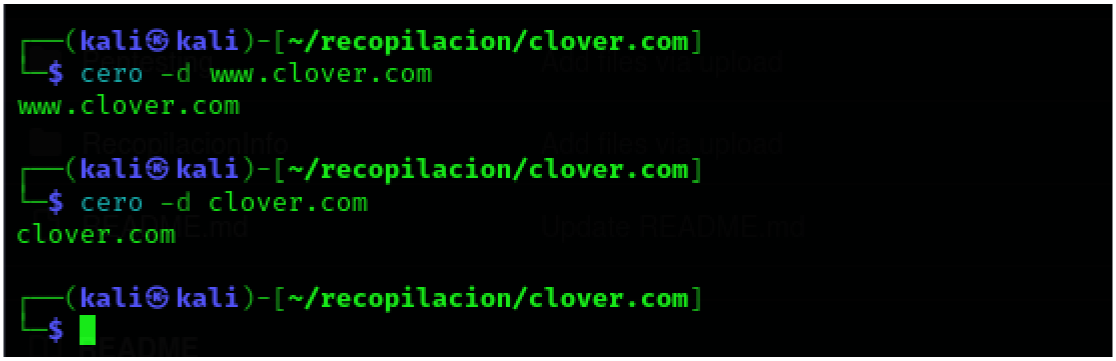
2.2.2.1 *Análisis*

Con esta herramienta no se encontró información relevante del dominio Clover.com

2.2.3 TLS probing -> cero

Se utilizo la herramienta ceo para Conseguir información a través de los certificados SSL/TSL

cero -d clover.com



```
┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ cero -d www.clover.com
www.clover.com

┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ cero -d clover.com
clover.com

┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ 
```

2.2.3.1 *Análisis*

Con esta herramienta no se encontró información relevante del dominio Clover.com

2.2.4 Web scraping -> katana

Luego se utilizo la herramienta Katana para navegar el sitio

```
echo clover.com | katana scan  -H "X-HackerOne-Research: newsir20k"
```

```
echo clover.com | katana -silent -jc -o katanaoutput.txt -kf robotstxt,sitemapxml "X-HackerOne-Research: newsir20k"
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/katanaoutput.txt

2.2.4.1 Análisis

Con esta herramienta solo se encontró información de https://connect.clover.com y https://clover.com, pero no brindo suficiente información

2.2.5 Certificate Transparency Logs -> ctfr

La herramienta ctfr permite consultar en los Certificate Transparency Logs asi:

```
ctfr -d clover.com > ctfr.txt
```

El resultado se comparte aqui

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/ctfr.txt

2.2.5.1 Análisis

Con esta herramienta se encontró valiosa información (967 certificados relacionados) entre los dominios a destacar se encuentran estos

perf.catalyst.clover.com

admin.clover.com

api-accounts.prod.catalyst.clover.com

api-auth.prod.catalyst.clover.com

api.catalyst.clover.com

api-dr.catalyst.clover.com

api.prod.catalyst.clover.com

2.2.6 Archivos web/cache -> gau

Usando la herramienta **gau** se busco en el cache del del sitio encontrando 45404 url de cache

```
gau https://www.clover.com/v3/merchants/ --from 202406 --o gaumer.txt
```

```
gau --threads 5 clover.com --o gauoutput.txt
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/gau202405.txt

2.2.6.1 Análisis

Con esta herramienta se encontró valiosa información entre los dominios a destacar se encuentran estos que aunque deberían estar protegidos con autorizacion como los directorios padres, estos directorios no tienen seguridad.

https://www.clover.com/v3/shop/resellers/BVG1JKB6RM0DM/chain_agent_id

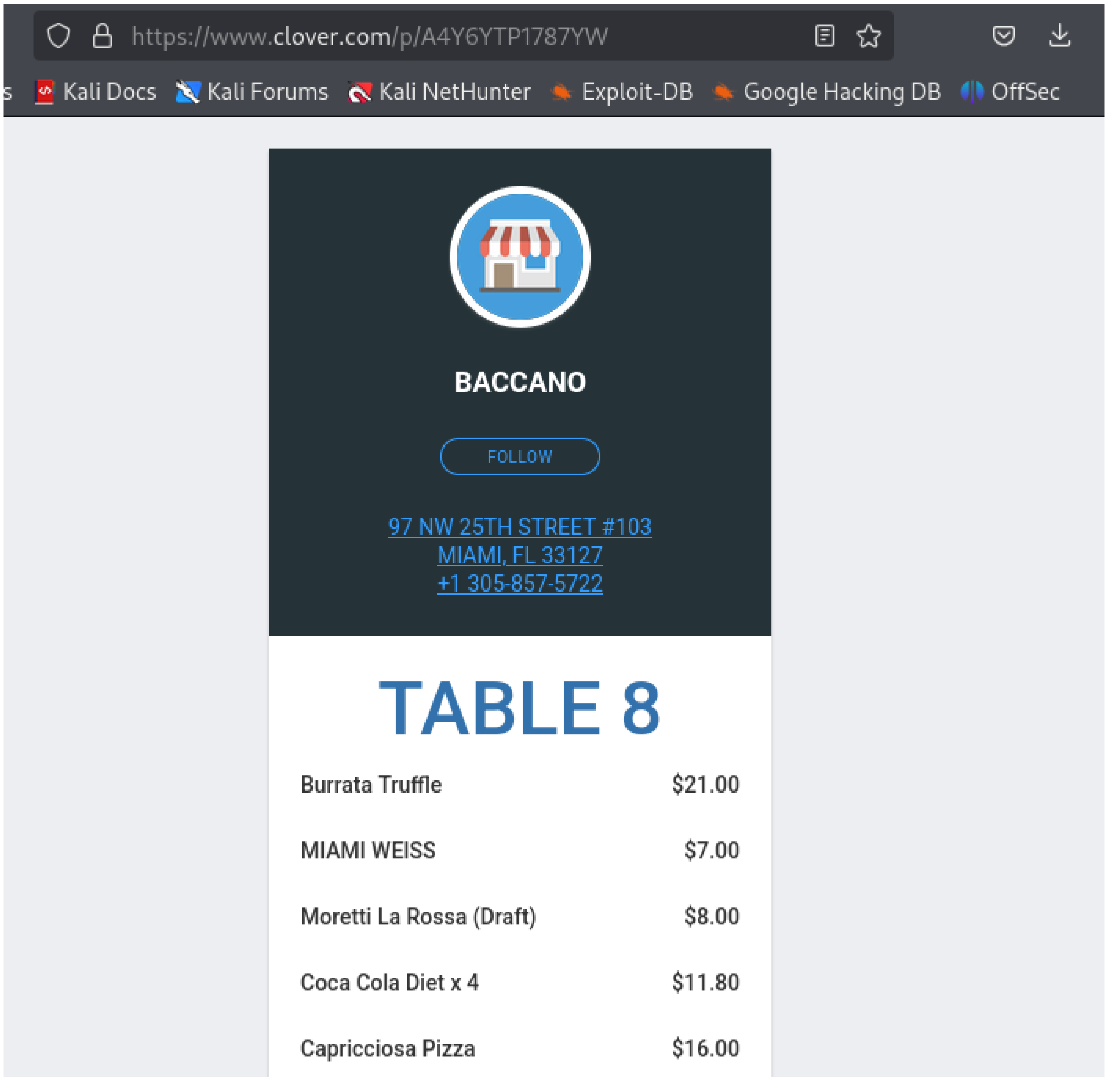
https://www.clover.com/v3/shop/resellers/BVG1JKB6RM0DM/promos/khL4pD

https://www.clover.com/v3/merchants/WG9YG9J7M9ZC1/ecomm_payment_configs

Un descubrimiento importante es que se estableció que se pueden consultar ordenes de pedido de cualquiera de los clientes sin necesidad de usuario ni clave

Por ejemplo, al ingresar a

https://www.clover.com/p/A4Y6YTP1787YW

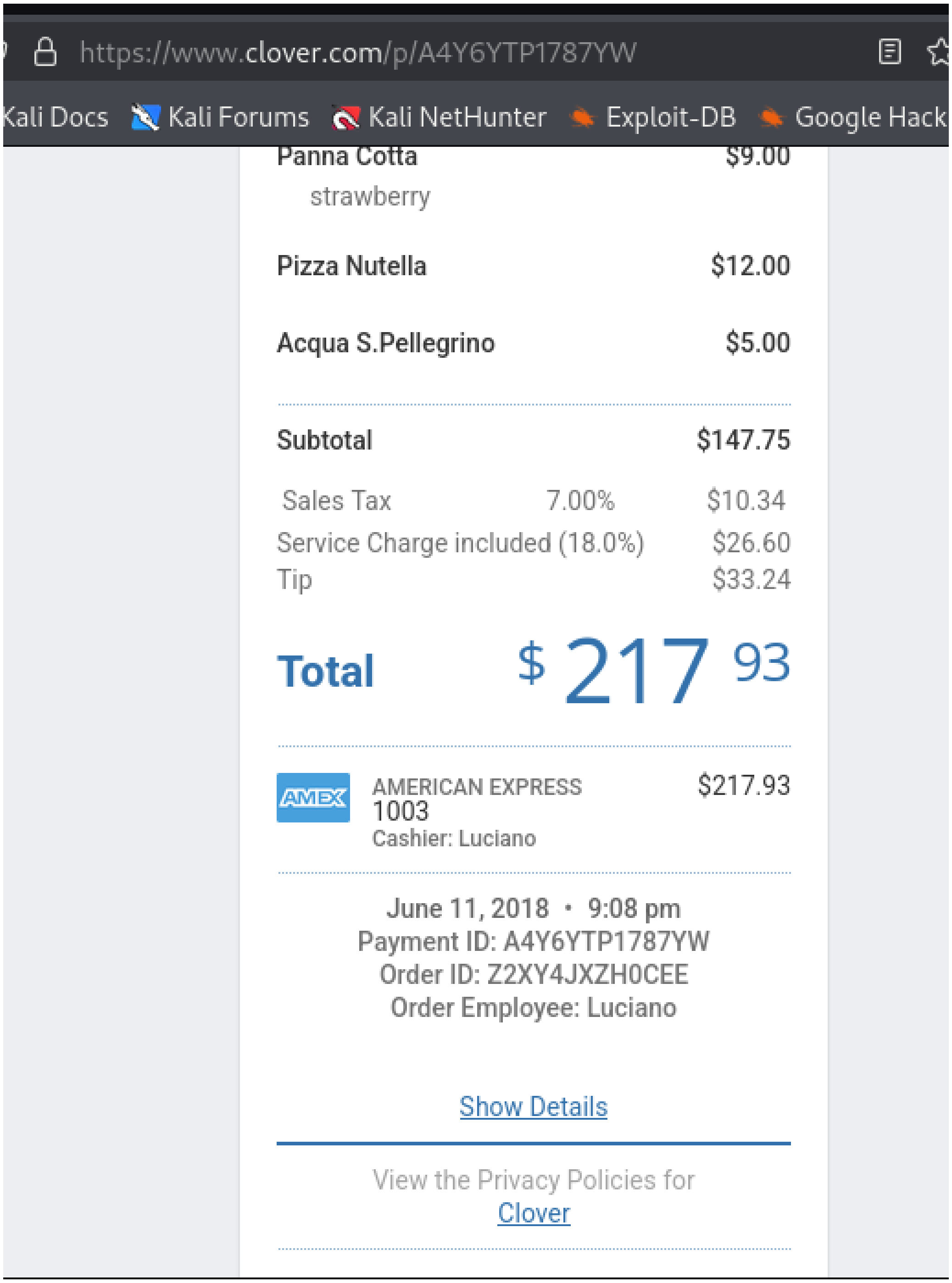


BACCANO

97 NW 25TH STREET #103
MIAMI, FL 33127
+1 305-857-5722

TABLE 8

Burrata Truffle	$21.00
MIAMI WEISS	$7.00
Moretti La Rossa (Draft)	$8.00
Coca Cola Diet x 4	$11.80
Capricciosa Pizza	$16.00



https://www.clover.com/p/A4Y6YTP1787YW

Panna Cotta strawberry		$9.00
Pizza Nutella		$12.00
Acqua S.Pellegrino		$5.00
Subtotal		$147.75
Sales Tax	7.00%	$10.34
Service Charge included (18.0%)		$26.60
Tip		$33.24
Total		$ 217 93
AMEX AMERICAN EXPRESS 1003 Cashier: Luciano		$217.93

