



Familia
Holk
Gold 7/8



Introducción

Durante mi paso por Holk Gold he empezado desde 0, pero como paso el tiempo fui recopilando todo lo aprendido y todo lo que yo sabía, así que por este medio les hago llegar a ustedes una guía con los siguientes temas:

- Que es un bin?
- Terminología
- Como crear tus cuentas con bin?
- VPN bueno y malo
- Extrapolación
- Como sacar tus cuentas autopagables vía sentry
- Que es una cc y los riesgos al hacer una compra física
- Como realizar una compra física
- Como sacar tus propios dorks
- Cómo usar SQLi

Que es un bin?

Un bin por lo regular son los primeros 6 dígitos de una tarjeta de crédito (puede tener más) estos bins tienes dos formas:

- 1.-el bin dice todo generado (no tiene fecha y ccv)

Ejem. 554222xxxxxxxxxx

lp usa.

- 2.-el q incluye fecha y ccv

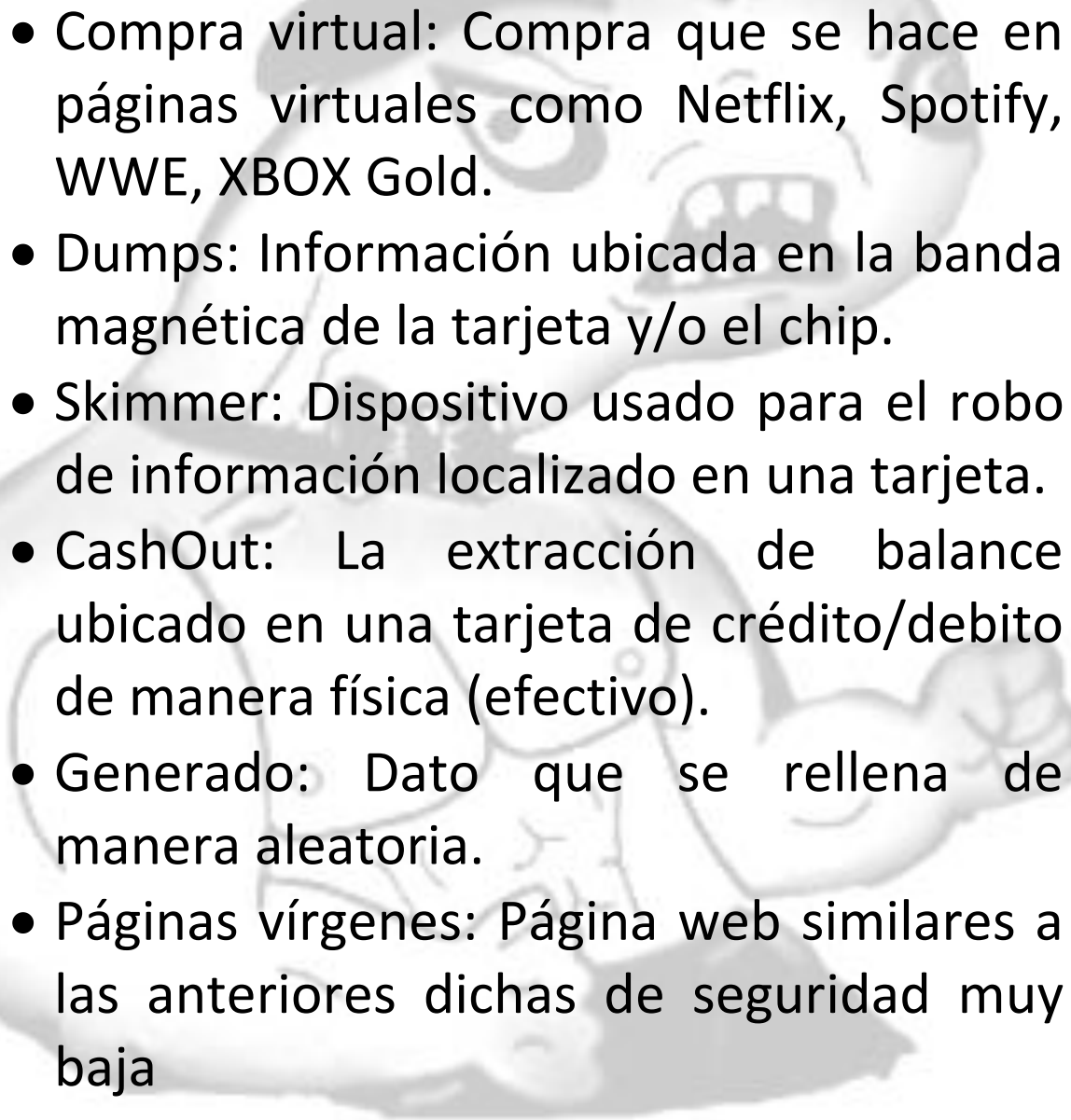
Ejemplo. 552344xxxxxxxxxx

Fecha: 02/21 ccv:180

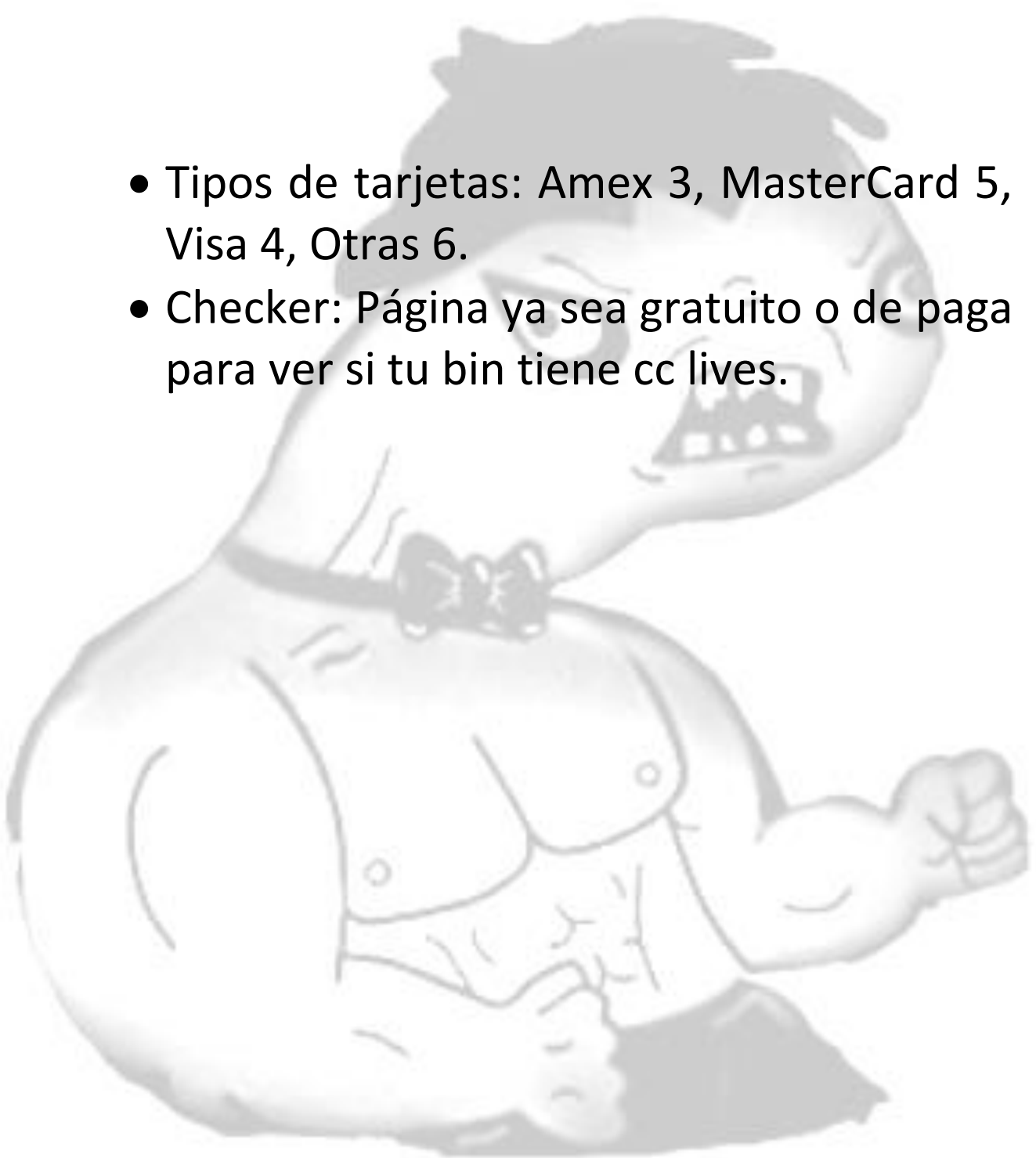
p usa.

Terminología

- CC: Credit Card (Tarjeta de crédito o débito)
- CC Live: Tarjeta con fondos que suele pasar más fácil.
- BTC: Bitcoins, moneda virtual.
- Lives: CC's que se encuentran en un estado de uso presente, es decir, que aún sirven.
- DROP: Persona que recibe por ti los pedidos que ejecutes.
- Ship: Confirmación de pago de alguna tienda virtual.
- Scam: Una estafa o un timo.
- Compra física: Compra que se hace desde páginas como "Amazon (AMZ), Mercado libre (ML), Linio, EBay, etcétera y se hace envío.

- 
- Compra virtual: Compra que se hace en páginas virtuales como Netflix, Spotify, WWE, XBOX Gold.
 - Dumps: Información ubicada en la banda magnética de la tarjeta y/o el chip.
 - Skimmer: Dispositivo usado para el robo de información localizado en una tarjeta.
 - CashOut: La extracción de balance ubicado en una tarjeta de crédito/debito de manera física (efectivo).
 - Generado: Dato que se rellena de manera aleatoria.
 - Páginas vírgenes: Página web similares a las anteriores dichas de seguridad muy baja
 - Pa'l monte: Te pillaron :v
 - Pasarela: Método de pago de las páginas.
 - -Shipped: Correo que confirma que tu pedido te va a llegar.

- Tipos de tarjetas: Amex 3, MasterCard 5, Visa 4, Otras 6.
- Checker: Página ya sea gratuito o de paga para ver si tu bin tiene cc lives.



