

Ejemplo práctico de por qué debes encriptar tus comunicaciones

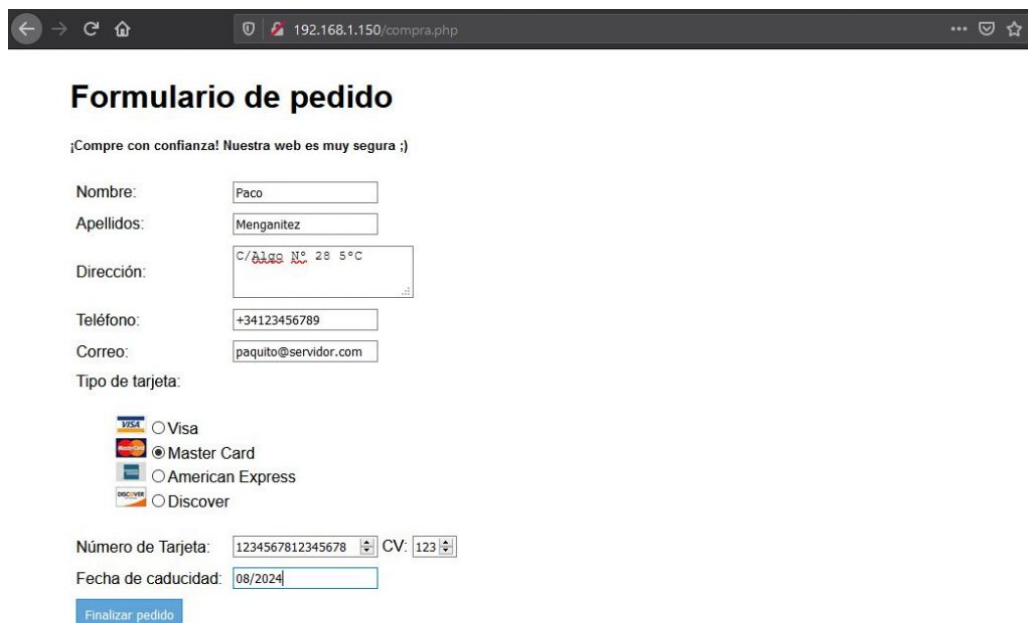
Publicado el [El Informatico](#) - 1 de diciembre de 2020 -

Ya he hablado en [otro artículo](#) sobre algunos de los algoritmos más básicos de encriptación y por qué es importante asegurarse de que las comunicaciones estén debidamente cifradas. En éste artículo voy a hacer una demostración de lo que puede pasar si haces caso omiso a dicho artículo y decides usar internet ignorando las advertencias de seguridad.

¿Vamos de compras?

Comprar en una página que no ofrezca como mínimo un certificado TLS para garantizar al menos que la comunicación está cifrada y que el destinatario es quien dice ser, no es muy buena idea... Pero, ¿Qué es lo peor que puede pasar?

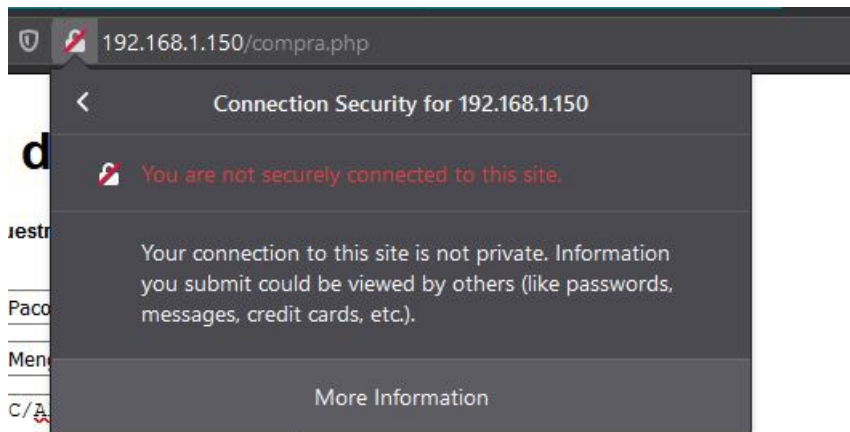
En la siguiente imagen tenemos un formulario típico de compra. Fíjate en el icono del candado con la franja roja en la dirección del navegador. Eso indica que **la página no usa un certificado TLS**.