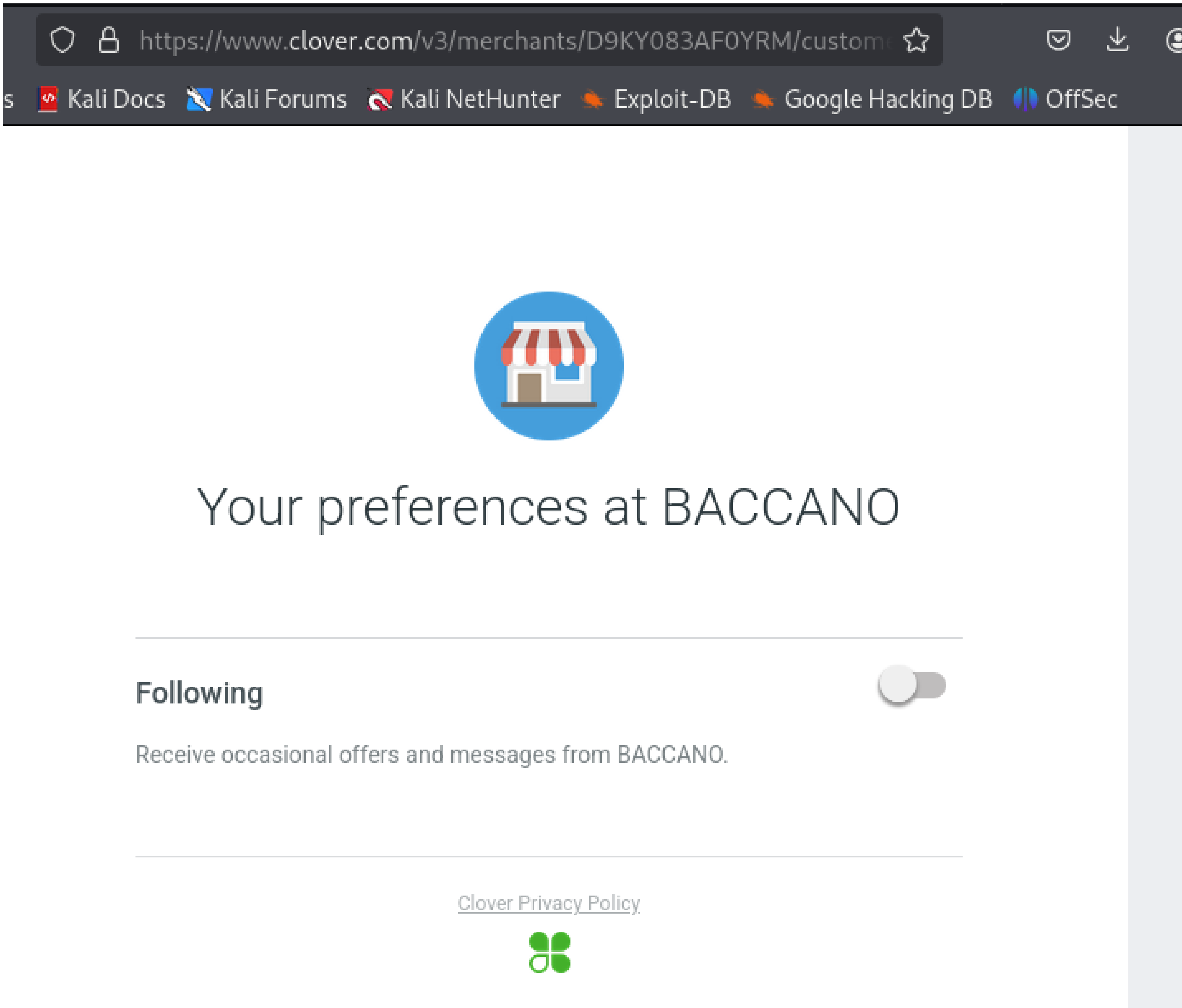
June 11, 2018 • 9:08 pm
Payment ID: A4Y6YTP1787YW
Order ID: Z2XY4JXZH0CEE
Order Employee: Luciano

Show Details

View the Privacy Policies for
Clover

Además de ver toda la información de la transacción. Permite hacer click en el botón Follow y permite ingresar a las preferencias del cliente para que se modifique el envio de mensajes de ofiertas o mensajes.

https://www.clover.com/v3/merchants/D9KY083AF0YRM/customers/7723X1CB8GBGC/profile



https://www.clover.com/v3/merchants/D9KY083AF0YRM/custom

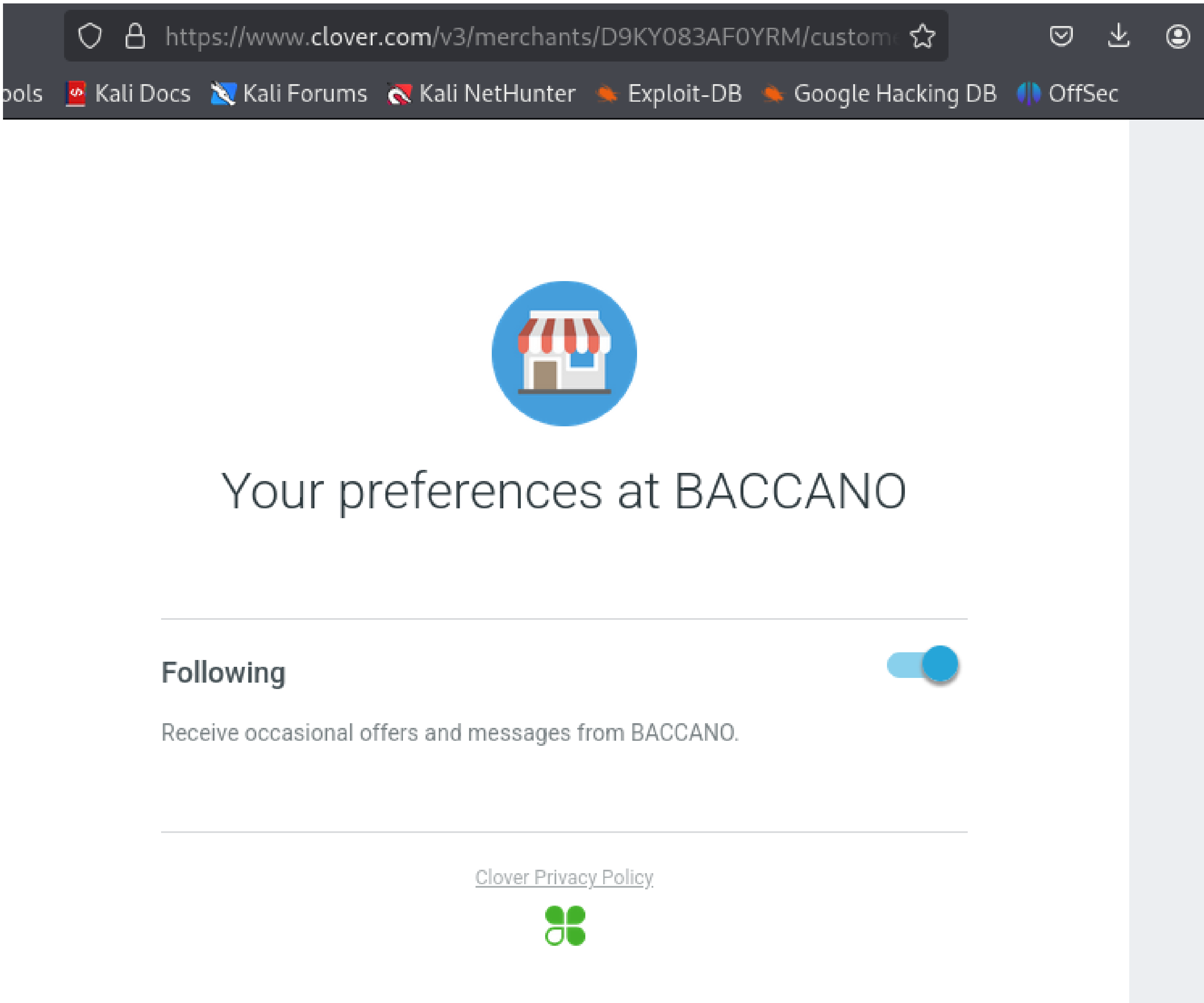
Your preferences at BACCANO

Following

Receive occasional offers and messages from BACCANO.

Clover Privacy Policy

Obviamente un una persona ajena no debería poder modificar esta información



https://www.clover.com/v3/merchants/D9KY083AF0YRM/custom

Your preferences at BACCANO

Following

Receive occasional offers and messages from BACCANO.

Clover Privacy Policy

Este incidente fue reportado a hackerone.com/

https://hackerone.com/bugs?subject=user&report_id=3000389

Con el siguiente reporte

Shipping Requirements

Vulnerability Summary

A user without having to authenticate in the system, can view an invoice, and additionally, can enter this URL and modify the customer's message sending preferences in their profile.

The target where the vulnerability was found

https://www.clover.com/v3/merchants/{mId}/customers/{idCustomer}/profile

Detailed steps to reproduce it, or steps you followed when it was reproducible

go to

https://www.clover.com/p/{PaymentID}

click on the Following button

Click on the Following slider button

And the customer's profile has already been modified to receive offers or messages without needing any credentials

Tools and methods used to identify and exploit the vulnerability

gau https://www.clover.com/v3/merchants/ --from 202406

webbrowser

Any artifacts used or identified during discovery (screenshots welcome)

Detailed description of impact

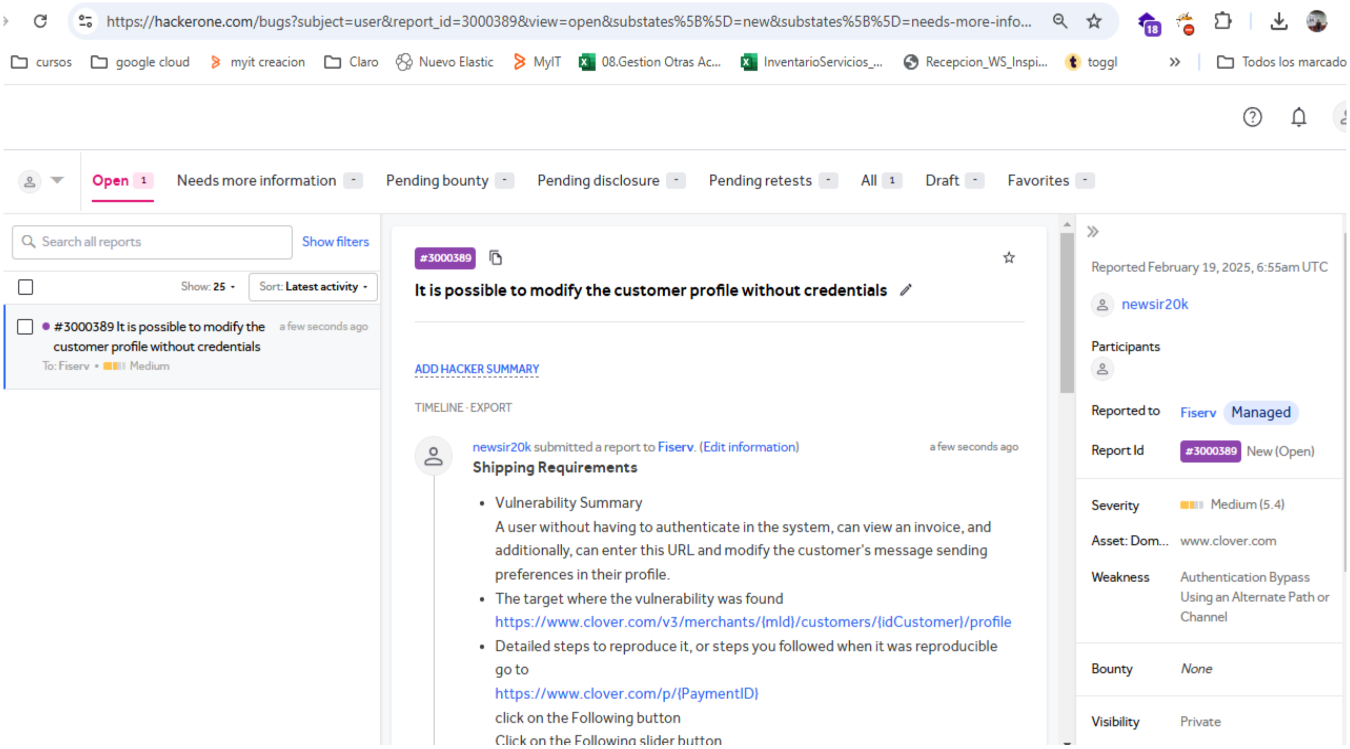
What is the full scope of the impact this represents for Fiserv and its users or customers? loss of credibility of POS products

Was any sensitive data identified or accessible as part of your test? If so, please provide details.