Creación de cuentas con bins

Fácil ejemplo si el bin dice esto

Bin Dezzter

123456xxxxxxxxxx

IP USA

Todo Generado

Van a ir a su VPN y pondrán su IP en USA, ya que esta así prosigue a la siguiente página:

cc.namsopro.com

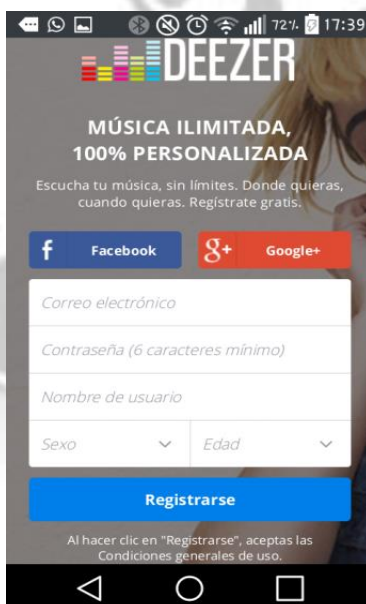
Ya que están ahí ingresan su bin.

The screenshot shows the NamsopCCGen v5 web application. At the top, there's a navigation bar with 'Iniciar sesión' and 'Registrarse' links. Below it, the title 'NamsopCCGen v5' is displayed. A 'Menu' button is visible. The main section is titled 'Generador' and includes social media links for Twitter and Facebook. A form is present with the following fields: 'Inserte su Bin' (containing '123456xxxxxxxxxx'), 'Agregar' (with a plus icon), 'Fecha' (checked), 'CCV2' (checked), 'Tipo Banco' (unchecked), and 'Cantidad a crear' (set to '10').

The screenshot shows the 'Generar Tarjetas' screen. At the top, there's a dropdown menu labeled 'Rnd'. Below it, a button labeled '</> Generar Tarjetas' is visible. The main area displays a list of 10 generated card numbers, each followed by a date in YYYYMM format. A close button (X) is in the top right corner. At the bottom, there's a button labeled 'Guardar en un archivo'.

123456754673375311120221913	120221913
123456155853884610120211900	120211900
123456113865484010120191214	120191214
1234560541154745106120201439	120201439
123456387414475412120191162	12120191162
1234568635450663106120191131	106120191131
1234566675104778104120211829	104120211829
1234566462434313109120191624	13109120191624
1234567600855518101120191469	18101120191469
1234562518524413101120221139	13101120221139

Bueno hecho es te paso no dirigimos a la página de deezer y nos registramos.



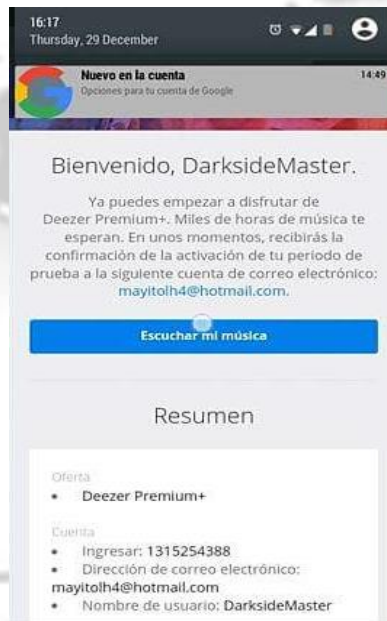
The screenshot shows the Deezer mobile app's registration interface. At the top, the Deezer logo is displayed. Below it, the text reads "MÚSICA ILIMITADA, 100% PERSONALIZADA" and "Escucha tu música, sin límites. Donde quieras, cuando quieras. Regístrate gratis." There are two social login buttons: "Facebook" and "Google+". Below these are input fields for "Correo electrónico", "Contraseña (6 caracteres mínimo)", and "Nombre de usuario". There are also dropdown menus for "Sexo" and "Edad". A prominent blue "Registrarse" button is at the bottom. A small disclaimer states: "Al hacer clic en 'Registrarse', aceptas las Condiciones generales de uso."

Después de registrarnos nos mandara al método de pago, ponemos nombre random amos a la pestaña del generador (namso) copian los primeros 16 dígitos de la cc generada los siguientes son el mes y el año os últimos tres son el CCV.



The screenshot shows the Deezer payment page, titled "PAGO". It contains a form for entering payment details. The fields are: "Nombre del titular de la tarjeta" (empty), "Número de tarjeta bancaria" (with the value "4859 3424 6578 1748" and a checkmark), "Fecha de expiración" (with dropdowns for "Mes" and "Año"), and "Código de seguridad" (with a dropdown and a checkmark). Below the form, there is a message: "Empezar mi periodo de prueba de 30 días, luego pagar MXN 99/mes." At the bottom, there is a small disclaimer: "Confirmo que he leído y acepto Condiciones generales de uso. Al dar click en « Empezar mi periodo de prueba », acepto tener acceso inmediato al servicio sin beneficiarme de un..."

Pegan los 16 dígitos de la cc fecha y el
CCV = Código de seguridad
Si el bin es funcional les saldrá esto.



Y listo su primera cuenta
Si no les da prueben con otra cc.

VPN

El VPN es una app o programa que funciona para cambiar la dirección IP esta es muy utilizada por los bineros ya que se utiliza para cambiar de IP al país correspondiente al bin

Existen varias por ejemplo:

- vyprvpn
- tunellbear
- opera vpn
- HMA.
- Hide my ip

Etc...

Hay uno llamado hola VPN este no lo utilicen si les cambiara la IP pero usara la suya para otro usuario.

Extrapolación

Suponemos que es una CC
5436275676566765 Pero ojo que las ex
se hacen solo cuando el bin muere y
nunca jalan al 100 a la primera debes
tener paciencia hasta que te agarre el
ritmo, (siempre guarda la última cc que
te caló) Suponemos que esa es la Cc
ultima que te caló y la vamos a
extrapolar).

Fácil lo haces en namso 5 donde dice
generar cc a bin o lo haces a mano como
yo

(543627) 5676566765

Lo que está en paréntesis no se toca

Coges el resto

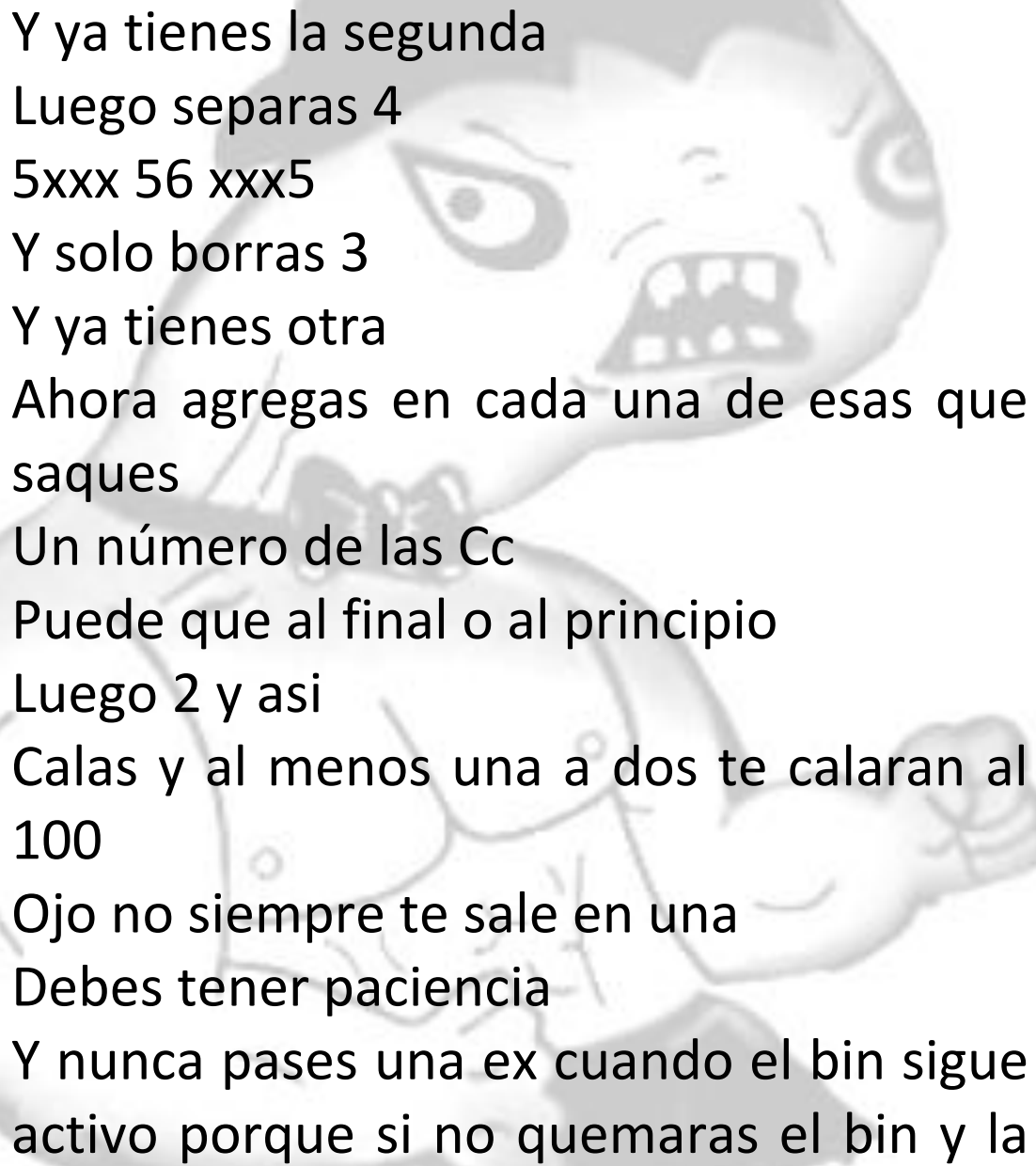
Primer paso separas dos

x6 76xx67 6x

Ya tienes tu primera ex

Luego separas 3

xx7 6xx6 7xx



Y ya tienes la segunda
Luego separas 4
5xxx 56 xxx5
Y solo borras 3
Y ya tienes otra
Ahora agregas en cada una de esas que
saques
Un número de las Cc
Puede que al final o al principio
Luego 2 y así
Calas y al menos una a dos te calaran al
100
Ojo no siempre te sale en una
Debes tener paciencia
Y nunca pases una ex cuando el bin sigue
activo porque si no quemaras el bin y la
ex nunca te va a jalar

Cuentas autopagables (Sentry)

sentry es una herramienta de crackeo o programa usado para sacar cuentas de alguien que básicamente la suda o paga, se ha estado usando estos últimos años para sacar cuentas de diferentes plataformas y alguna gente las vende algo que es muy pendejo y es motivo de ban si encontramos una publicación de ese estilo de parte de ustedes sea o no en el muro de holk gold. Como se usa? Es fácil, y pasó por pasó pueden hacer todo bien, les daré la palabra clave o de felicidad al usar esto. :v "hit" es cuando localiza una cuenta que está siendo actualmente usada y pagada, es una de las cuentas que calaran y si les entra, será un éxito, aquí un pequeño video para que se guíen mejor ya que la mayoría de ustedes no entienden del todo a pesar de lo que eh escrito y lo sé.