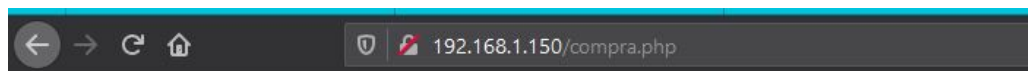
The screenshot shows a web browser window with the address bar displaying "192.168.1.150/compra.php". A red warning bar is visible in the address bar, indicating a security issue. The page title is "Formulario de pedido". The form contains the following fields and options:

- Nombre: Paco
- Apellidos: Menganitez
- Dirección: C/ de la No. 28 5°C
- Teléfono: +34123456789
- Correo: paquito@servidor.com
- Tipo de tarjeta:
 - ☐ Visa
 - ☒ Master Card
 - ☐ American Express
 - ☐ Discover
- Número de Tarjeta: 1234567812345678 CV: 123
- Fecha de caducidad: 08/2024
- Finalizar pedido

Si hacemos click sobre dicho icono, el navegador (en éste caso es Firefox) nos advertirá de que la conexión no es segura y que no debemos introducir ningún dato personal.

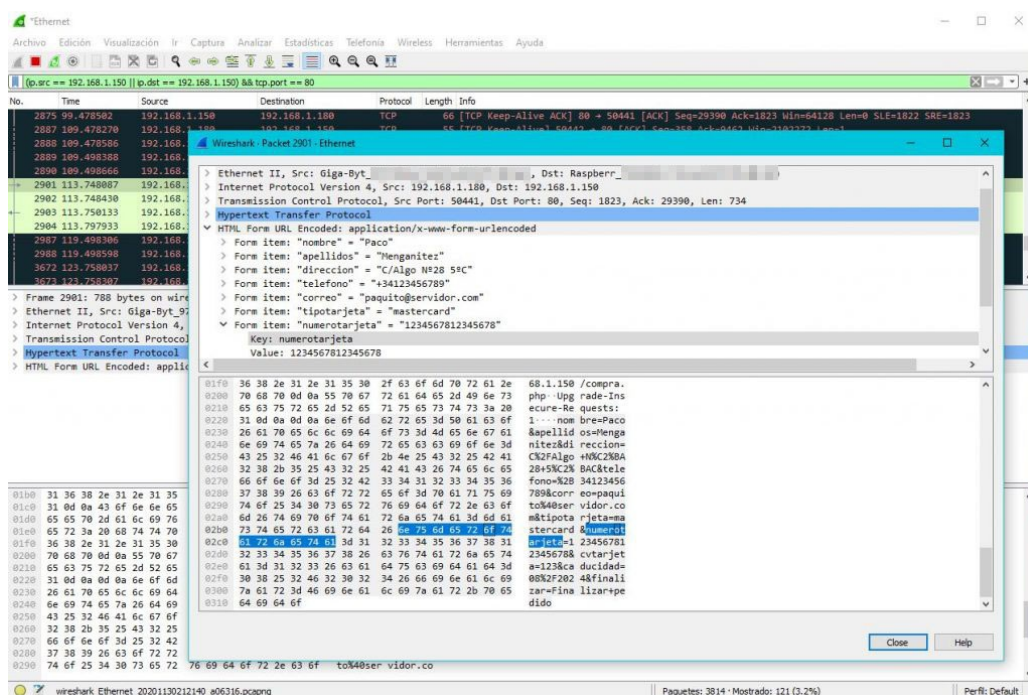


Pero en éste caso, voy a hacer caso omiso a lo que diga Firefox (¡Quién es Mozilla para decirme a mi lo que debo o no hacer!). Si hago click en “Finalizar Pedido”...



Comprueba los paquetes en Wireshark ;)

La página me dice que compruebe los paquetes en Wireshark, una herramienta que sirve para capturar los paquetes de datos que pasan a través de la interfaz de red. Si hago lo que me pide la página, podré descubrir el contenido de los paquetes que se han mandado al servidor en el momento que he hecho click en el botón de finalizar el pedido.



```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "nombre" = "Paco"
> Form item: "apellidos" = "Menganitez"
> Form item: "direccion" = "C/Algo Nº28 5ºC"
> Form item: "telefono" = "+34123456789"
> Form item: "correo" = "paquito@servidor.com"
> Form item: "tipotarjeta" = "mastercard"
> Form item: "numerotarjeta" = "1234567812345678"
> Form item: "cvtarjeta" = "123"
> Form item: "caducidad" = "08/2024"
> Form item: "finalizar" = "Finalizar pedido"
```

Al no estar las comunicaciones cifradas, el mensaje es visible a cualquiera que pueda acceder al contenido de los paquetes que se intercambian el cliente (en éste caso el navegador) y el servidor. Incluso si el dueño de la página fuese de fiar, un tercero podría haberse hecho con la información que se ha mandado al servidor.