Supporting material/references:

Please list any additional materials (e.g. screenshots, logs, etc.) relevant to your test

Any data downloaded, identified, captured (or proof of deletion/destruction)



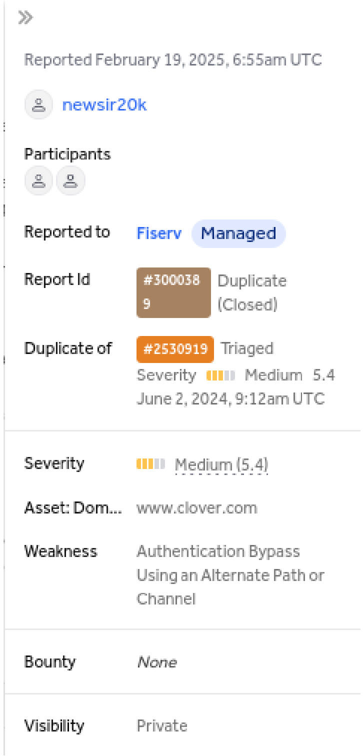
It is possible to modify the customer profile without credentials

newsir20k submitted a report to Fiserv. (Edit information)

Shipping Requirements

- Vulnerability Summary
  A user without having to authenticate in the system, can view an invoice, and additionally, can enter this URL and modify the customer's message sending preferences in their profile.
- The target where the vulnerability was found
  https://www.clover.com/v3/merchants/{mId}/customers/{idCustomer}/profile
- Detailed steps to reproduce it, or steps you followed when it was reproducible
  go to
  https://www.clover.com/p/{PaymentID}
  click on the Following button
  Click on the Following slider button

La respuesta obtenida fue que ya estaba reportado previamente

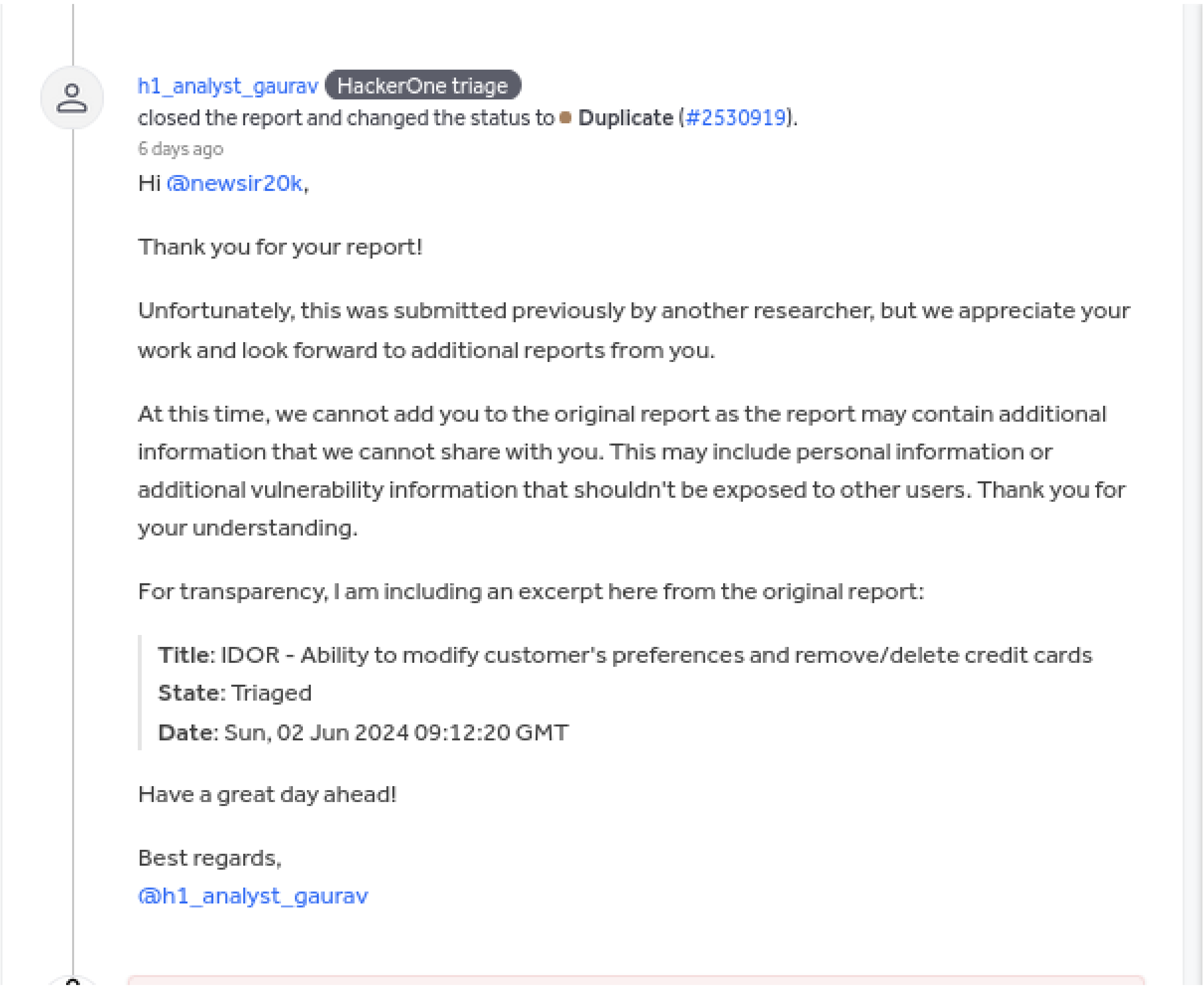


Reported February 19, 2025, 6:55am UTC

newsir20k

Participants

Reported to	Fiserv Managed
Report Id	#3000389 Duplicate (Closed)
Duplicate of	#2530919 Triaged Severity Medium 5.4 June 2, 2024, 9:12am UTC
Severity	Medium (5.4)
Asset: Dom...	www.clover.com
Weakness	Authentication Bypass Using an Alternate Path or Channel
Bounty	*None*
Visibility	Private



h1_analyst_gaurav
closed the report and changed the status to ● **Duplicate** (#2530919).
6 days ago

Hi @newsir20k,

Thank you for your report!

Unfortunately, this was submitted previously by another researcher, but we appreciate your work and look forward to additional reports from you.

At this time, we cannot add you to the original report as the report may contain additional information that we cannot share with you. This may include personal information or additional vulnerability information that shouldn't be exposed to other users. Thank you for your understanding.

For transparency, I am including an excerpt here from the original report:

> **Title**: IDOR - Ability to modify customer's preferences and remove/delete credit cards
> **State**: Triaged
> **Date**: Sun, 02 Jun 2024 09:12:20 GMT

Have a great day ahead!

Best regards,
@h1_analyst_gaurav

2.2.7 Concatenar todos los resultados y ejecutar permutaciones -> alterx + dnsx

cat subdominios.txt | alterx | dnsx > combinadosvalidos.txt

se genera el listado de dominios aleatorios en el archivo combinadosvalidos.txt

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/combinadosvalidos.txt

3 Técnicas de Fingerprinting

3.1 Identificar subdominios online -> httpx

Para dejar únicamente los subdominios validos y que responden al DNS se ejecutaron las herramientas httpx y unfurl asi

```
sort -u combinadosvalidos.txt subdominiosvalidados.txt ctfr_validado.txt > subcombinados1.txt
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/subcombinados1.txt

```
cat subcombinados1.txt|httpx -silent > vivos_subdominios2.txt
```

```
cat vivos_subdominios2.txt|unfurl --unique domains > vivos_subdominios.txt
```

El resultado final fueron dos archivos el archivo vivos_subdominios.txt que contienen los subdominios

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/vivos_subdominios.txt

y el archivo vivos_subdominios2.txt que tiene el protocolo de cada dominio (http o https)

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/vivos_subdominios2.txt

3.2 Escanear puertos y detectar servicios -> masscan / nmap

Convertimos los dominios en ips

```
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
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/subdominiosfinal_ips.txt

3.2.1 NMAP

```
nmap -p80 --script http-headers --script-args 'http.headers={["X-HackerOne-Research"]="newsir20k"}' <objetivo>
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/nmap_Xmas.txt https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/nampUDP.txt

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/nmaprapido.txt

3.2.1.1 Analisis

De especial interés se encontraron puertos abiertos no cifrados en todos los dominios como

80/TCP/ http y 5050/TCP/sip, 8080/tcp open http-proxy

Adicionalmente se destacan los siguientes puertos que aunque aparecen filtrados podrían investigarse mas a fondo

au.clover.com (66.6.29.162) y ert-self-serve-ui.catalyst.clover.com (167.86.43.39)

21/tcp filtered ftp

22/tcp filtered ssh

25/tcp filtered smtp

543/tcp filtered klogin

2000/tcp filtered cisco-sccp

179/tcp filtered bgp

cld-stage-merchants.clover.com (66.22.56.145)

21/tcp filtered ftp

22/tcp filtered ssh

25/tcp filtered smtp

119/tcp filtered nntp

179/tcp filtered bgp

389/tcp filtered ldap

2000/tcp filtered cisco-sccp

2049/tcp filtered nfs

10000/tcp filtered snet-sensor-mgmt

49154/tcp filtered unknown

cld-stage-talent.clover.com (66.22.56.35)

```
1025/tcp filtered NFS-or-IIS

6001/tcp filtered X11:1
```

otp.catalyst.clover.com (66.22.30.155)

```
1/tcp   filtered ftp

22/tcp   filtered ssh

25/tcp   filtered smtp

179/tcp  filtered bgp

427/tcp  filtered svrloc

445/tcp  filtered microsoft-ds

1110/tcp filtered nfsd-status

1433/tcp filtered ms-sql-s

8888/tcp filtered sun-answerbook
```

3.2.2 MASSCAN

```
sudo masscan --ports 0-65500 -iL subdominiosfinal_ips.txt > masscanTodos.txt
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/masscanTodos.txt

Analisis

Después de ejecutar masscan, se destaca que se encontraron **Puertos de interfaces de administración típicas como los puertos 2082, 2083, 2086, 2087, 2095, 2096.** Estos puertos suelen estar asociados a paneles de control como cPanel/WHM. Si estos servicios se exponen sin las debidas medidas de seguridad (por ejemplo, contraseñas fuertes, actualizaciones constantes, restricciones de IP) pueden ser un vector de ataque significativo. Los servidores que tienen estos puertos abiertos con los siguientes:

```
104.17.71.206
104.16.241.118
104.16.96.80
104.17.73.206
199.60.103.225
104.17.72.206
104.16.242.118
104.16.94.80
104.17.74.206
```