<https://youtu.be/-GWHXtaPmvnl>



(Vyprvpn.ini) Está es una configuración que usaran ahorita para la plataforma seleccionada (Vyprvpn) usen 150 bots y hagan todo lo que dice el video mejor el proxyless

Espero les funcione, es importante decir que no cambien ni correo ni contraseña de las cuentas sacadas.

O básicamente serán desactivadas por el dueño, suerte de nuevo, ya saben qué hacer.

Que es una cc y los riesgos al hacer una compra física

¿Qué es una cc?

Simple en inglés es Credit Card :v

En español truncó es Tarjeta de crédito.

Ya pasando el Significado simple de cc digo otra cosa.

¿Qué es una cc Fullz?

Es una tarjeta con todos sus datos.

Cómo es eso preguntan

Simple mijines

Es una tarjeta con sus direcciones de facturación, país de origen y nombré de del propietario.

¿Qué es una cc Live?



Es una cc generada basada de un bin que tiene créditos.

Sin olvidar que cada compañía de tarjetas de crédito ejemplo.

Visa y MasterCard tienen 16 dígitos.

3 números que son la cvv y las fechas.

Las Cc Amex tienen 15 dígitos y empieza con un 3.

Tiene 4 números que son la cvv y sus fechas.

Ya pasado eso sigo con el siguiente tema.

Sé que solo vieron la palabra "FÍSICAS" se les alumbro los ojos para saber cómo se hacen.

Pero antes de eso explicó.

¿Hay algún Riesgo al hacer una física?

Pues en realidad si hay riesgos como que te caiga la patrulla y Pal Monte papú :V.

En realidad si tiene algunos riesgos, si sabes que hiciste todo bien no habrá problema, si tuviste un incidente al pasar el pago no hay que alarmarse si usan un Drop y facturen a otra dirección que no sea su residencia no hay problema.

Puede que me desvíe del tema sólo quiero decir que no exageren en sus compras ósea, no quieran comprarse un puto iPhone con bins.

Ahí necesitan Ccs Fullz y con drop por si los pedos.

Si te preguntas ¿es legal binear?

Pues no :v ya que le estas robando pero vlv si estas solo comprando membresías kks.

Ya que pase este tema sobre riesgos no muy especificado que la mayor pena en mi pais es el robo de identidad y eso conlleva a 5 a 10 años de Cárcel pero eso pasa si tratas de comprar algo muy sobrepasado valor.

Ya cuando sepan más podrán realizarlo.

Ya que pase el tema este sigo con el otro.

Posible es lo que más esperan

Cómo se hace una física?

Pues siendo sincero amigos es muy fácil, si estas usando bin claro no vayas a Joder amazon con un algo mayor de 100 dólares pensando que pasara.

Amazon pasa hasta mi credencial estudiantil.

Con bin se haría empieza con cosas pequeñas 5 dólares e ir subiendo.

Algunos dirán, ME COMPRE UNA CC COMO HAGO PARA NO QUEMARLA?

Pues simple no se la mamen comprando cosas mayores a su balance.

Me desvíe del tema sorry.

Tengo un vídeo de cómo realizar una física pero enseñó misa datos reales y pues no.

En explicación.

Primero necesitamos un VPN

Poner la IP del bin que dice el bin

Ejemplo:

41472021xxxxxxxxx

Ip Usa (ni lo calen es el chabelo místico).

Ponen su VPN en Usa.

Van a la página que dice el bin

Eligen su producto y le dan en Checkout.

Cuando lleguen donde dice

Shipping Adress

Ahí ponen todos sus datos reales o como carajos llegara sus pedidos?

Luego

Generan el bin ósea en cc.namsopro.com u otro generador.

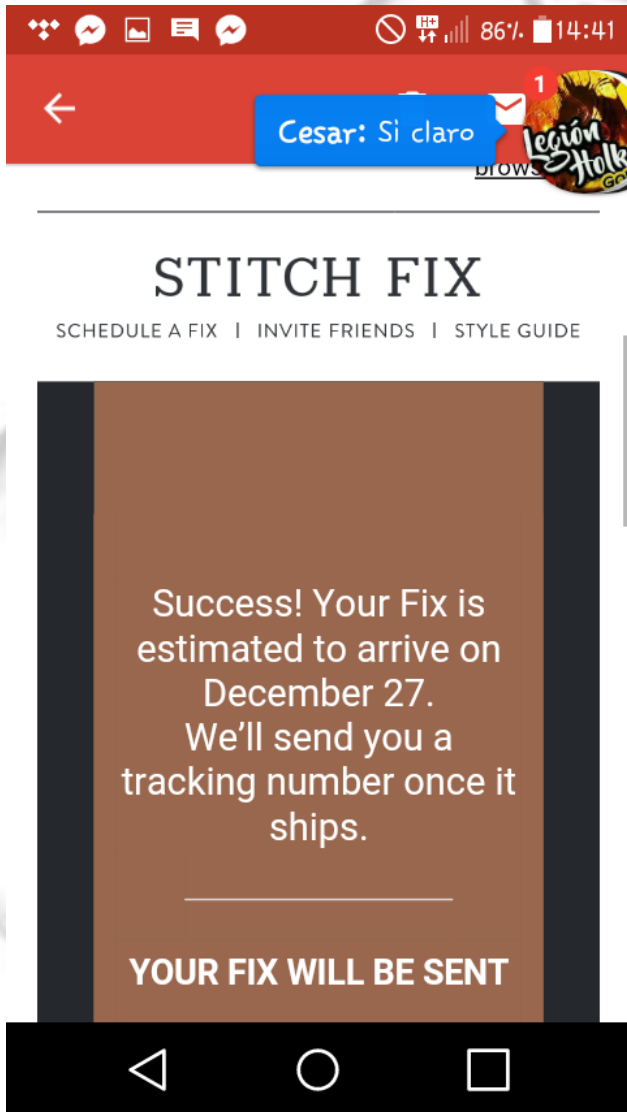
Sacan lives de un checker (recomiendo sacar siempre sacar lives)

Ya que ahí pedirán la cc.

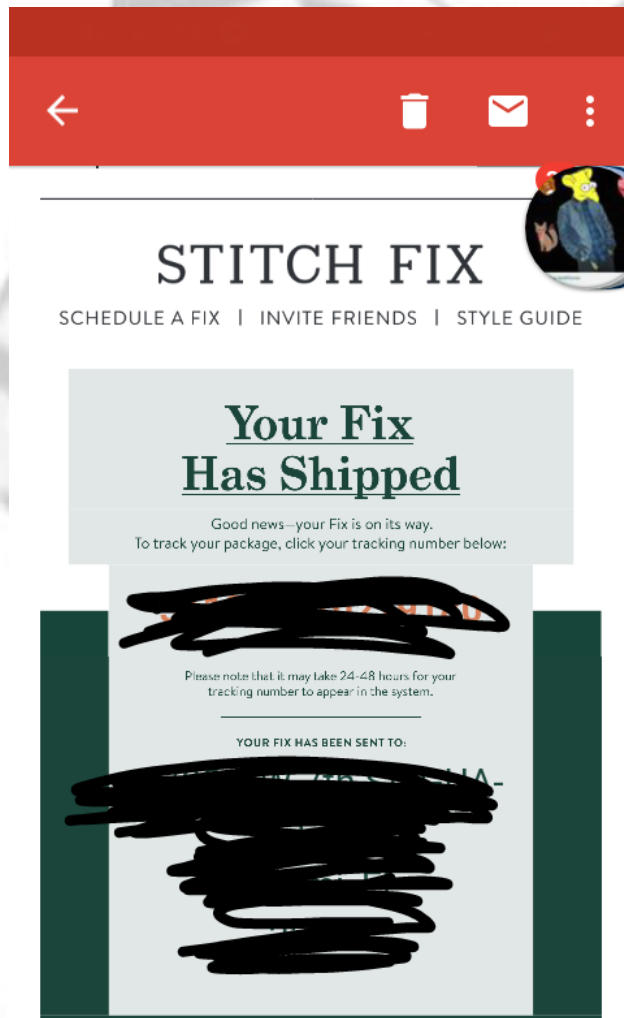
abajo de donde ponen la cc o cuando esten en la Shipping adress dira "Use Shipping adress for Billing Adress?" le dan que no

Ya que tienen que poner otra ya que en la billing dejan la factura y ahí puede ser que te cargue el payaso.

Cuando les manden este mensaje en su eMail Registrado.



Es que paso pero aún no ha dado ship si



Reciben este mensaje

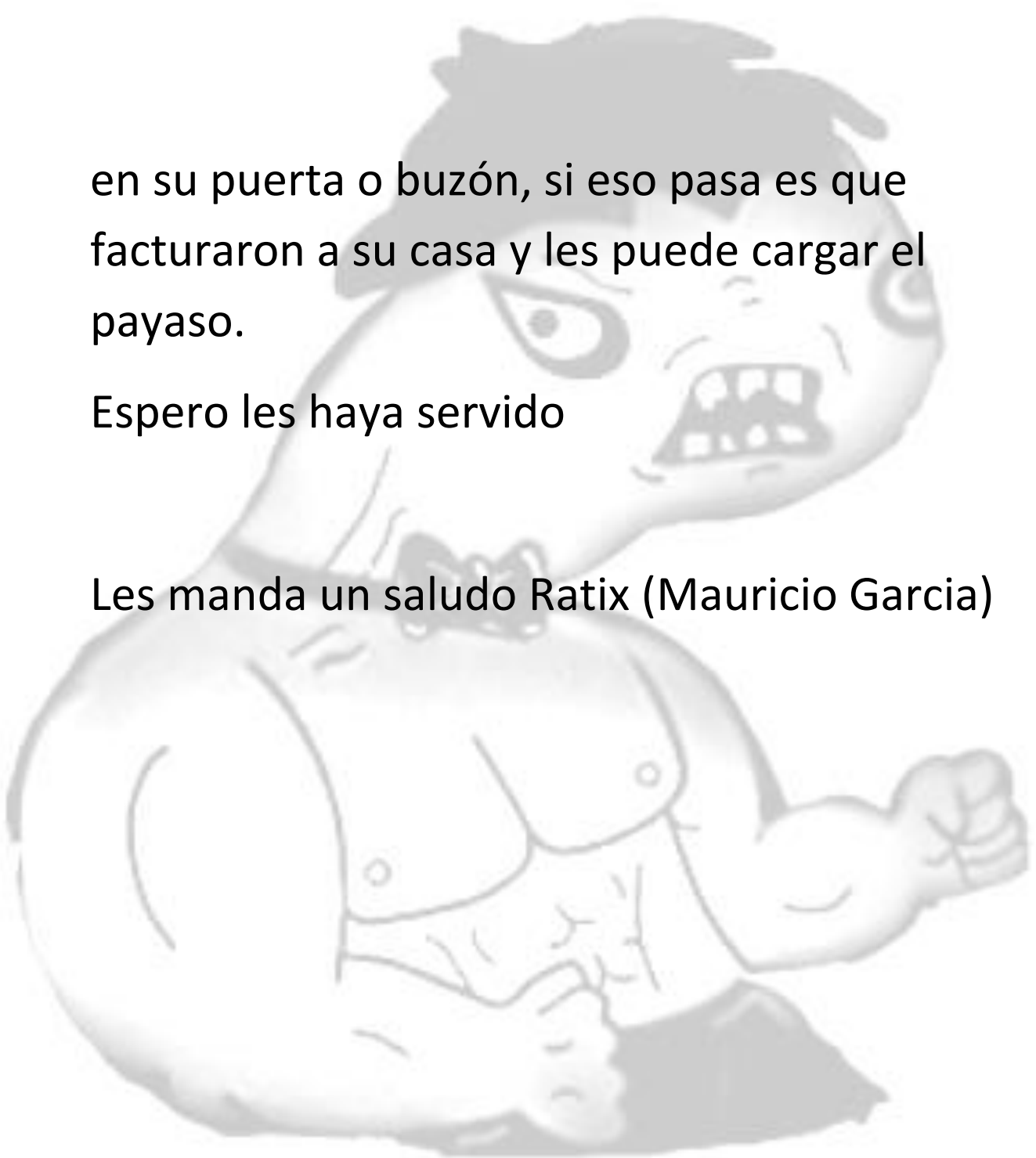
Apláudanse ya que es su primer ship.