Es decir, si ésto hubiese sido un ataque real, el atacante se hubiese hecho con todos mis datos, incluido mi correo, teléfono, y lo que es peor, acceso a mi tarjeta de crédito. Afortunadamente se trata una página de demostración que he colocado en un servidor en mi red local, pero el mensaje es claro: **ten cuidado**. Si te conectas a una página que no utiliza algún tipo de cifrado, alguien podría interceptar tus comunicaciones.

¿Cómo es esto posible?

Cuando hacemos una conexión a un ordenador o equipo remoto, estamos intercambiando paquetes de datos entre ambos ordenadores. Para entenderlo de una manera simple, esos paquetes de datos funcionan de manera similar a como nosotros hacemos logística en la vida real.

Si tú compras algo por internet, ese “algo” debe llegarte en un paquete, que contiene una serie de etiquetas con la trazabilidad del paquete para saber de donde viene y a donde tiene que llegar. El paquete debe de ser transportado por un medio, que puede ser por tierra (carretera), mar, o aire. O incluso una combinación de éstos, y puede pasar por múltiples almacenes hasta llegar a su destino.

De igual forma en una red de comunicaciones, cuando enviamos datos a un equipo, esos datos se encapsulan en **paquetes**. Esos paquetes llevan información sobre su origen y destino, y por cada punto que pasan en la red, se añade una capa de información extra. Esos paquetes viajan por un medio, que en éste caso es nuestra red, hasta llegar a su destino.

Si en el ejemplo de la logística, alguien lograra interceptar tu paquete, se puede hacer con su contenido y saber lo que contiene. Y de igual forma, en internet, si alguien intercepta tus paquetes de datos, pueden hacerse con su contenido y saber lo que contienen. Esto es posible de diversas maneras. Por ejemplo, controlando

alguno de los equipos de tu red, si tú te conectas a una red a través de un dispositivo bajo el control de un atacante (como un portal cautivo o un proxy), o controlando alguno de los nodos a los que te conectas.

Un ejemplo sería **atacando el router con el que te conectas a internet**. Si un atacante se hace con el control del router no sólo tiene acceso total a tu red interna, sino que además controla todas las comunicaciones de tu casa. Esto no es algo descabellado, existen multitud de routers que tienen algún tipo de vulnerabilidad. Un ejemplo que me llamó la atención fue que alguno de los routers de la marca D-Link, hace ya algunos años, **tenían una puerta trasera que le permitía a cualquier atacante hacerse con el control del mismo**.

De igual modo, **existe una vulnerabilidad en el protocolo UPnP** que, de no ser parcheada en los dispositivos, podría facilitarle a un atacante hacerse con el control del mismo, asumiendo que por alguna razón el servicio UPnP estuviese expuesto a la red de internet (que por lo general no debería de ser el caso).

Comprando con SSL/TLS

Esta vez, voy a realizar la misma compra que realicé al comienzo del artículo, pero ésta vez **he activado un certificado TLS en el servidor web**. De modo que la conexión ahora se realiza con cifrado de datos.

Formulario de pedido

¡Compre con confianza! Nuestra web es muy segura ;)