104.17.70.206
104.16.93.80
199.60.103.31
104.16.92.80
104.16.95.80

3.3 Identificar tecnologias web -> gowitness / Wappalyzer / whatweb

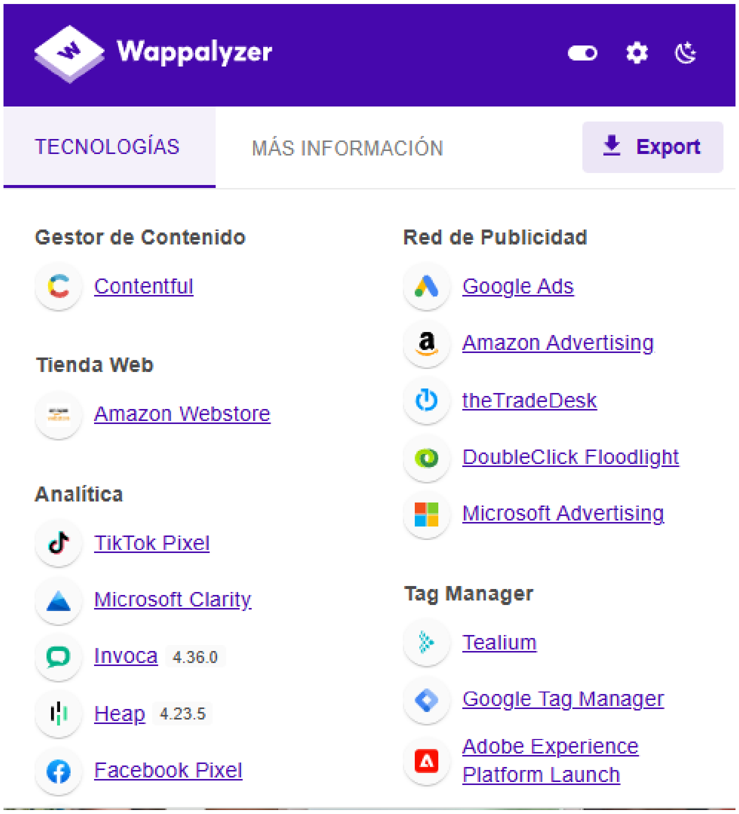
3.3.1 Gowitness

gowitness file -f subdominios.txt

https://github.com/oscartobar/practicaskeepcoding/tree/main/RecopilacionInfo

3.3.2 Wappalyzer

Se encuentra que el sitio esta desarrollado en REACT y como framework de UI tiene BootStrap, como CDN usa CloudFlake



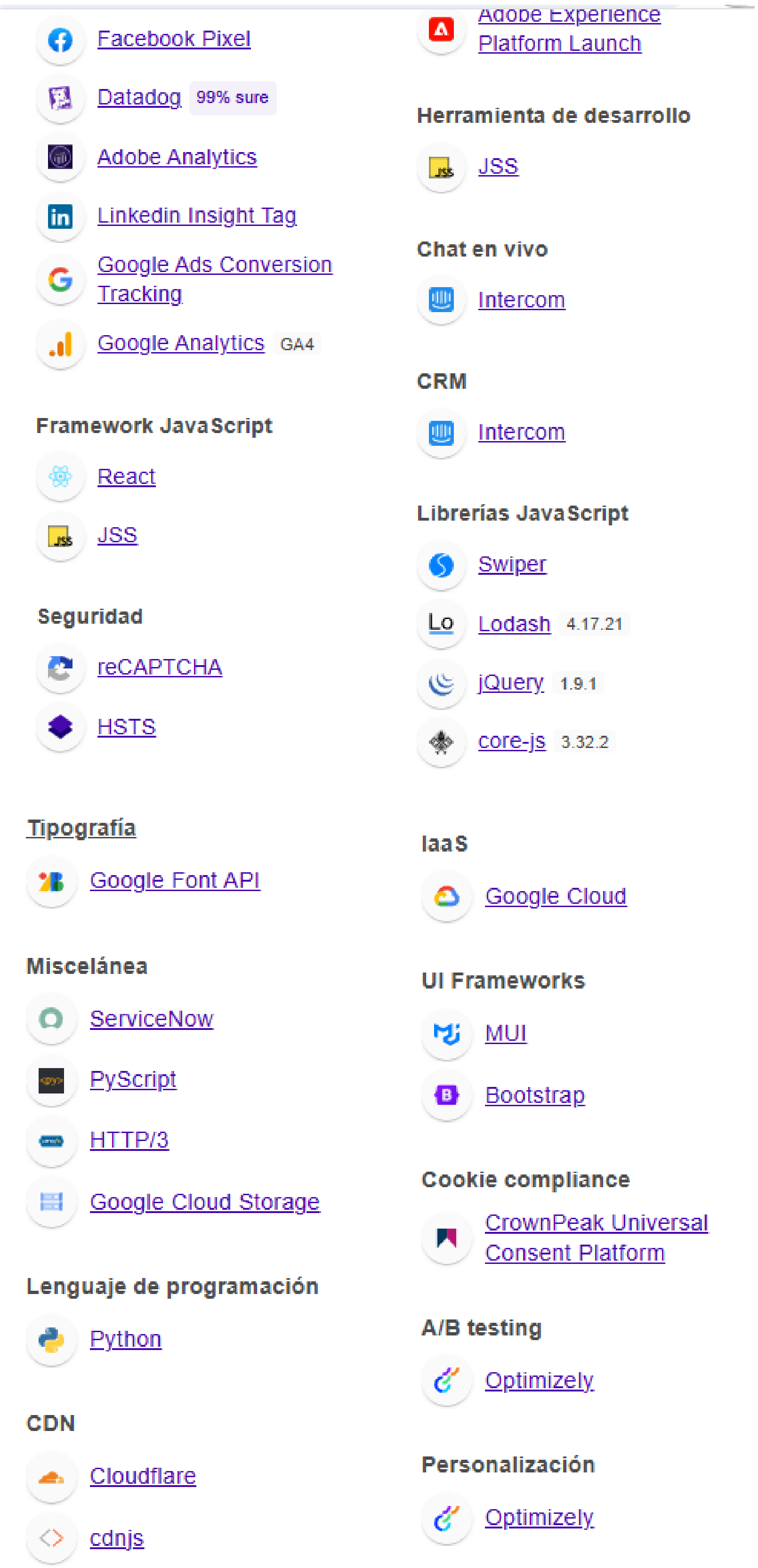
Gestor de Contenido
- Contentful

Tienda Web
- Amazon Webstore

Analítica
- TikTok Pixel
- Microsoft Clarity
- Invoca 4.36.0
- Heap 4.23.5
- Facebook Pixel

Red de Publicidad
- Google Ads
- Amazon Advertising
- theTradeDesk
- DoubleClick Floodlight
- Microsoft Advertising

Tag Manager
- Tealium
- Google Tag Manager
- Adobe Experience Platform Launch



- Facebook Pixel
- Datadog 99% sure
- Adobe Analytics
- Linkedin Insight Tag
- Google Ads Conversion Tracking
- Google Analytics GA4

Framework JavaScript

- React
- JSS

Seguridad

- reCAPTCHA
- HSTS

Tipografía

- Google Font API

Miscelánea

- ServiceNow
- PyScript
- HTTP/3
- Google Cloud Storage

Lenguaje de programación

- Python

CDN

- Cloudflare
- cdnjs

- Adobe Experience Platform Launch

Herramienta de desarrollo

- JSS

Chat en vivo

- Intercom

CRM

- Intercom

Librerías JavaScript

- Swiper
- Lodash 4.17.21
- jQuery 1.9.1
- core-js 3.32.2

IaaS

- Google Cloud

UI Frameworks

- MUI
- Bootstrap

Cookie compliance

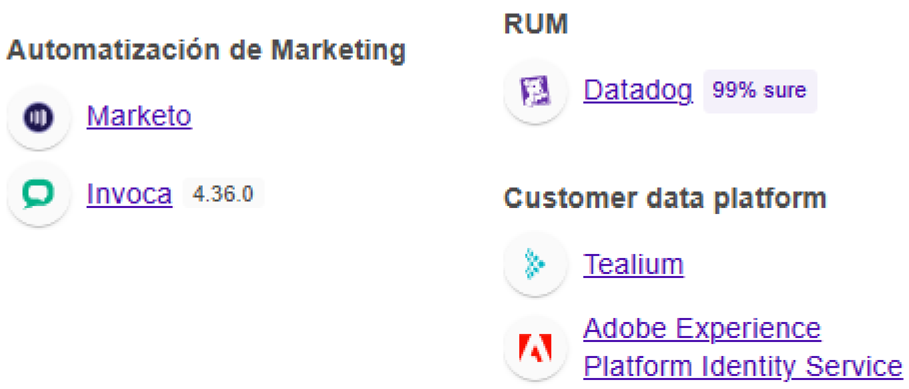
- CrownPeak Universal Consent Platform

A/B testing

- Optimizely

Personalización

- Optimizely



Automatización de Marketing

Marketo

Invoca 4.36.0

RUM

Datadog 99% sure

Customer data platform

Tealium

Adobe Experience Platform Identity Service

3.3.3 Whatweb

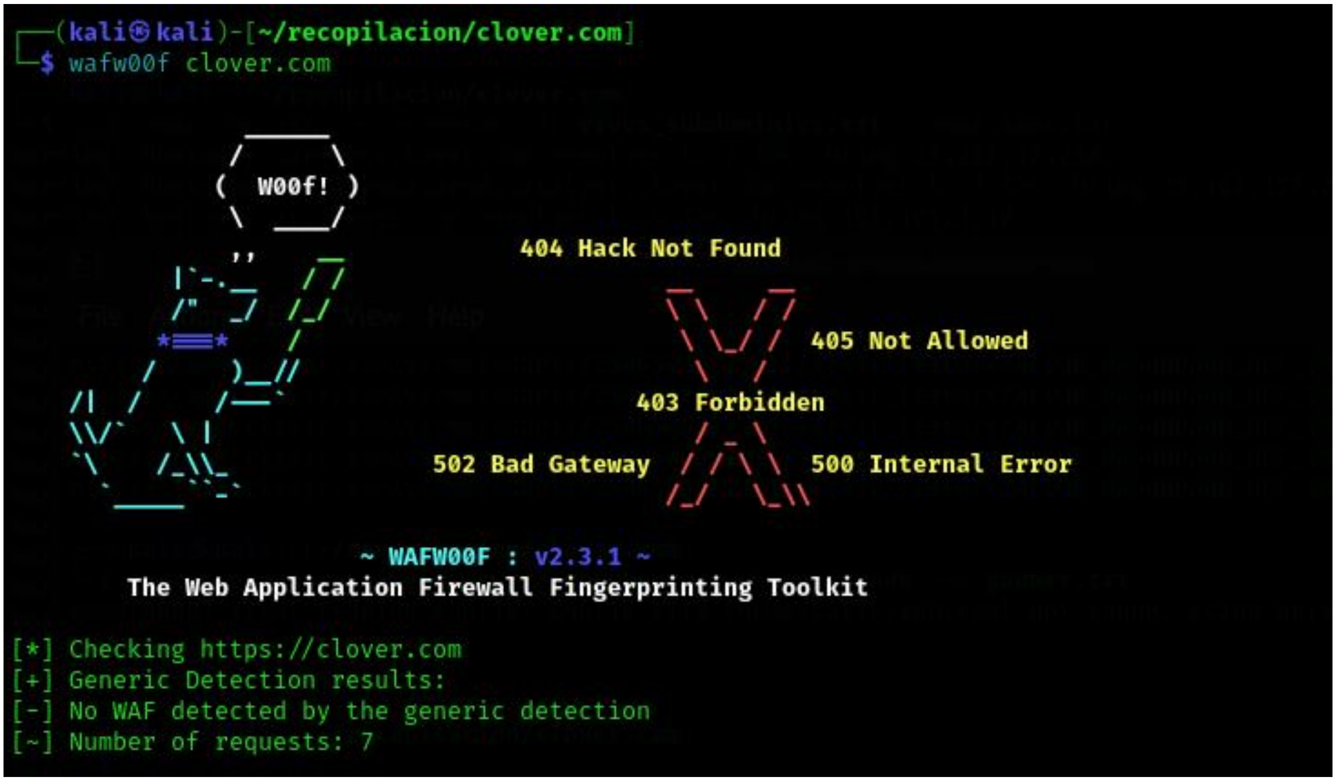
whatweb -i vivos_subdominios.txt > whatweb.txt

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/whatweb.txt

Como dato relevante algunos dominios tienen redideccion permante como http 301 y la mayoria responde 302 usando CloudFlake y los sitios que retornan http 200 al parececer no tienen WAF