Si el día que reciben el paquete ven algo que no cuadra pues se van y dejan que lo dejen

en su puerta o buzón, si eso pasa es que
facturaron a su casa y les puede cargar el
payaso.

Espero les haya servido

Les manda un saludo Ratix (Mauricio Garcia)



Como sacar tus propios dorks

Que son dorks?

Los Dork son palabras claves que se usa para encontrar sitios vulnerables.

Un ejemplo de Dork seria la siguiente :

noticia.php?id=

En google deberíamos poner la siguiente:

inurl:noticia.php?id=

Esto nos dará muchos resultados de sitios que quizás ya no sean vulnerables. Pero es por eso que debemos ir intentando dork , hasta que logremos dar con una.

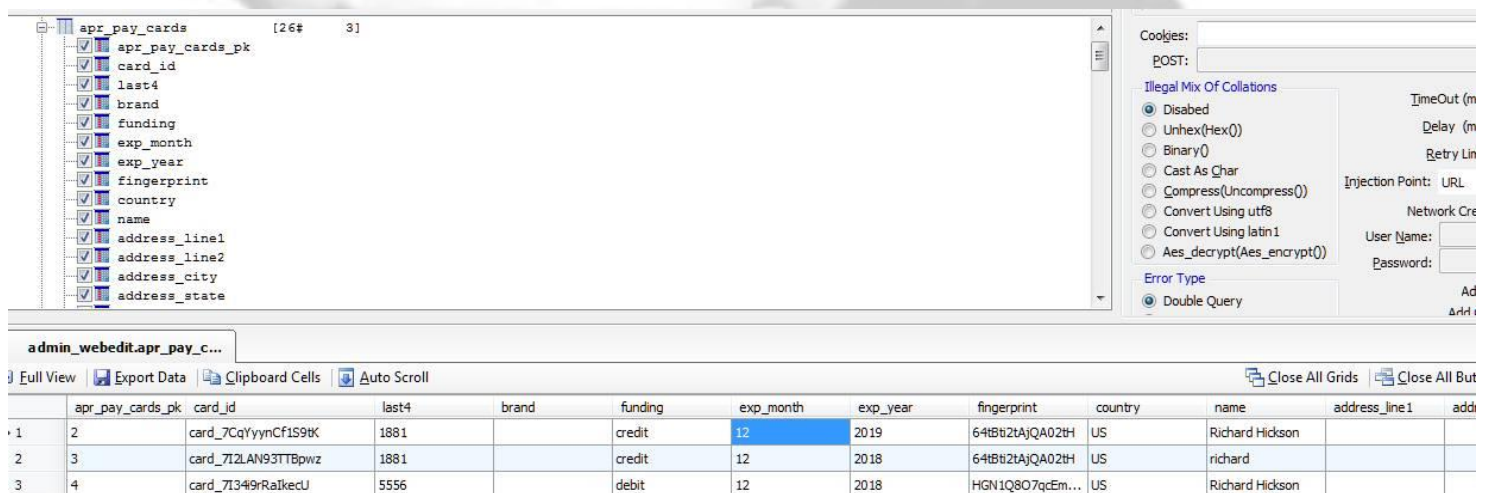
Como generar doks?

El método para generar dork seria cambiar el noticia por otro nombre, por ejemplo: News , photo , remeras , etc.

¿Ya tengo la página vulnerable, que hago?

Deberíamos buscar un programa llamado "Havij" con ese programa explotas y entras a la Bases de Datos de la página y con ella sacas información , sacas los usuarios y contraseñas , etc.

Dorks en SQLi



The screenshot displays a web application security tool interface. On the left, a tree view shows the structure of a database table named 'apr_pay_cards'. The table has columns: apr_pay_cards_pk, card_id, last4, brand, funding, exp_month, exp_year, fingerprint, country, name, address_line1, address_line2, address_city, and address_state. The main panel shows a table of data for this table. The table has 4 columns: apr_pay_cards_pk, card_id, last4, and brand. The data rows are:

apr_pay_cards_pk	card_id	last4	brand
2	card_7CqYynCf1S9K	1881	
3	card_712LAN93TTBpwz	1881	
4	card_71349Raikecu	5556	

On the right side of the interface, there are settings for the attack, including 'Illegal Mix Of Collations' and 'Error Type' (set to 'Double Query'). The 'Injection Point' is set to 'URL'. The 'User Name' and 'Password' fields are empty.

Cómo usar SQLi

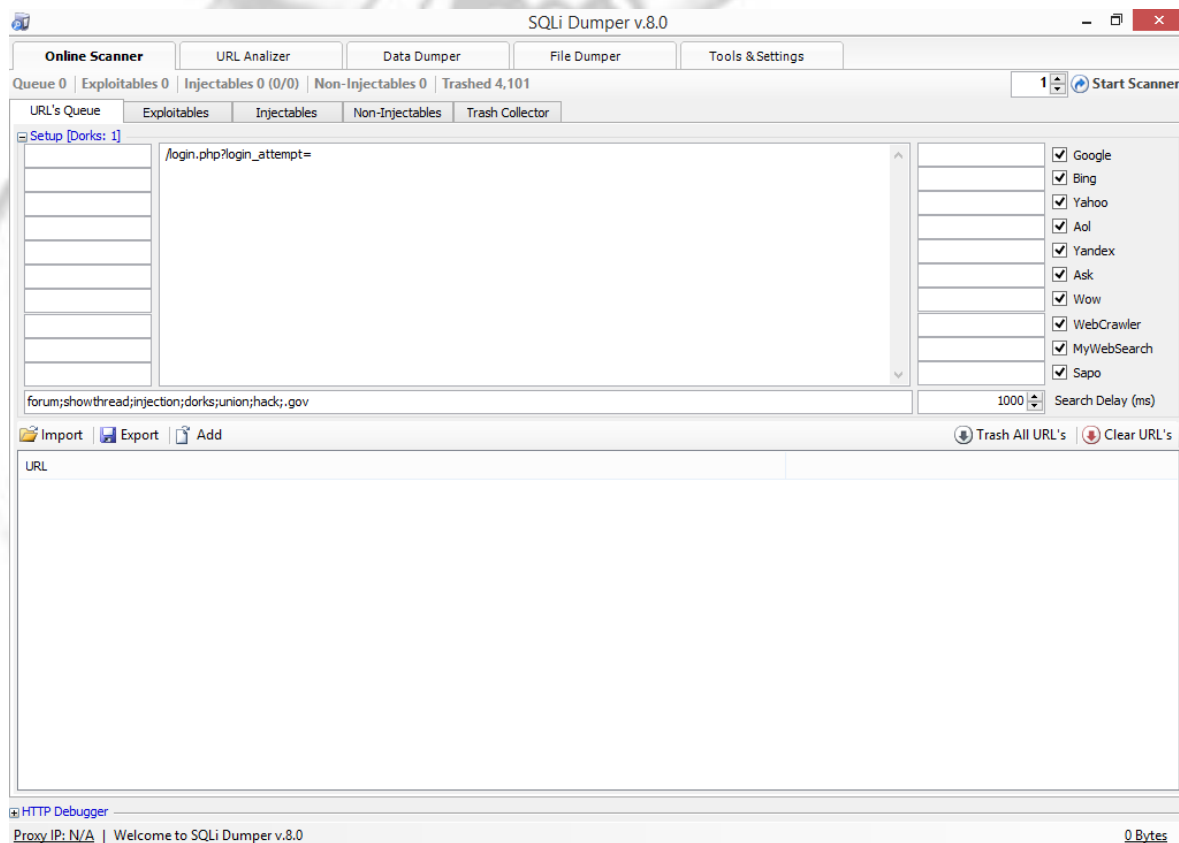
Guia sobre uso de SQLi Dumper.

En esta Guia se les explicara lo que es SQLi y como realizar inyecciones de este mismo

SQL Injection es una vulnerabilidad que permite a un atacante realizar consultas a una base de datos, se vale de un incorrecto filtrado de la información que se pasa a través de los campos y/o variables que usa un sitio web, es por lo general usada para extraer credenciales y realizar accesos ilegítimos, práctica un tanto neófita, ya que un fallo de este tipo puede llegar a permitir ejecución de comandos en el servidor, subida y lectura de archivos, o peor aún, la alteración total de los datos almacenados.