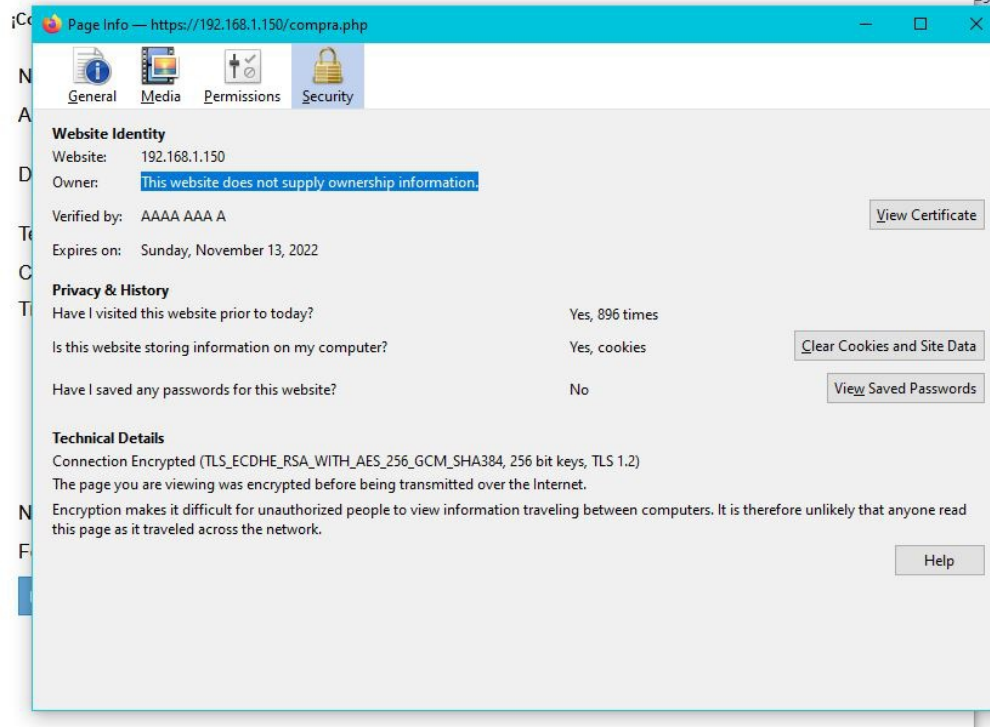
Nombre:	<input type="text" value="Paco"/>
Apellidos:	<input type="text" value="Menganitez"/>
Dirección:	<input type="text" value="C/Algo N°28 5°C"/>
Teléfono:	<input type="text" value="+34123456798"/>
Correo:	<input type="text" value="paquito@servidor.com"/>
Tipo de tarjeta:	

-  ☐ Visa
 ☒ Master Card
 ☐ American Express
 ☐ Discover

Número de Tarjeta:	<input type="text" value="1234567812345678"/>	CV:	<input type="text" value="123"/>
Fecha de caducidad:	<input type="text" value="08/2024"/>		

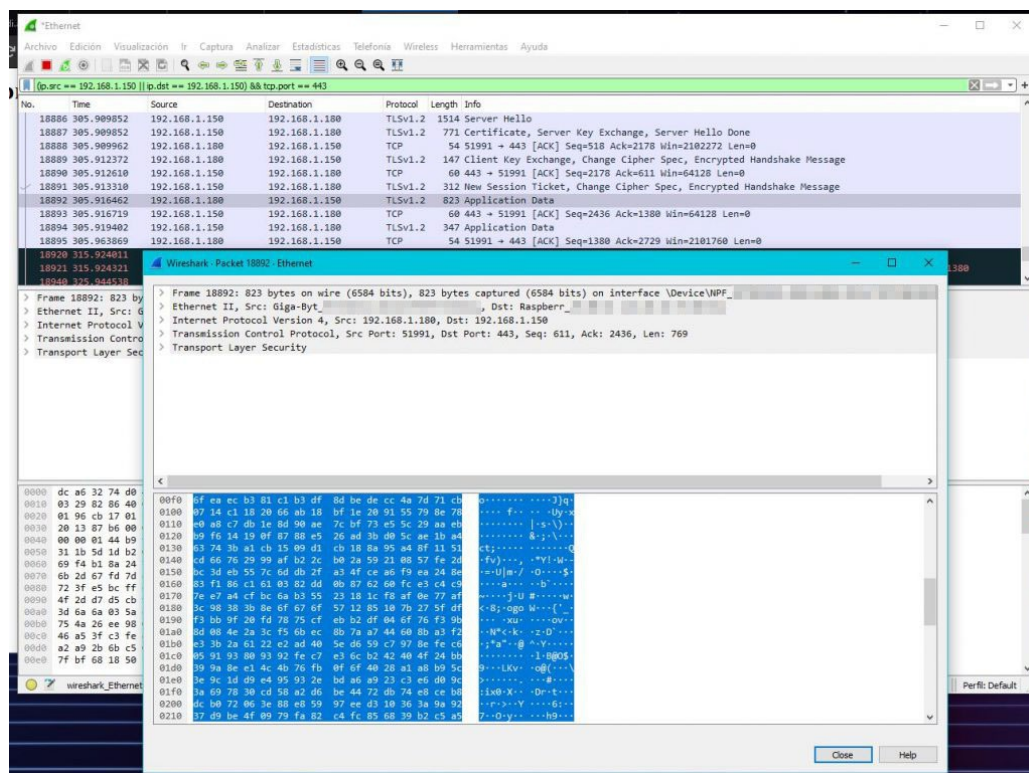
En éste caso, la barra de direcciones aparece con el candado con un símbolo de advertencia amarilla. La conexión sigue siendo insegura, y el motivo es porque estoy usando un **certificado firmado por mí mismo**. De modo que el navegador no puede verificar que el destinatario es quien dice ser. Pero si vemos las propiedades del certificado, vemos que al menos la comunicación si está encriptada.