3.4 Identificar posibles WAF -> wafw00f

No se encontró un WAF para el dominio clover.com



```
┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ wafw00f clover.com

                   ______
                  /      \
                 (  W00f! )
                  \  ____/
                  ,,    __            404 Hack Not Found
              |`-.__   / /                      __     __
              /"  _/  /_/                       \ \   / /
             *===*    /                          \ \_/ /  405 Not Allowed
            /     )__//                           \   /
       /|  /     /---`                        403 Forbidden
       \\/`   \ |                                 / \
       `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
         `_____``-`                             /_/   \_\

                        ~ WAFW00F : v2.3.1 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://clover.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

3.5 Descubrimiento de contenido / fuzzing -> ffuf

ffuf -t 20 -mc 200,400,401,403 -fs 42 -c -v -u https://clover.com/FUZZ -w /usr/share/wordlists/dirb/big.txt > fuuf.txt

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/fuuf.txt

En el descubrimiento del sitio clover.com se encontraron los siguientes sitios los cuales pueden ser analizados con otras herramientas para verificar sus vulnerabilidades

https://clover.com/login

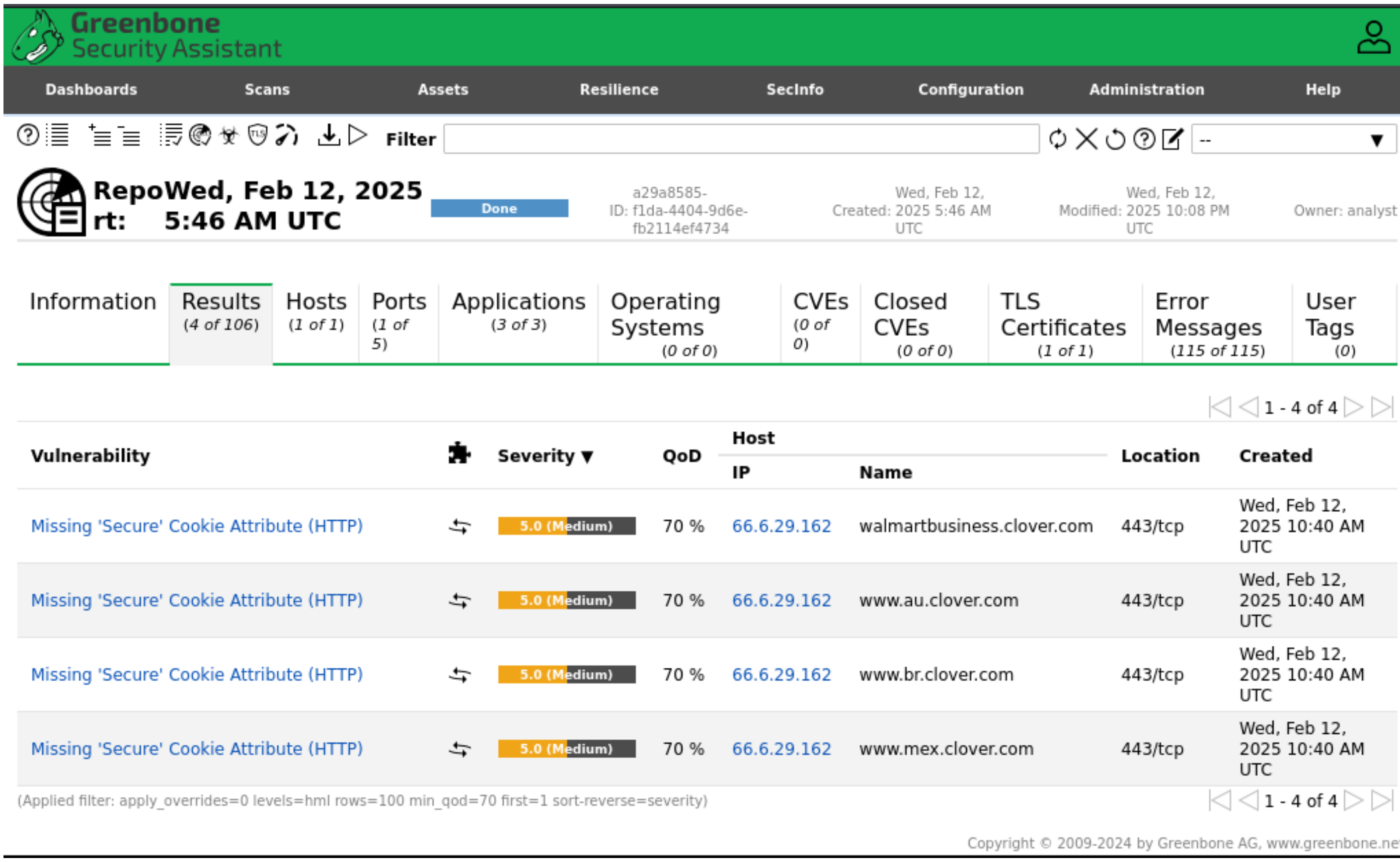
https://clover.com/reporting

https://clover.com/transactions

4 Análisis de vulnerabilidades

4.1 Análisis estandar -> Greenbone y Nuclei

4.1.1 Greenbone



RepoWed, Feb 12, 2025
rt: 5:46 AM UTC

Done

ID: a29a8585-f1da-4404-9d6e-fb2114ef4734

Created: Wed, Feb 12, 2025 5:46 AM UTC

Modified: Wed, Feb 12, 2025 10:08 PM UTC

Owner: analyst

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Missing 'Secure' Cookie Attribute (HTTP)	⇆	5.0 (Medium)	70 %	66.6.29.162	walmartbusiness.clover.com	443/tcp	Wed, Feb 12, 2025 10:40 AM UTC
Missing 'Secure' Cookie Attribute (HTTP)	⇆	5.0 (Medium)	70 %	66.6.29.162	www.au.clover.com	443/tcp	Wed, Feb 12, 2025 10:40 AM UTC
Missing 'Secure' Cookie Attribute (HTTP)	⇆	5.0 (Medium)	70 %	66.6.29.162	www.br.clover.com	443/tcp	Wed, Feb 12, 2025 10:40 AM UTC
Missing 'Secure' Cookie Attribute (HTTP)	⇆	5.0 (Medium)	70 %	66.6.29.162	www.mex.clover.com	443/tcp	Wed, Feb 12, 2025 10:40 AM UTC

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

Copyright © 2009-2024 by Greenbone AG, www.greenbone.ne

4.1.1.1 HALLAZGO

Se encontró que existe una falla en los dominios,

www.au.clover.com

www.br.clover.com

www.mex.clover.com

walmartbusiness.clover.com

Por que existe una cookie que no utiliza el atributo "Secure" y se envía a través de una conexión SSL/TLS.

Esto permite que el cliente pase una cookie al servidor a través de canales no seguros (HTTP) y, posteriormente, permite que un atacante realice, por ejemplo, ataques de secuestro de sesión.

Evidencia

The cookie(s):

Set-Cookie: __uzma=6fe244ca-7bec-4203-8a0d-07c7c205030b; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28 GMT ; Max-Age=***replaced***; SameSite=Lax

Set-Cookie: __uzmb=1739339908; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28 GMT ; Max-Age=***replaced***; SameSite=Lax

Set-Cookie: __uzme=5055; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28 GMT ; Max-Age=***replaced***; SameSite=Lax

Set-Cookie: __uzmc=992541095754; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28 GMT ; Max-Age=***replaced***; SameSite=Lax

Set-Cookie: __uzmd=1739339908; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28 GMT ; Max-Age=***replaced***; SameSite=Lax

is/are missing the "Secure" cookie attribute.

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/report-greenbone.pdf

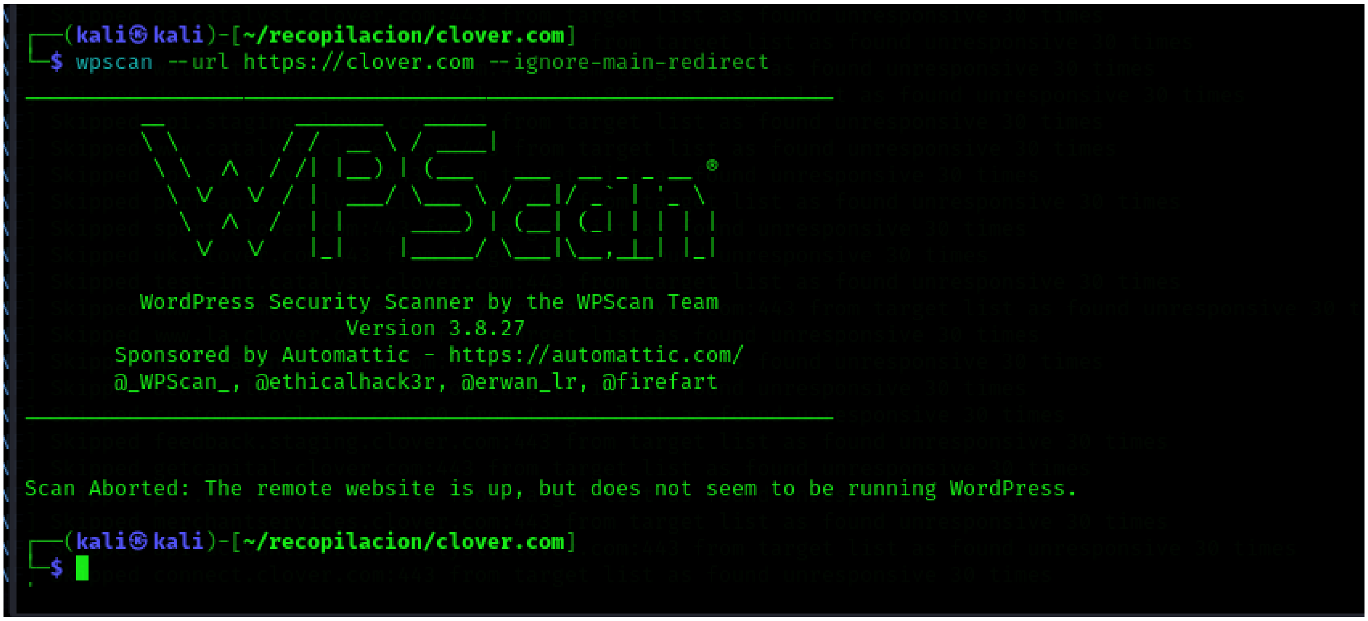
4.1.2 Nuclei

Se ejecuto la herramienta pero únicamente arrojo informacion informativa (INFO) del dominio principal.