Link de descarga de SQLi:

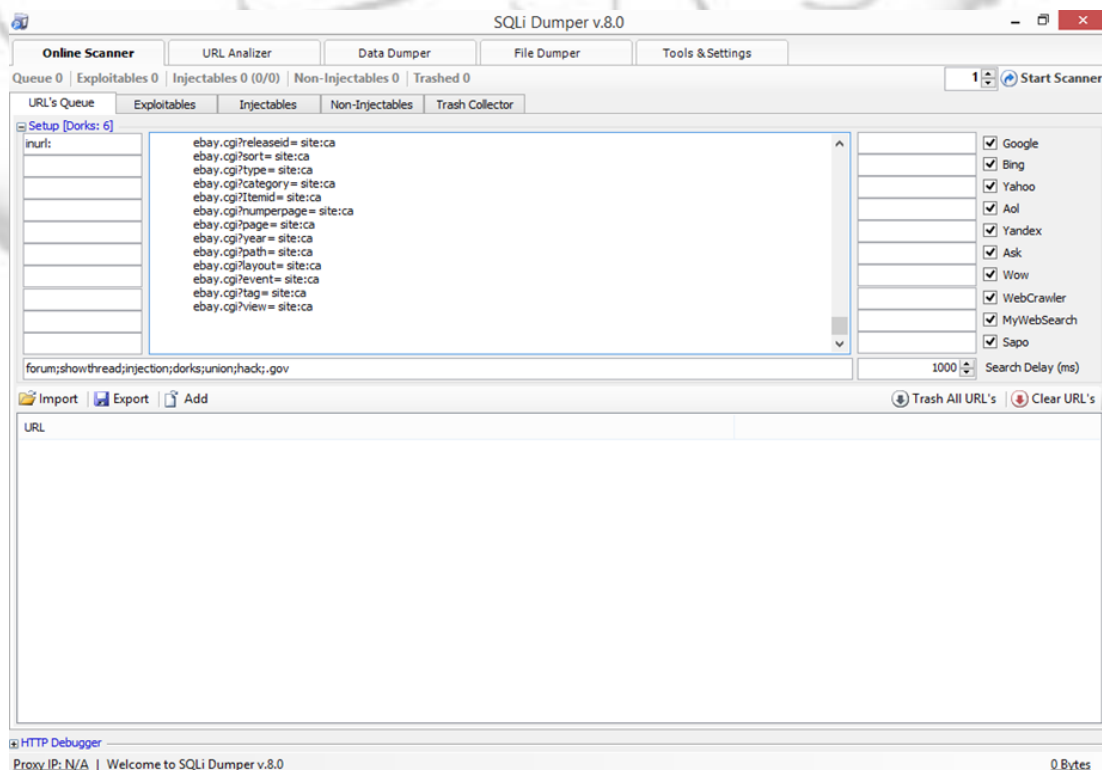
<https://mega.nz/#!HFh2kT5Y!t61dvC1DcelpQhVBO5GeKGvA8jMIHokSmQdTUhvJWno>



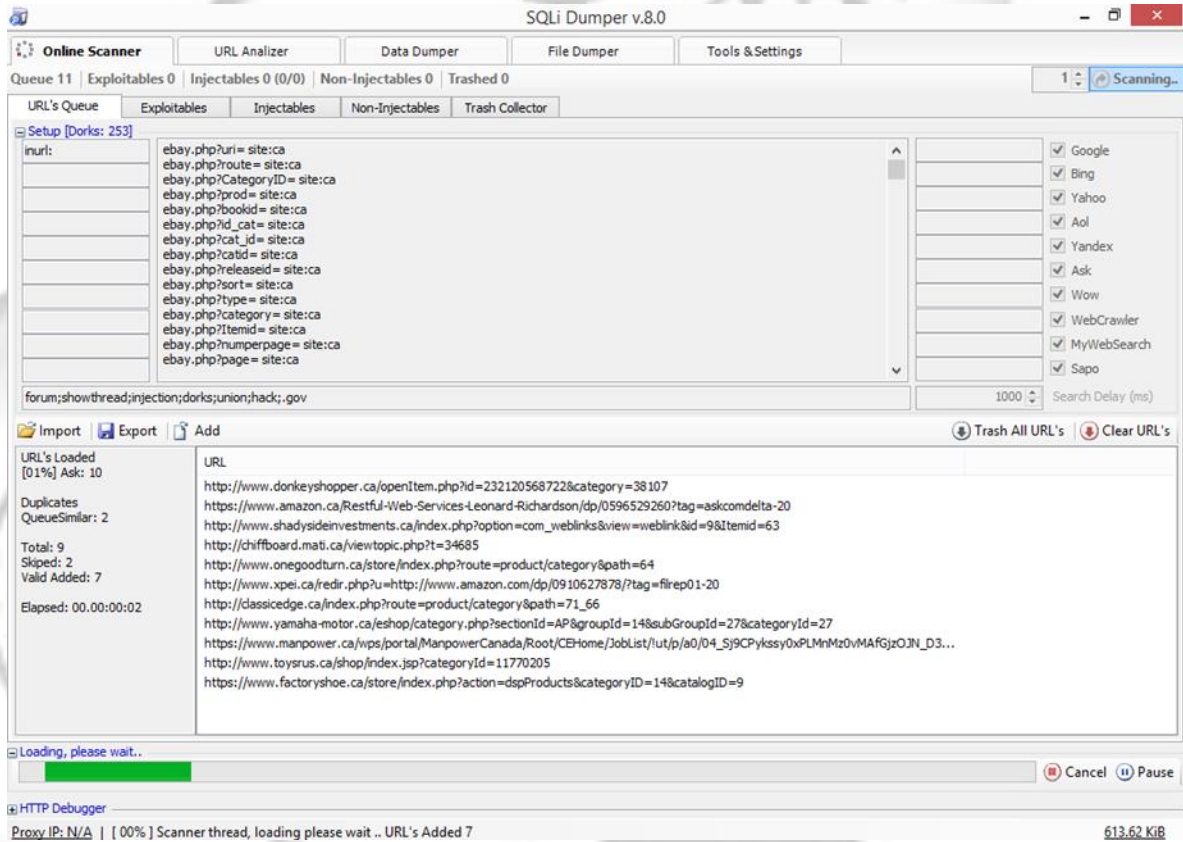
A si se ve el programa, en la parte blanca se van a insertar los dorks, ¿Qué son los dorks? Los dorks los podemos interpretar como textos claves sacados de google, estos se utilizan para extraer información valiosa o sensible desde Google

Lo que ven ahí es en la parte blanca es la base de un dork, alado del signo “=” se puede poner cualquier página, ya sea PayPal, Uber, Netflix, etc...

Simple teniendo ya todos los Dorks los copias y pegas en la parte blanca



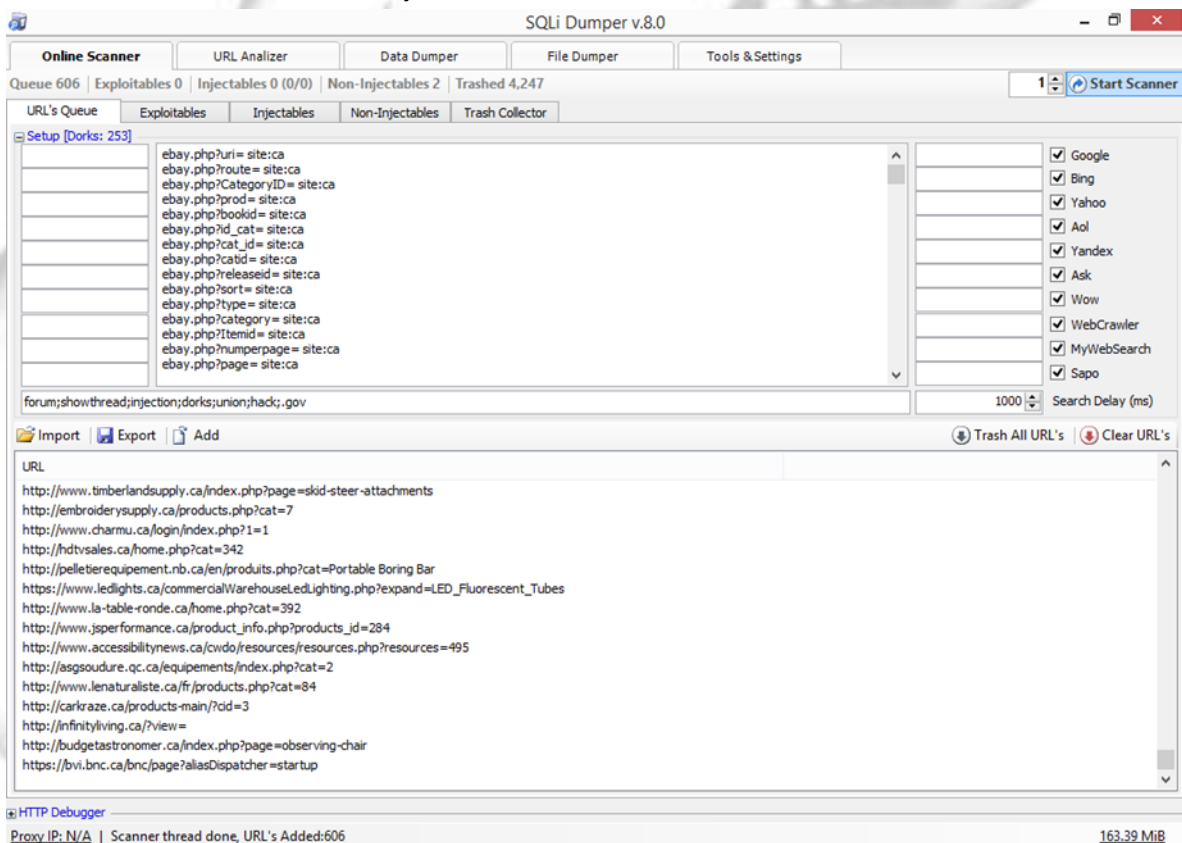
Ya con los dorks le dan en “Start Scanner”, una vez que le den empezara a escanear los dorks



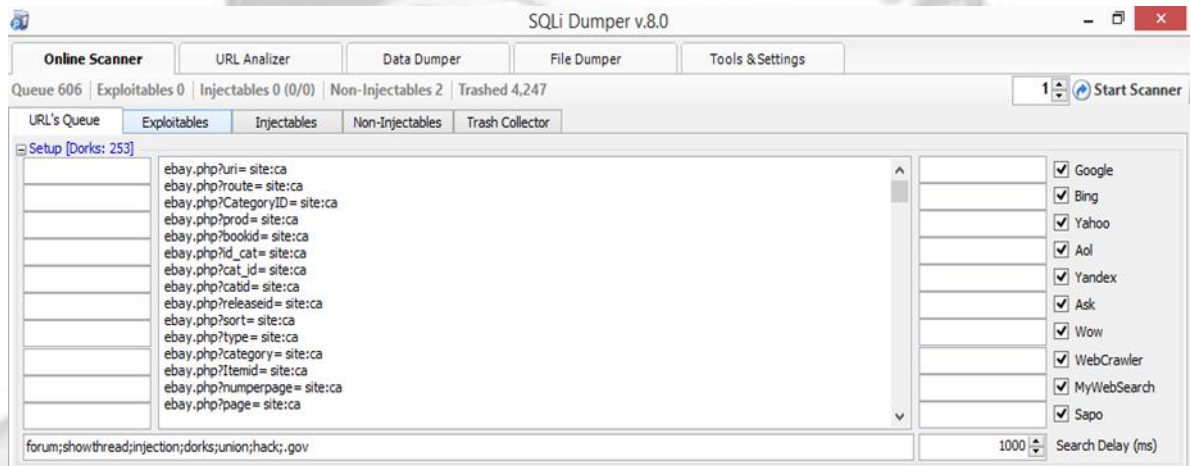
Yo recomiendo que esperen unos 15 o 20 minutos para que el programa haya recabado bastantes urls o si son pacientes esperen hasta que acabe con todos los dorks, si no fueron pacientes y esperaron 15 o 20 minutos denle

“Cancel”, este botón se encuentra en la parte inferior derecha de su monitor.