Formulario de pedido



Al ser un servidor de prueba en mi red local, no estoy usando un dominio y, por tanto, debo usar un certificado no válido. Pero en la práctica, si encuentras una página de éste tipo, tratala siempre como si no usase certificado y no des información personal a menos que estés 110% seguro o segura de que el destinatario es quien dice ser.

En cualquier caso, al finalizar la compra y verificar los paquetes capturados, la cosa cambia con respecto a la primera vez.



En éste caso, gracias a la encriptación de datos mediante el protocolo HTTPS, el

atacante no habría sido capaz de hacerse con los datos del usuario, ya que están encriptados.

En éste caso, he activado en el servidor los protocolos TLS 1.1 y TLS 1.2. Por defecto, si vas a dar datos bancarios, deberías usar TLS 1.2 o TLS 1.3. **NUNCA TLS 1.0 o 1.1, ya que son vulnerables.** Así mismo, el algoritmo de cifrado **no debe usar en ningún caso algoritmos como MD5 para la generación de contraseñas.** AES y SHA son siempre las mejores opciones.

Excepciones

La única excepción a la hora de usar certificados TLS (o SSL) es **a la hora de acceder a los servicios ocultos de tor.** Es un poco “anti-intuitivo” el pensar que no debes preocuparte por la encriptación a la hora de conectarte a un servicio oculto, pero recuerda que la propia red de TOR ya encapsula y encripta, punto a punto, toda la conexión. Tener un certificado válido podría desenmascararte a ti y al servicio a la hora de realizar la verificación del certificado, y no tiene sentido usar uno sin firma válida si ya está encriptada la conexión.

No obstante, si usas TOR para conectarte a la web normal, **sí es obligatorio conectarte a páginas exclusivamente por HTTPS con certificado TLS.** De no hacerlo, la conexión entre el servidor y el nodo de salida no estará encriptada, lo cuál es inseguro. Para garantizar que la conexión se realiza con TLS, existen plugins para el navegador como **HTTPS Everywhere**, que forzarán que la conexión sea mediante HTTPS, y la cortará si ésto no fuese posible.



ANTERIOR

2021: Por qué es más importante que nunca entender la tecnología (Y aprender a usarla)

SIGUIENTE

Chatbots en Python 3.x

Buscar ...



Entradas Recientes

- [Encriptación LUKS con CRYPTSETUP](#)
- [Se acabaron las bromas. A partir de ahora vas a estar constantemente vigilado en todas partes.](#)
- [Microsoft anuncia su nueva versión de su sistema operativo: Windows 11](#)
- [La historia de Internet en España](#)
- [Terminología moderna usada en tecnología digital](#)
- [Desactiva la ejecución de JavaScript de los archivos PDF, en Firefox y TOR browser.](#)

Categorías

[Actualidad](#)[Android](#)[Básicos](#)[Ciberseguridad](#)[Criptografía](#)[Emulación / Virtualización](#)[FOSS](#)[Hacking](#)[Informática](#)[Internet](#)[Juegos](#)[Opinion](#)[Otros](#)[Personal](#)[Privacidad](#)[Programación](#)[Tecnología](#)[Time Machine](#)[Tutoriales](#)

RSS

[Subscribirse al feed RSS](#)

[Inicio](#)[Catálogo](#)[Tutoriales](#)[Política de privacidad](#)[Política de Cookies](#)[Acerca de mi](#)[Acerca de ElInformati.co](#)