```
nuclei -u clover.com > nuclei.txt
```

https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/nuclei.txt

4.2 Análisis web -> wpscan

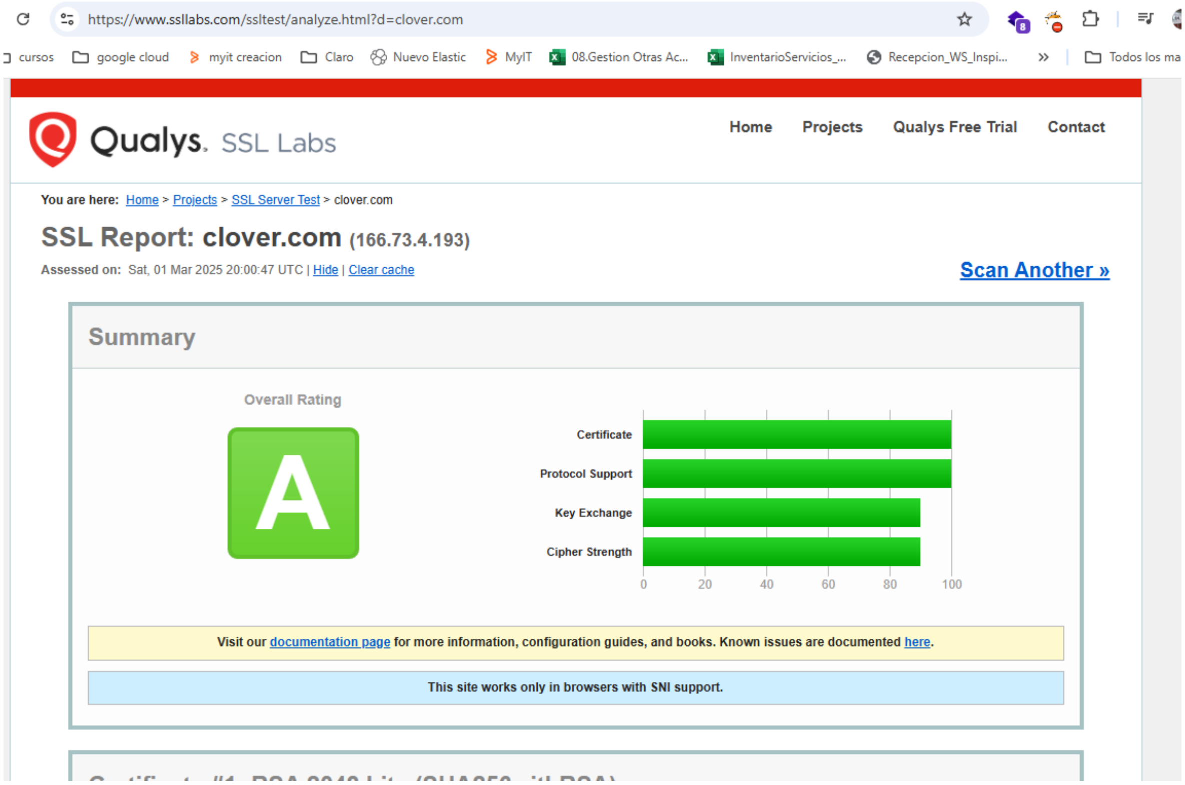


```
┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ wpscan --url https://clover.com --ignore-main-redirect
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

┌──(kali㉿kali)-[~/recopilacion/clover.com]
└─$ 
```

El sitio clover.co no usa WordPress

4.3 Análisis SSL/TLS

Los certificados del sitio tienen una calificación A



https://www.ssllabs.com/ssltest/analyze.html?d=clover.com

You are here: Home > Projects > SSL Server Test > clover.com

SSL Report: clover.com (166.73.4.193)

Assessed on: Sat, 01 Mar 2025 20:00:47 UTC | Hide | Clear cache

Scan Another »

Summary

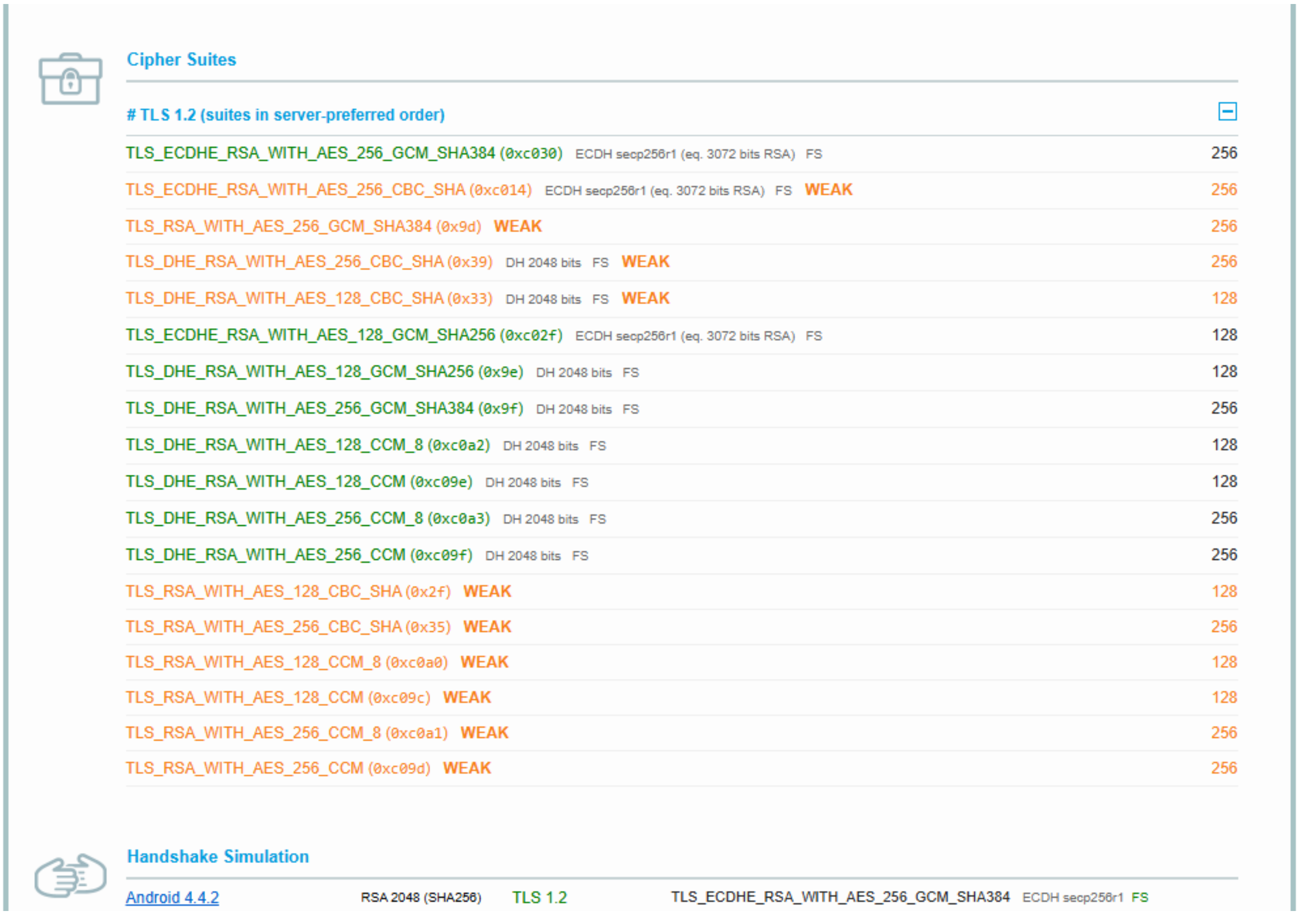
Overall Rating

A

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

Algunos de las suites de cifrado son de cifrado débil



Cipher Suites

TLS 1.2 (suites in server-preferred order)

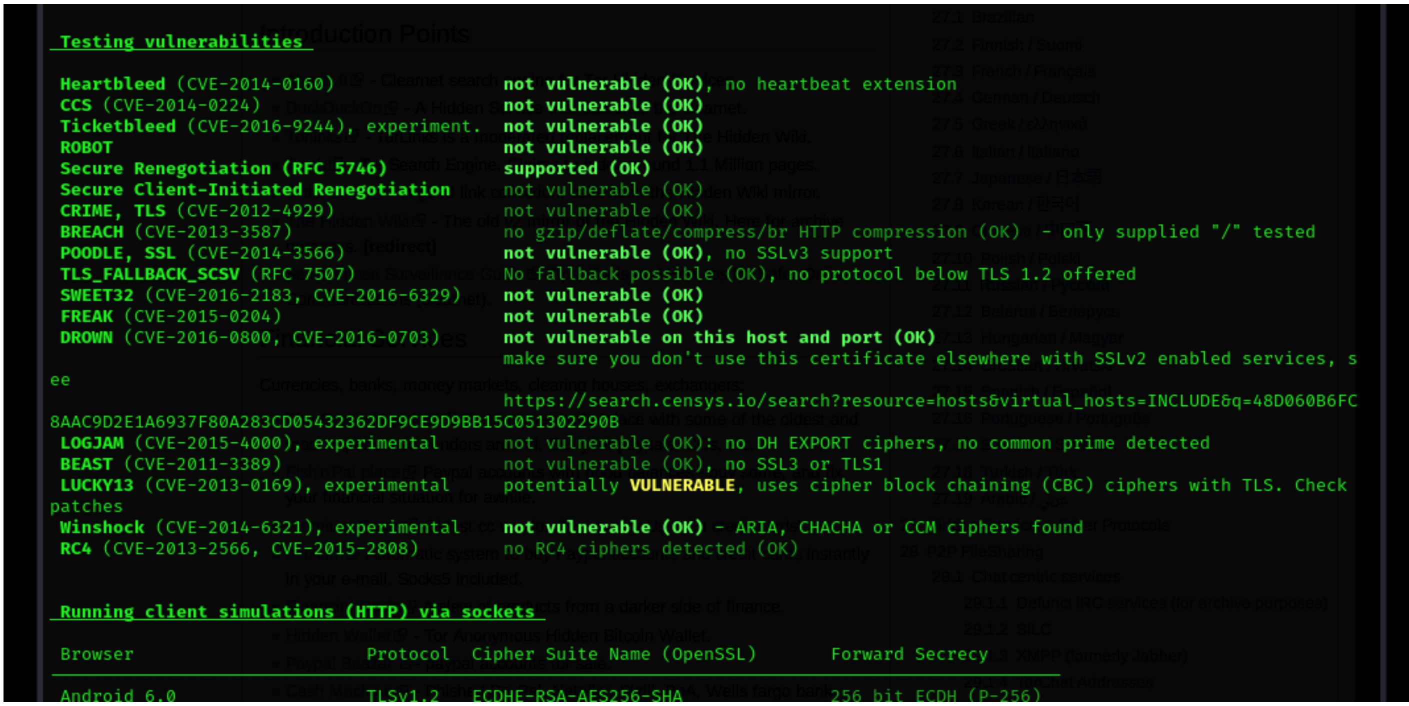
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits FS	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)	WEAK	128
TLS_RSA_WITH_AES_128_CCM (0xc09c)	WEAK	128
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)	WEAK	256
TLS_RSA_WITH_AES_256_CCM (0xc09d)	WEAK	256

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Se encontró una potencial vulnerabilidad

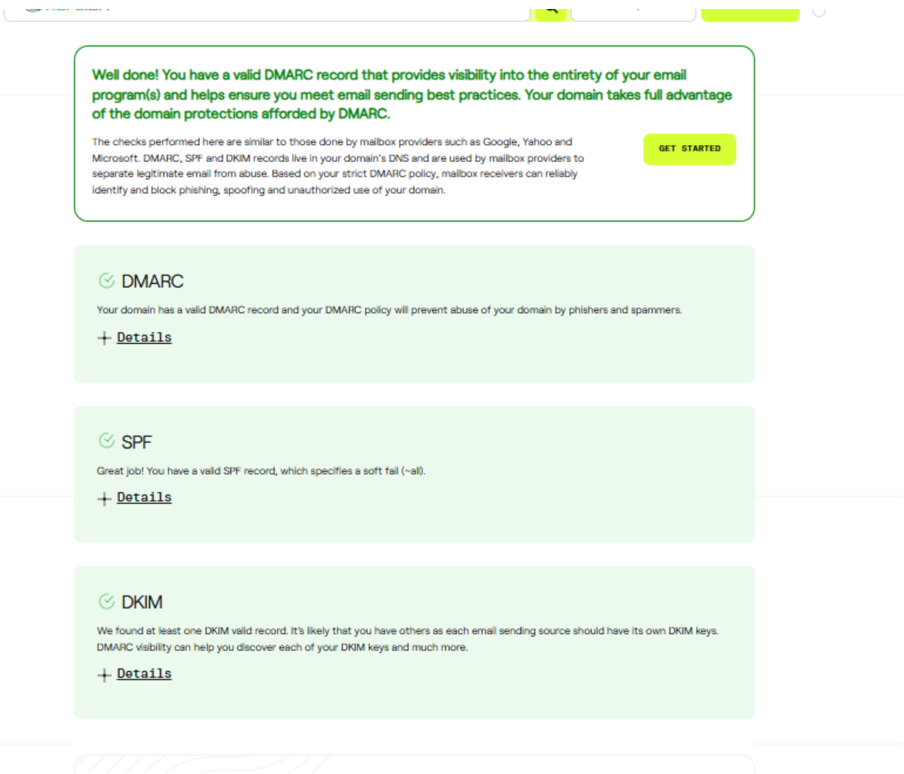
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP compression (OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services, s
ee
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=48D060B6FC
8AAC9D2E1A6937F80A283CD05432362DF9CE9D9BB15C051302290B
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no common prime detected
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check
patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - ARIA, CHACHA or CCM ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)


 Running client simulations (HTTP) via sockets 

 Browser                      Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
------------------------------------------------------------------------------------------------
 Android 6.0                  TLSv1.2   ECDHE-RSA-AES256-SHA              256 bit ECDH (P-256)
```

4.4 Análisis de servidores correo (DMARC/DKIM/SPF)

El dominio tiene configurado correctamente DMARC/DKIM/SPF para el dominio clover.com



Well done! You have a valid DMARC record that provides visibility into the entirety of your email program(s) and helps ensure you meet email sending best practices. Your domain takes full advantage of the domain protections afforded by DMARC.