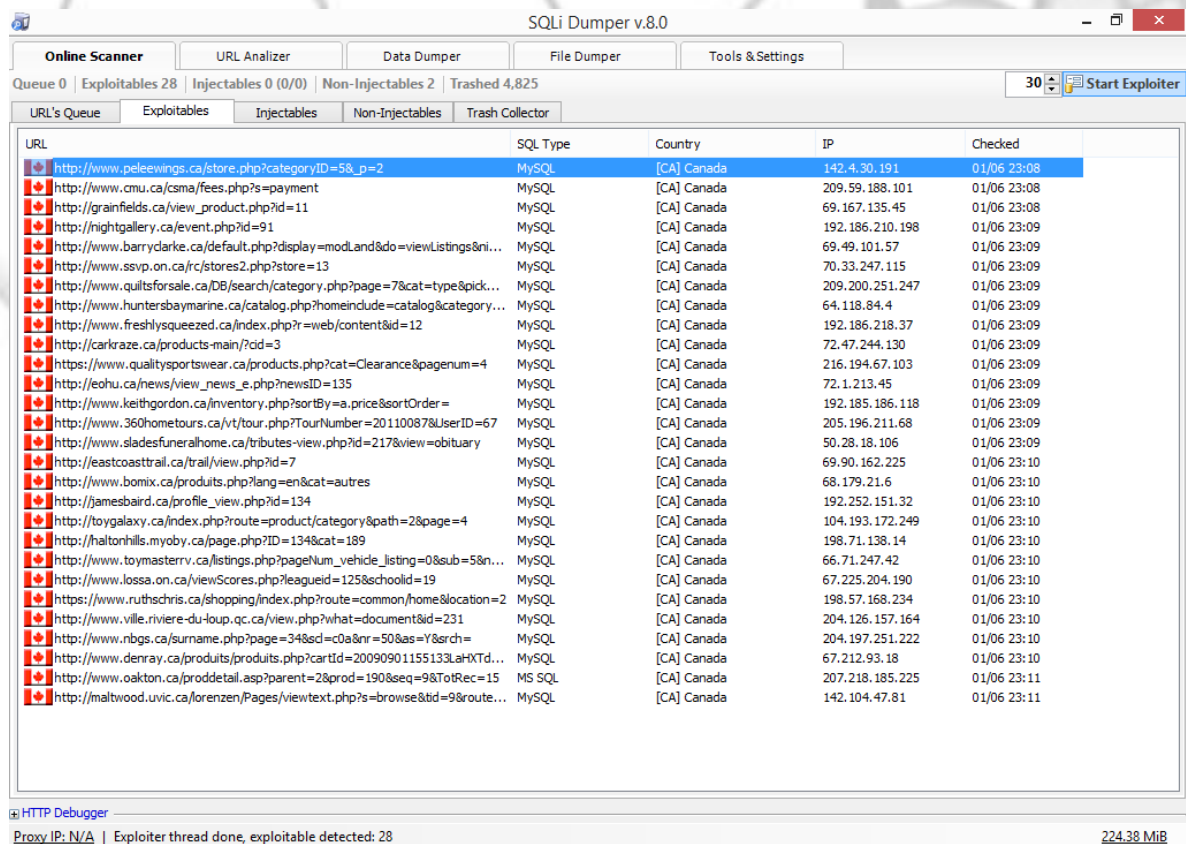
Una vez cancelado les saldrán las urls escaneadas, este será el interfaz



Ahora nos iremos a “Exploitable”

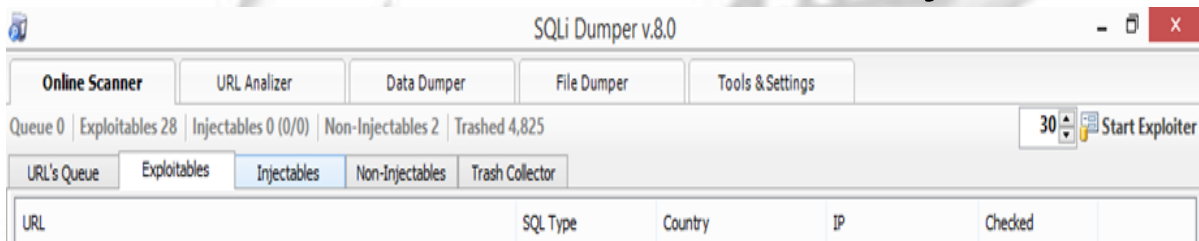


Ya en Exploitable le daremos en Start

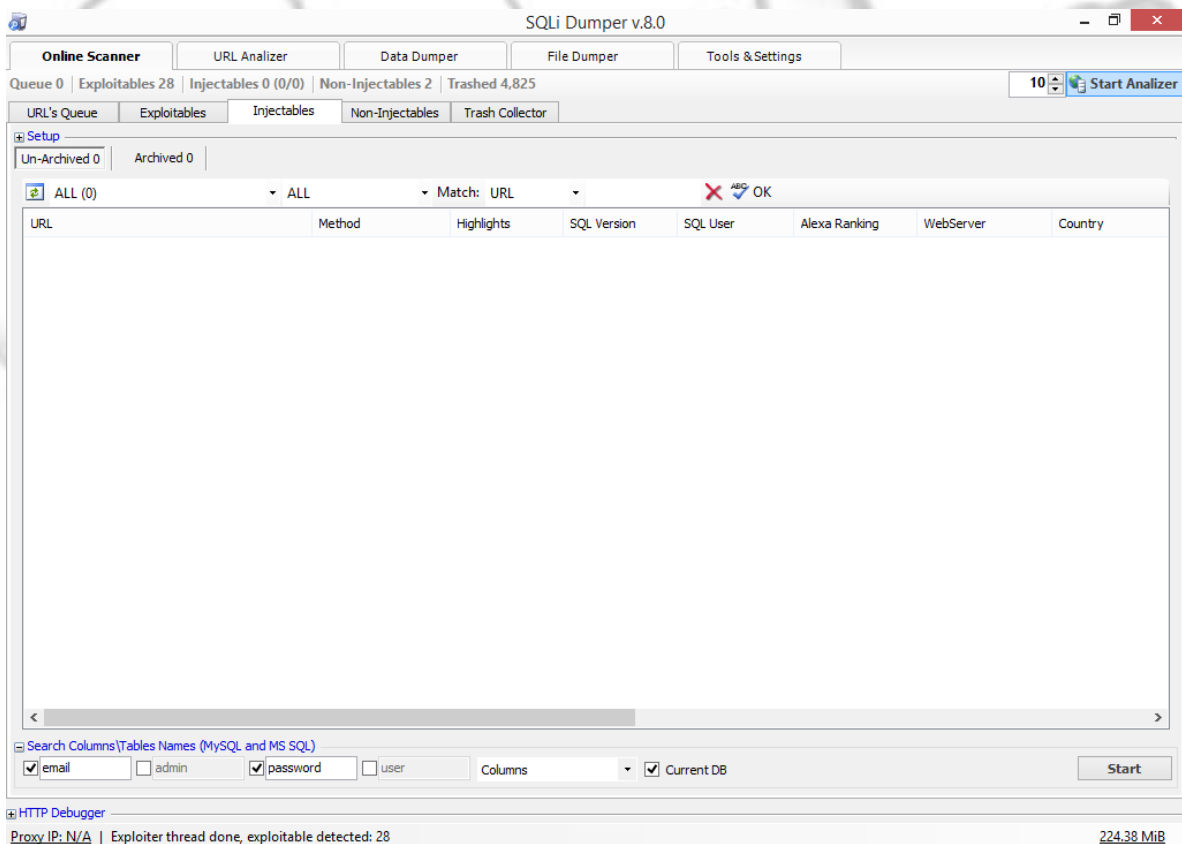


Exploiter, esperamos a que la barra de porcentaje llegue a 100%, ya acabado les saldrán las paginas

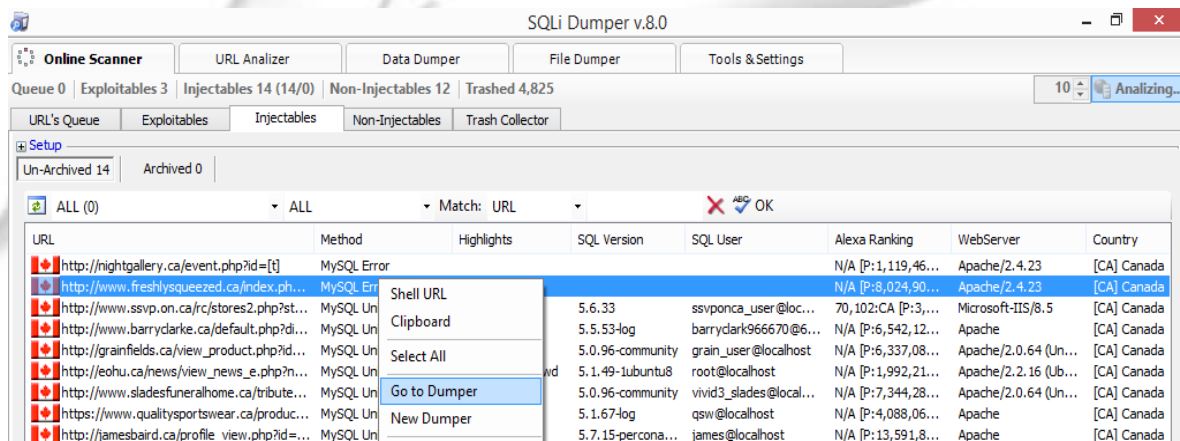
Ahora nos vamos a “Injectables”



