

## **Telmex. Obtener información a partir del nombre.** **darko ([darko@raza-mexicana.org](mailto:darko@raza-mexicana.org))**

Como muchos ya saben, Paginas Blancas; ahora obtener información a partir del nombre de la persona (siempre y cuando este registrada a su nombre la línea telefónica) no deja de ser muy útil como el pasado *Razagle* que te daba información a partir del numero telefónico, cabe aclarar que este recurso, servicio o como lo quieran ver Telmex lo da gratuito y te limita el numero de búsquedas por día, claro **siempre y cuando** estés registrado a lo que llama **Mi Telmex**.

Han salido a la luz algunas vulnerabilidades, algunas otras reportadas hacia Telmex otras cuantas muchas no XD y creo que debido a eso y a que los desarrolladores altamente calificados no han podido hacer algo realmente útil para el funcionamiento correcto de **Mi Telmex** han cambiado la forma de autenticación, han cambiado la aplicación como tal (antes de recibos telefónicos) y ahora hasta han cambiado la forma de registro si valgame la chingadamadre, parece que no saben hacer las cosas bien, la forma en que han cambiado el registro para hacer uso de la aplicación es que ahora ya no te pide los datos del número de factura para el registro y creo que fue por que se dieron cuenta de que se podía hacer bypass muy fácil, weno la verdad no muy fácil pero al menos se dieron cuenta, lo único bueno de esto es que quizás se generaron mas plazas de empleo a la gente de call center ya que ahora te piden comunicarte con ellos para darte de alta en su aplicación, que raro y que feo no? digo, se supone que la tecnología y los recursos y sobre todo los sueldos de los desarrolladores deberían solucionar eso pero en fin...

Y ya hablando de esto, otra cosa que mejoraron fue el 'limitar tu tiempo' en la aplicación si ésta no detecta algún movimiento, que... por cierto también se puede hacer bypass. Así como también su implementación de autenticación por cookies que la verdad aun, aun dejan mucho que desear, el formato que usan para la autenticación que realmente se usa 1 parámetro a lo mucho 2 y es el numero telefónico, pero se puede jugar en algunos módulos solo con 1 parámetro ya que es el que realmente están autenticando y comprobando, y se puede obtener información aunque no pertenezca la cookie original a la línea esto gracias a su variable `CVE_USR=XXXXXX`, claro así como hay cosas malas (y aun hay mas...) también hay cosas buenas, entre ellas el que **ahora si** comprueban que la sesión pertenezca a quien dice ser (haciendo la comprobación cada cierto tiempo mediante un .jsp), cada que desea usar un modulo, si gracias a `mt_actualizaBreadC.jsp` que es quien se encarga de comprobar que seas quien dices ser cada que haces uso de **Mi Telmex** ahora si se merecen un aplauso los desarrolladores... ah, pero **ups** ☹ también se puede bypassear ☺ pero no para todos los módulos así que yo creo si merecen un poquitito de aplausos bravo bravo bravo!!!!

Se ve que tenia ganas de escribir cosas que no tienen nada que ver con el titulo o idea original de este pdf, pero creo que por allí hay gente interesada en encontrar vulnerabilidades en **Mi Telmex** y solo quería mencionar algo de lo que he encontrado, creo que es o fue la mejor forma de mencionar o decir lo poco que conozco.

Y ahora bien después de cosas que les vale madres, vamos a lo del título original, lo siguiente describe la manera de poder buscar datos de una línea telefónica Telmex a partir del nombre de la persona.

Cabe aclarar que a diferencia del servicio anterior *Fonos en Razagle* (buscar datos a partir de número telefónico), este servicio es gratuito y lo proporciona Telmex una vez que te hayas registrado en [www.online.telmex.com](http://www.online.telmex.com) con el nombre de Páginas Blancas, la ventaja de esto es que no necesitaras registrarte para poder hacer uso del servicio, además de que Telmex te limita el numero de búsquedas al día por sesión.

Pues bien, anteriormente había comentado que era necesario estar logueado en [www.online.telmex.com](http://www.online.telmex.com) para poder realizar las búsquedas, después de varias pruebas que he realizado me he dado cuenta que solo con crear la cookie y sin necesidad de colocar valores reales de una sesión pero si manteniendo el formato de la cookie es posible hacer uso del servicio. Las pruebas las he hecho bajo Firefox y con la extensión AnEC Cookie Editor.