The checks performed here are similar to those done by mailbox providers such as Google, Yahoo and Microsoft. DMARC, SPF and DKIM records live in your domain's DNS and are used by mailbox providers to separate legitimate email from abuse. Based on your strict DMARC policy, mailbox receivers can reliably identify and block phishing, spoofing and unauthorized use of your domain.

✓ DMARC

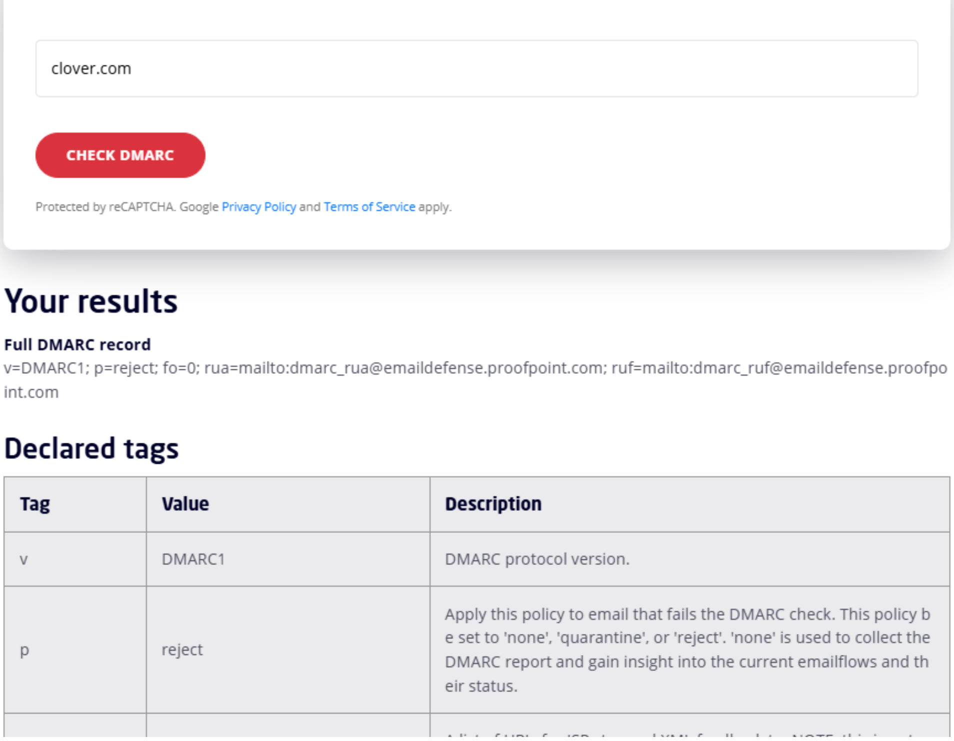
Your domain has a valid DMARC record and your DMARC policy will prevent abuse of your domain by phishers and spammers.

✓ SPF

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

✓ DKIM

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



clover.com

CHECK DMARC
Protected by reCAPTCHA. Google Privacy Policy and Terms of Service apply.

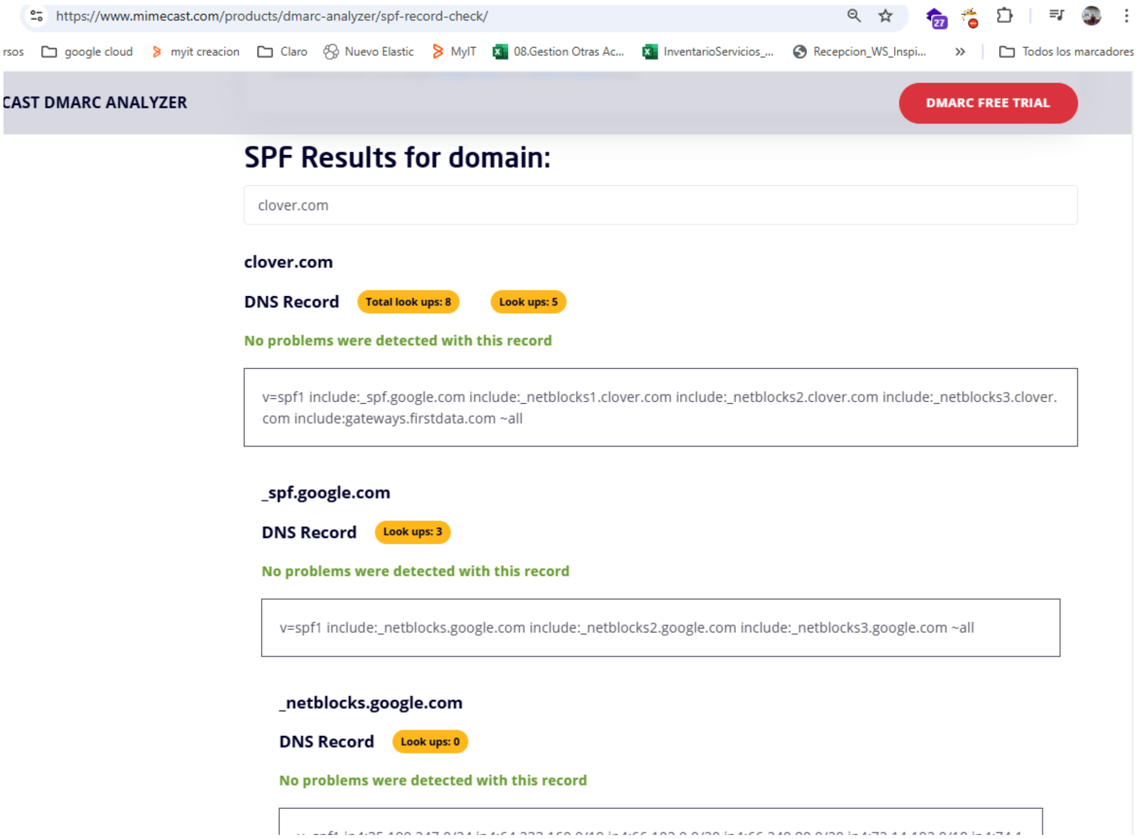
Your results

Full DMARC record

v=DMARC1; p=reject; fo=0; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com

Declared tags

Tag	Value	Description
v	DMARC1	DMARC protocol version.
p	reject	Apply this policy to email that fails the DMARC check. This policy be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current emailflows and their status.



SPF Results for domain:

clover.com

clover.com

DNS Record Total look ups: 8 Look ups: 5

No problems were detected with this record

```
v=spf1 include:_spf.google.com include:_netblocks1.clover.com include:_netblocks2.clover.com include:_netblocks3.clover.com include:gateways.firstdata.com ~all
```

_spf.google.com

DNS Record Look ups: 3

No problems were detected with this record

```
v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com ~all
```

_netblocks.google.com

DNS Record Look ups: 0

No problems were detected with this record

4.5 Detección de subdomain takeover (subzy)

Se encontraron los siguientes dominios los cuales permiten la adquisición de subdominios y podrían usarse se forma fraudulenta

c.clover.com

d.clover.com

c.staging.clover.com

docs.clover.com

d.staging.clover.com

nl.clover.com

partner.clover.com

sales.clover.com

talent.clover.com

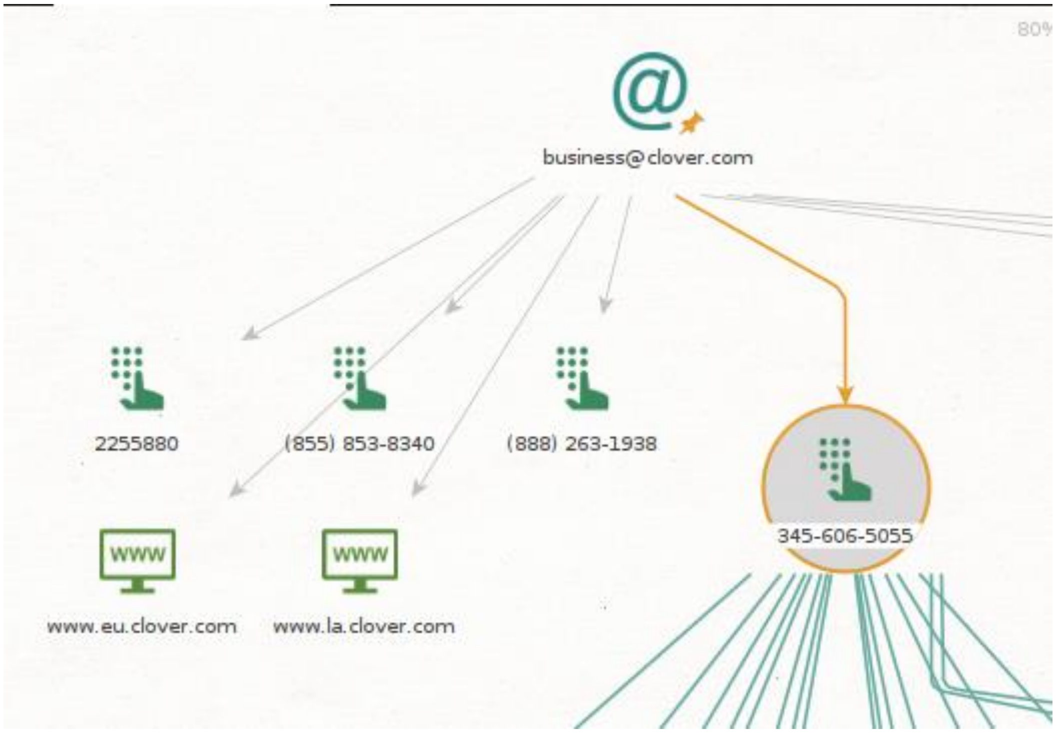
www.sales.clover.com

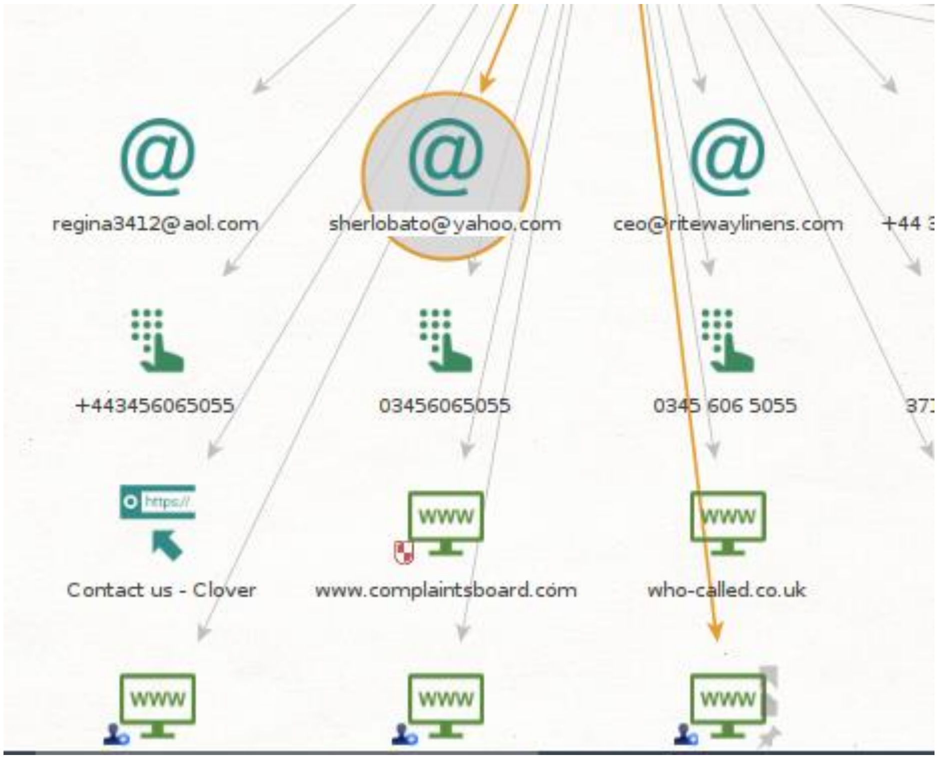
https://github.com/oscartobar/practicaskeepcoding/blob/main/RecopilacionInfo/subzy.txt