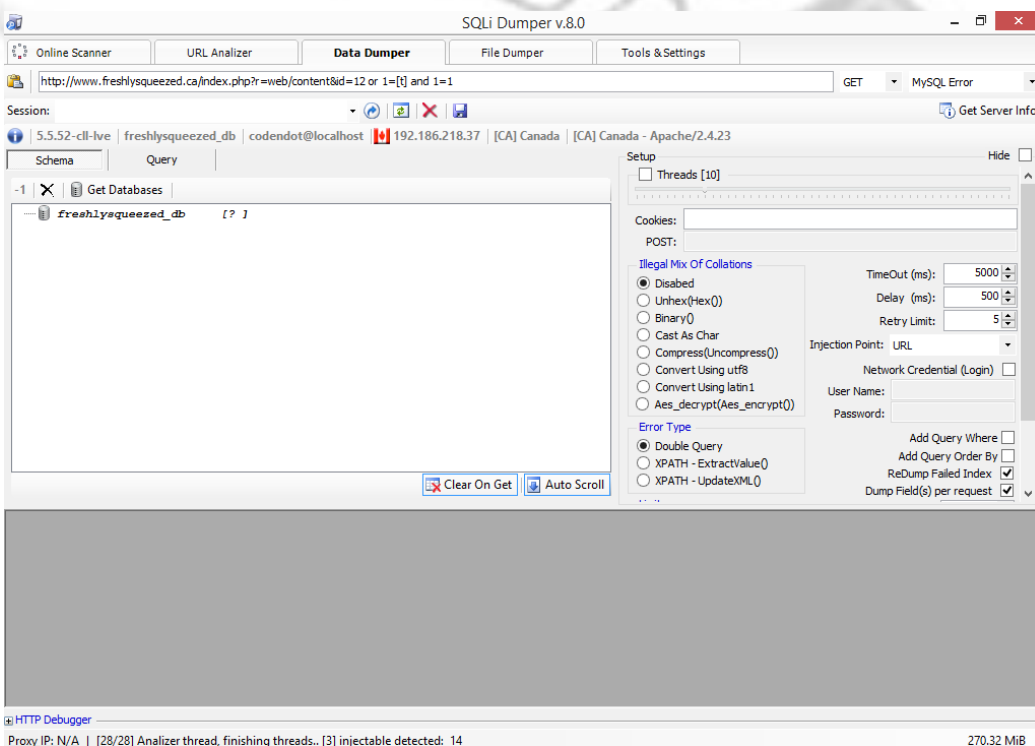
Y le damos en “Start Analyzer”



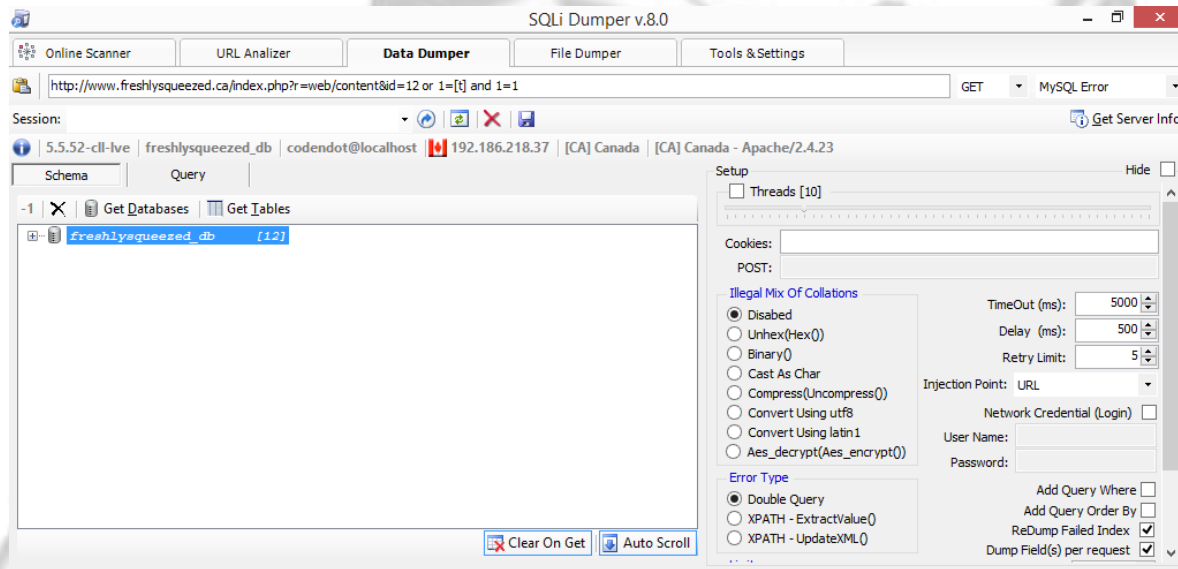
Esperamos a que acabe y nos saldrán las páginas que tiene vulnerabilidad, escogemos un link, el que sea y le damos click derecho y seleccionamos la opción que dice “Go to dumper”



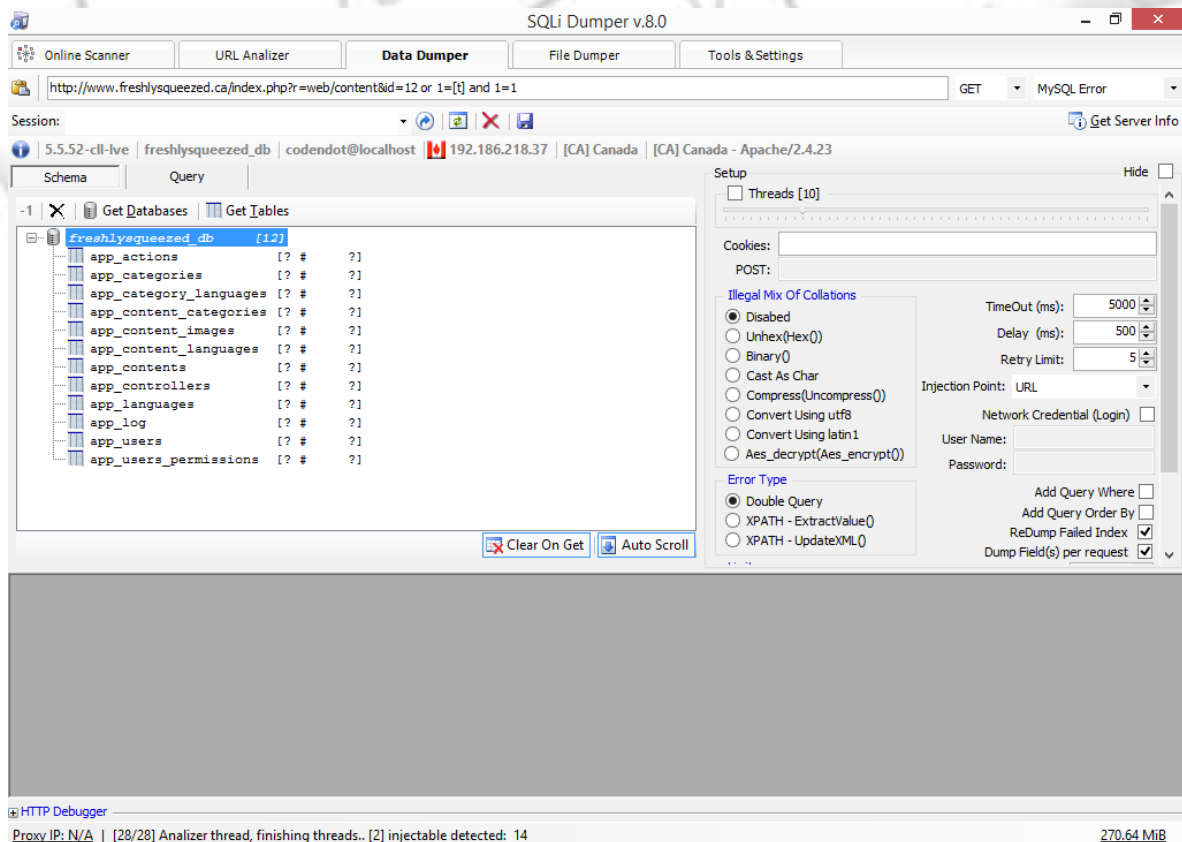
Esperamos a que la barra se llene y nos saldrá esto



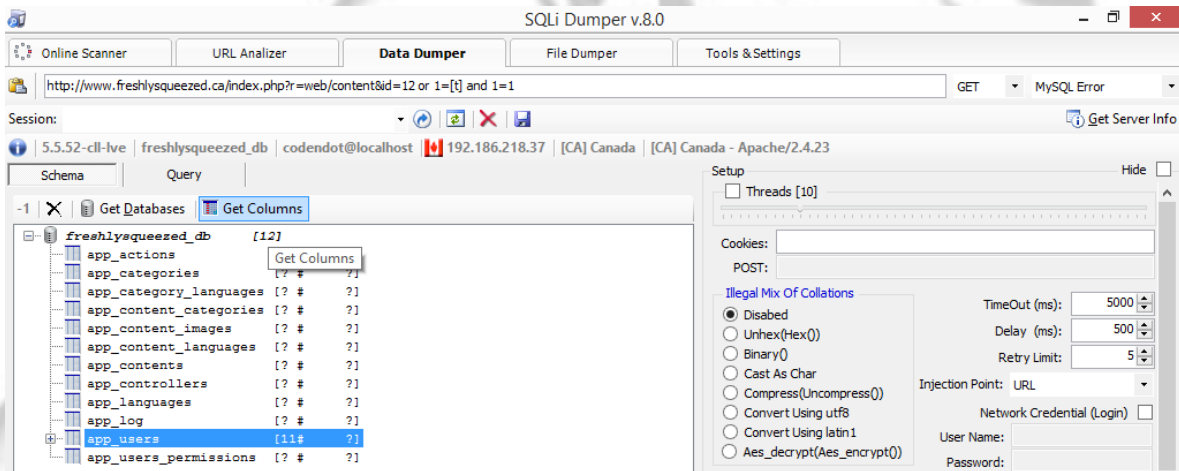
Seleccionamos la “Date base” y le damos en Get tables