La forma es la siguiente:

1. Crear la cookie con los siguientes valores

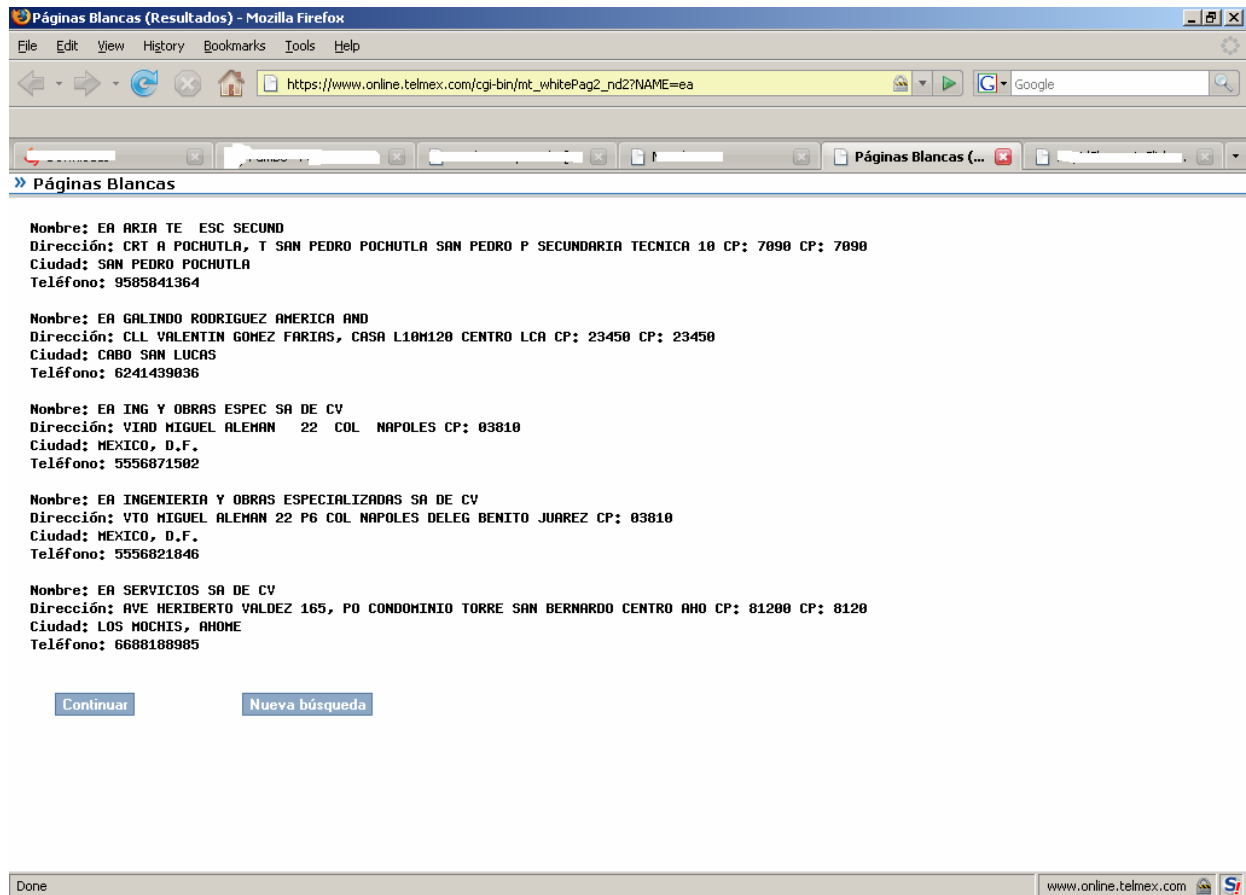
- Name: user
- Content: 0:0:0:0:
- Host: .telmex.com
- Path: /



2. Realizar la búsqueda a partir del nombre con la siguiente url:

· [https://www.online.telmex.com/cgi-bin/mt\\_whitePag2\\_nd2?NAME=ea](https://www.online.telmex.com/cgi-bin/mt_whitePag2_nd2?NAME=ea)

El resultado será la siguiente imagen:



Pues bien, allí esta lo prometido. Ahora solo resta esperar a que los desarrolladores altamente calificados a cargo de **Mi Telmex** solucionen esto.... y otras más que seguro ni piensan que existen o por las que vienen.

Y como siempre... gracias Telmex por hacernos la vida mas fácil.