5 Técnicas OSINT

Encontrar correos electrónicos y/o usuarios / información sensible:

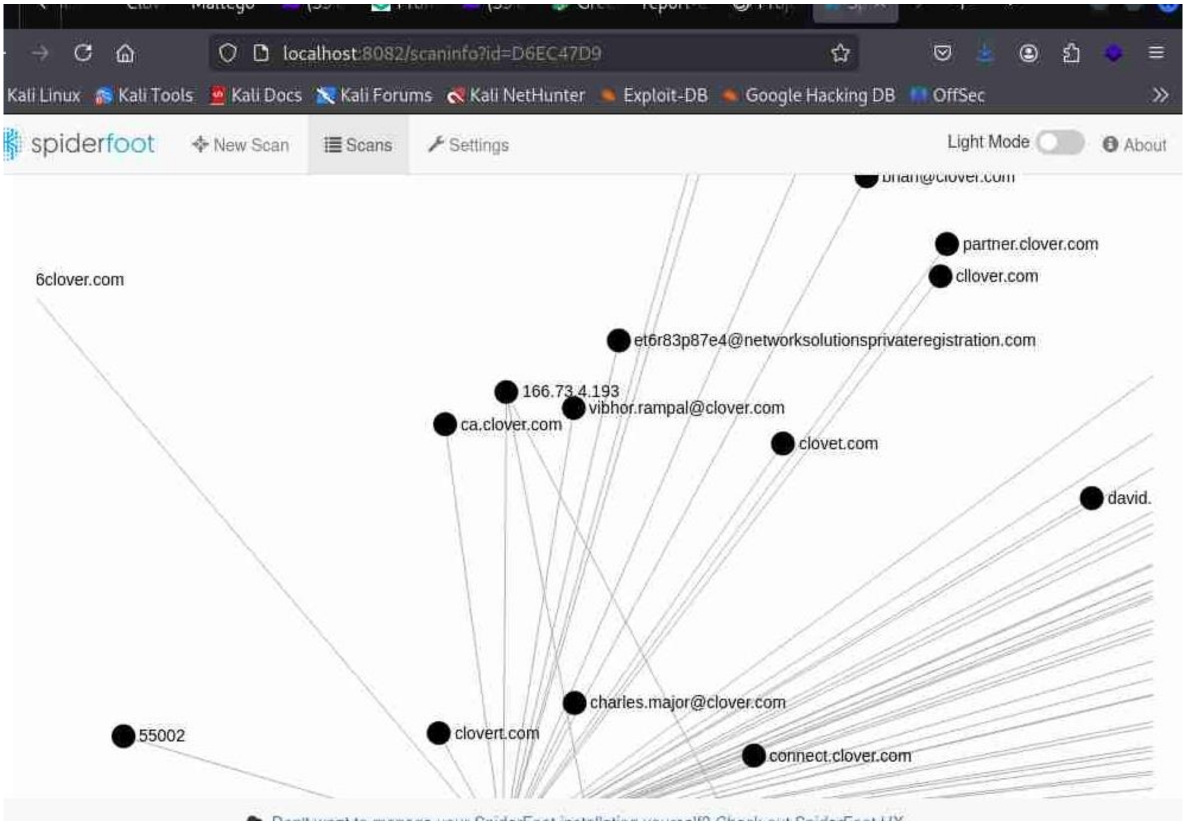
5.1 Maltego

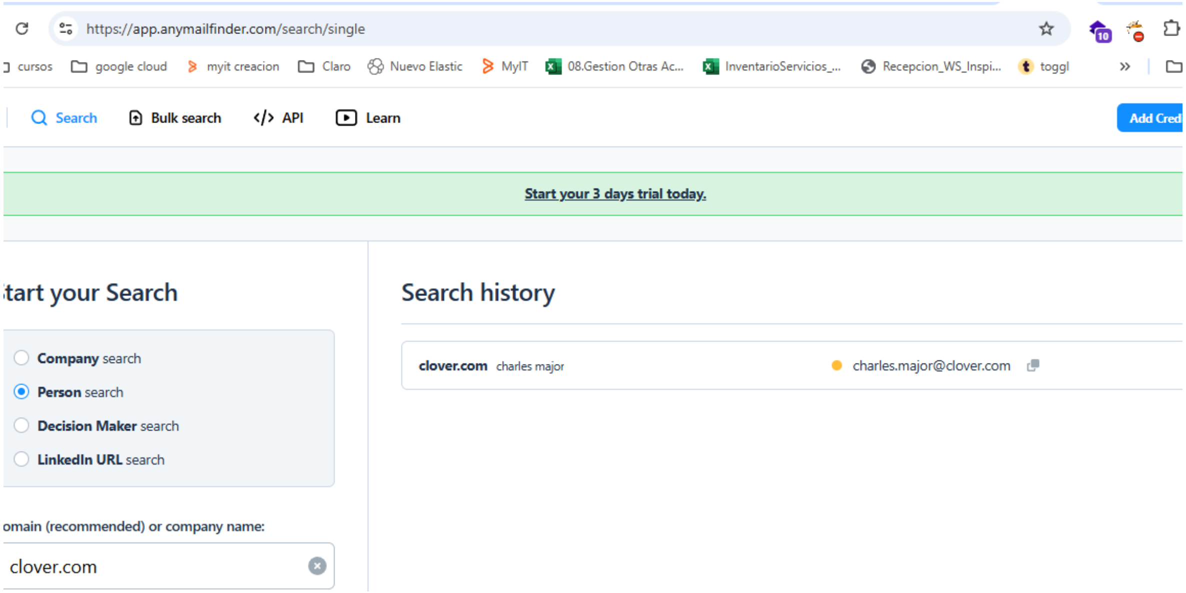

80%
business@clover.com
2255880
(855) 853-8340
(888) 263-1938
345-606-5055
www.eu.clover.com
www.la.clover.com


regina3412@aol.com
sherlobato@yahoo.com
ceo@ritewaylinens.com
+44 3
+443456065055
03456065055
0345 606 5055
37
https://
Contact us - Clover
www.complaintsboard.com
who-called.co.uk

5.2 Spiderfoot

Busqueda metadatos (exiftool + buscadores) Encontrar empleados potencialmente interesantes (por puesto, pro ejemplo): análisis de redes sociales (LinkedIn)





Start your 3 days trial today.

tart your Search

○ **Company** search
● **Person** search
○ **Decision Maker** search
○ **LinkedIn URL** search

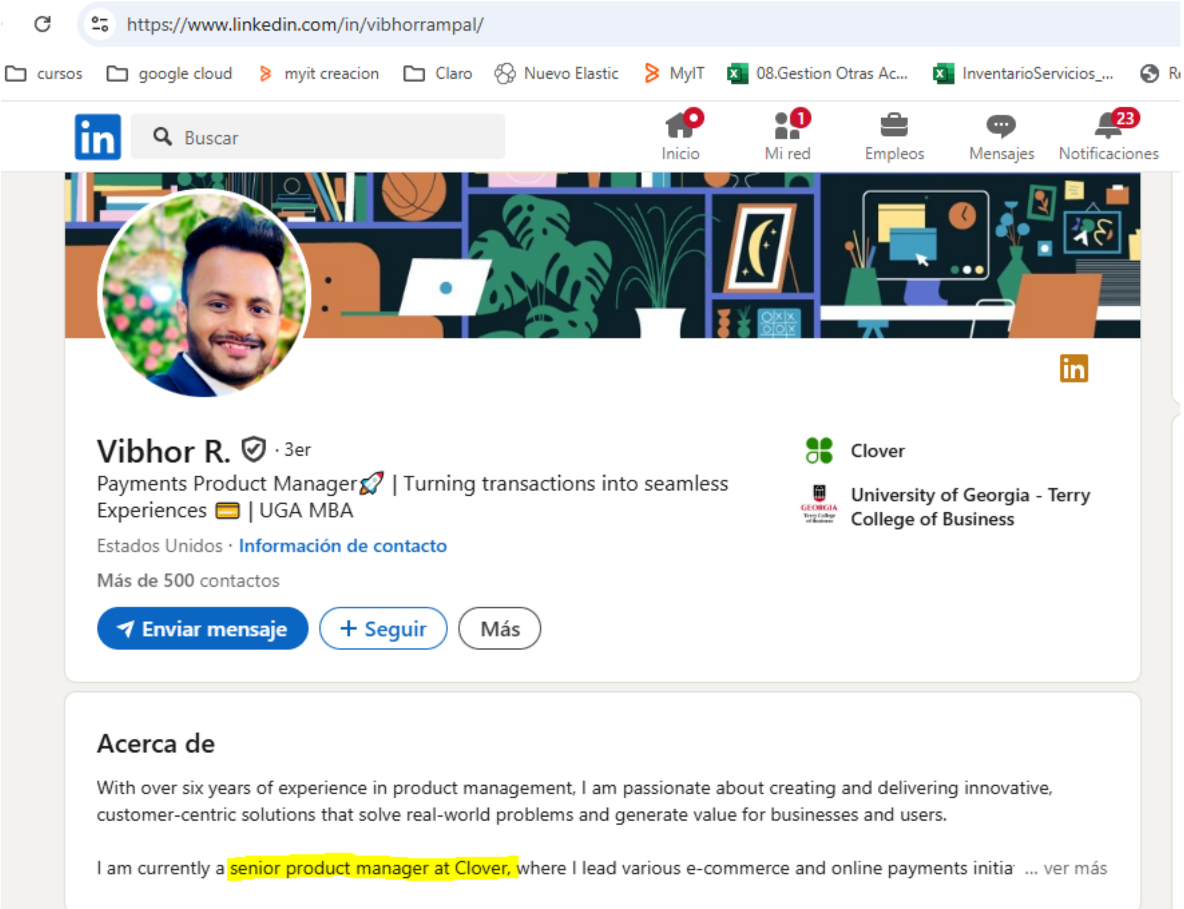
omain (recommended) or company name:

clover.com

Search history

clover.com charles major	●	charles.major@clover.com

Se encontro en LinkedIn el producto Manager de Clover y tiene publicado su correo personal



Vibhor R. · 3er

Payments Product Manager🚀 | Turning transactions into seamless Experiences 💳 | UGA MBA

Estados Unidos · Información de contacto

Más de 500 contactos

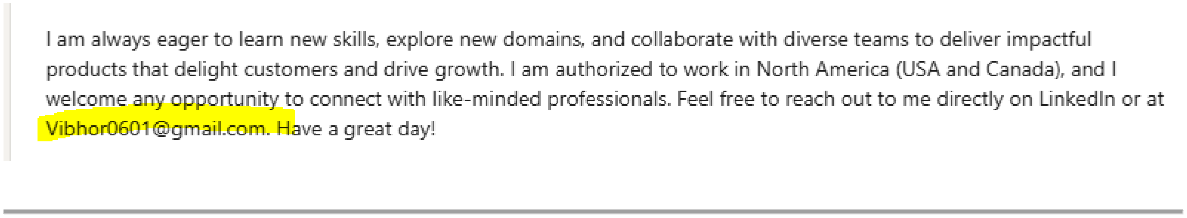
Clover

University of Georgia - Terry College of Business

Acerca de

With over six years of experience in product management, I am passionate about creating and delivering innovative, customer-centric solutions that solve real-world problems and generate value for businesses and users.

I am currently a senior product manager at Clover, where I lead various e-commerce and online payments initia ... ver más



> I am always eager to learn new skills, explore new domains, and collaborate with diverse teams to deliver impactful products that delight customers and drive growth. I am authorized to work in North America (USA and Canada), and I welcome any opportunity to connect with like-minded professionals. Feel free to reach out to me directly on LinkedIn or at Vibhor0601@gmail.com. Have a great day!