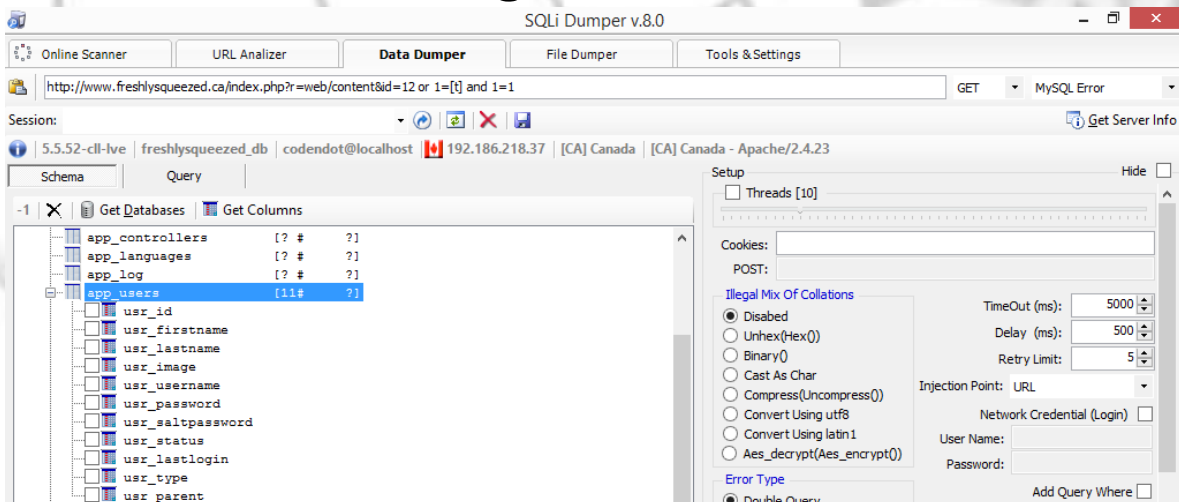
Nos aparecerán las opciones desglosadas, así



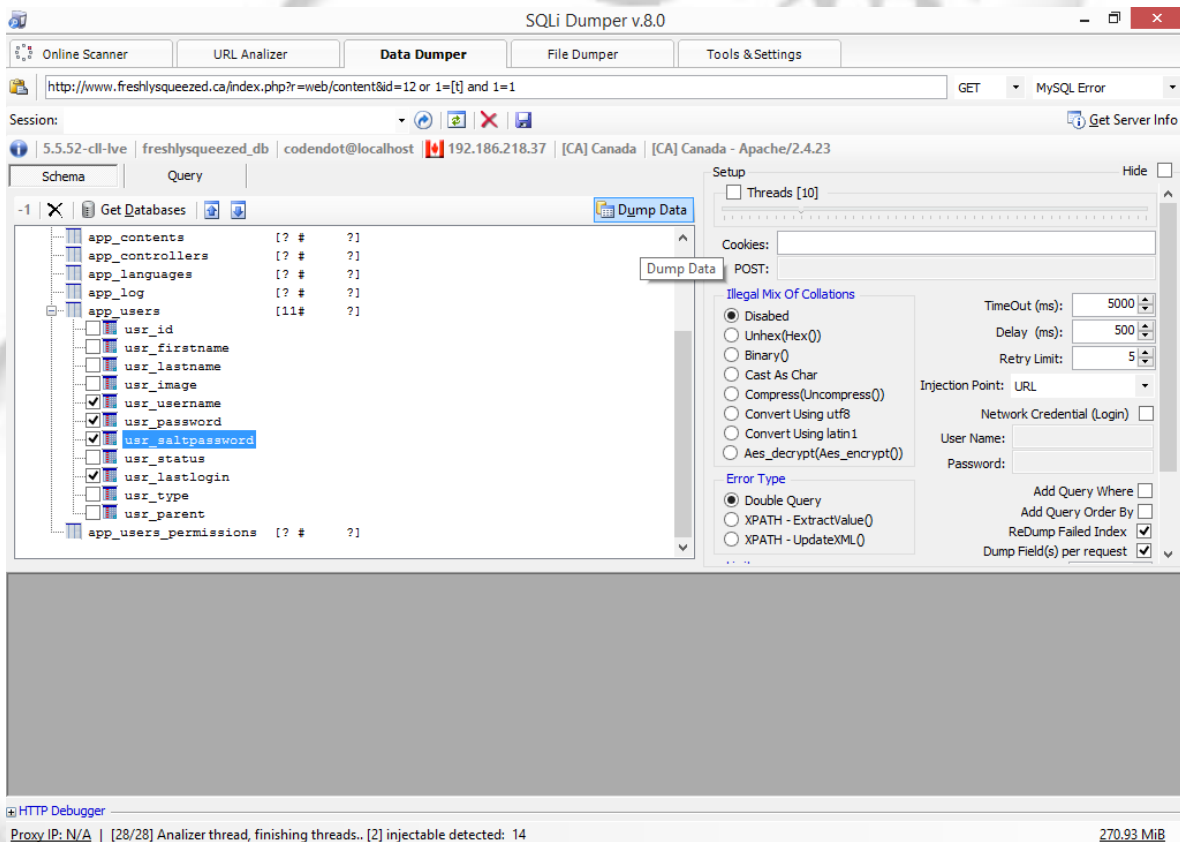
En este caso solo nos interesan los usuarios, los seleccionamos y le damos en “Get columns”



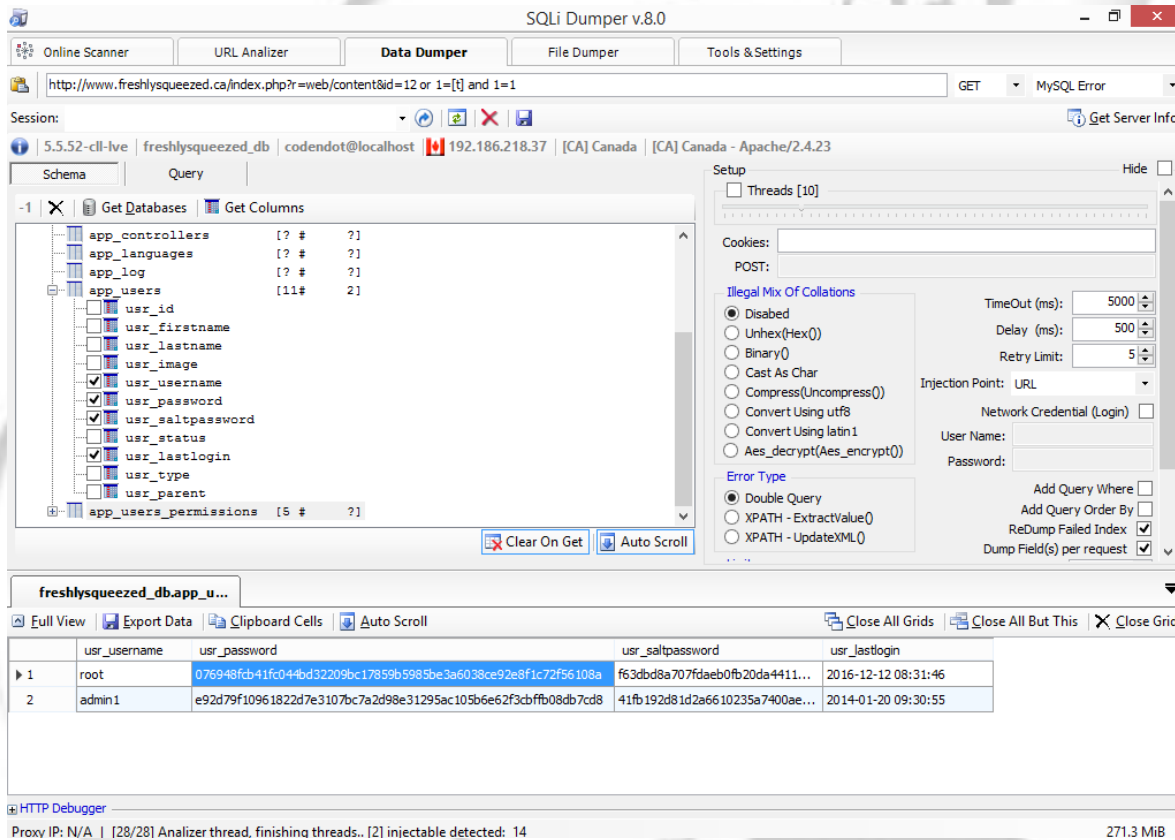
Nos saldrá el desglose de los usuarios así



En este caso seleccionare los username, password, lastlogin, saltpassword, ya seleccionados le damos en “Dump Data”



En este caso salieron users pero no preocupes ya que aún quedan muchas más por ver



The screenshot displays the SQLi Dumper v8.0 application window. The main interface shows a list of databases and tables on the left, with the 'app_users' table selected. The right pane shows the dump results for the 'app_users' table, listing columns: 'usr_username', 'usr_password', 'usr_saltpassword', and 'usr_lastlogin'. The dump results are shown in a table with two rows: 'root' and 'admin1'. The 'usr_password' column contains hex-encoded values, and the 'usr_saltpassword' column contains hex-encoded salt values. The 'usr_lastlogin' column shows the last login time for each user.

Session: 5.5.52-cll-lve | freshlysqueezed_db | codendot@localhost | 192.186.218.37 | [CA] Canada | [CA] Canada - Apache/2.4.23

Schema: Query

Get Databases: Get Columns

app_controllers [?] # [?]
app_languages [?] # [?]
app_log [?] # [?]
app_users [11# 2]
app_users_permissions [5 # ?]

usr_id
usr_firstname
usr_lastname
usr_image
usr_username
usr_password
usr_saltpassword
usr_status
usr_lastlogin
usr_type
usr_parent

app_users_permissions [5 # ?]

Clear On Get Auto Scroll

Setup

Threads [10]

Cookies:

POST:

Illegal Mix Of Collations

Disabled
Unhex(Hex())
Binary()
Cast As Char
Compress(Uncompress())
Convert Using utf8
Convert Using latin1
Aes_decrypt(Aes_encrypt())

Error Type

Double Query
XPath - ExtractValue()
XPath - UpdateXML()

TimeOut (ms): 5000
Delay (ms): 500
Retry Limit: 5

Injection Point: URL

Network Credential (Login)

User Name:
Password:

Add Query Where
Add Query Order By
ReDump Failed Index
Dump Field(s) per request

freshlysqueezed_db.app_u...

Full View Export Data Clipboard Cells Auto Scroll

Close All Grids Close All But This Close Grid

	usr_username	usr_password	usr_saltpassword	usr_lastlogin
1	root	076948fcb41fc044bd32209bc17859b5985be3a6038ce92e8f1c72f56108a	f63dbd8a707fdae0fb20da4411...	2016-12-12 08:31:46
2	admin1	e92d79f10961822d7e3107bc7a2d98e31295ac105b6e2f3cbfb08db7cd8	41fb192d81d2a6610235a7400ae...	2014-01-20 09:30:55

HTTP Debugger

Proxy IP: N/A | [28/28] Analyzer thread, finishing threads.. [2] injectable detected: 14

271.3 MiB

Esperamos que este tutorial te haya sido de ayuda

Creditos:

- Mario Alvarado (mayito)
- Mauricio Garcia (ratix)
- Daniel Munguia (3-pat)
- Chrystian Jossue (filtros)

