Web technologies

How Https Works

- Read the following Link.
- If you want to know more you can watch the following video.

Exercises

1. Translate to English the following terms

    a) Navegador de Internet Browser

    b) candado padlock

    c) Firma digital digital signature

    d) clave pública the public key

    e) clave privada the private key

    f) Encriptación encryption

    g) Cifrado encryption

    h) Confianza successful

    i) cadena chain

    j) certificado auto firmado self-signed certificates

2. Translate to Spanish the following terms

    a) Avocado

    b) Recipe receta

    c) Crab cangrejo

    d) eavesdrop escuchar a escondidas

    e) man-in-the-middle attack ataque en el medio

    f) tampered with manipulado / cambiado por

    g) stay tuned mantenganse al tanto

    h) handsake el apreton de manos

    i) Let’s recap recapitulemos

    j) third-party organization organizacion de terceros

    k) root raíz

    l) flavors sabores

3. Write to opposite to

    a) encryption algorithm.

    b) Cryptographic simmetric.

4. Go to https://howhttps.works/quiz/ and find out the following in your Web Browser

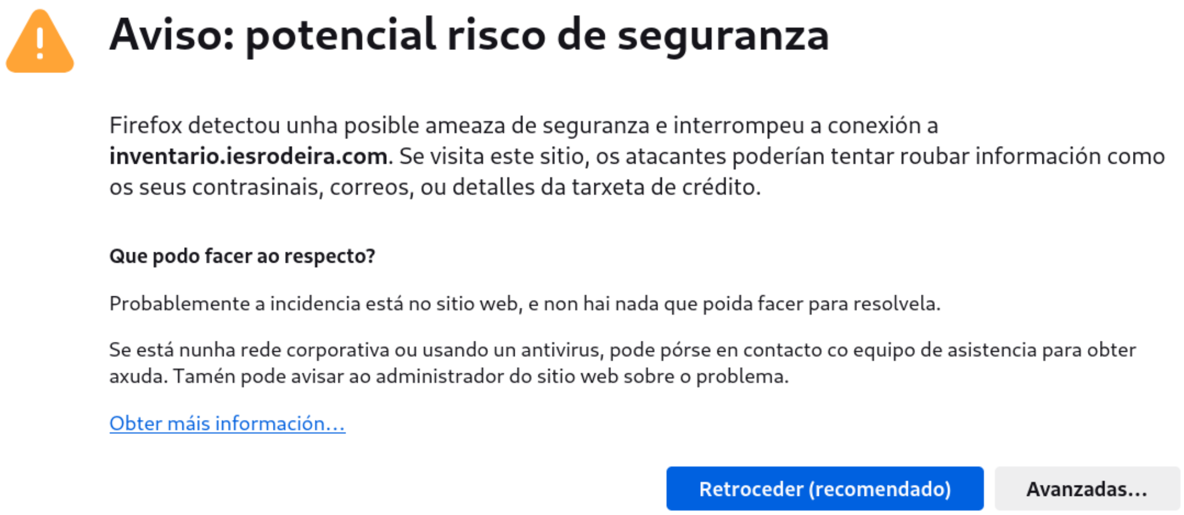
   a) How are you sure that uses https? see if there is a padlock on the URL bar of my browser.

   b) Find out the web page certificate and the encrypt algorithm used.

      the web page certificate: howhttps.works
      the encrypt algorithm: SHA-256

5. Go to https://inventario.iesrodeira.com/

   a) What's the problem? because of the last certificate is not a root certificate, so the chain is untrusted



Aviso: potencial risco de seguranza

Firefox detectou unha posible ameaza de seguranza e interrompeu a conexión a **inventario.iesrodeira.com**. Se visita este sitio, os atacantes poderían tentar roubar información como os seus contrasinais, correos, ou detalles da tarxeta de crédito.

Que podo facer ao respecto?

Probablemente a incidencia está no sitio web, e non hai nada que poida facer para resolvela.

Se está nunha rede corporativa ou usando un antivirus, pode pórse en contacto co equipo de asistencia para obter axuda. Tamén pode avisar ao administrador do sitio web sobre o problema.

Obter máis información…

   b) How would you solve it? buy a valid certificate for my website

   c) Find out the prize of buying a valid certificate for your web page

      for example: Certera SSL 3,99$/year

6. Answer the following questions.

a) Can someone spy on your data if your connection is not secured?

[✓ a.1. Yes]

a.2. No

b) Why do we need HTTPS?

b.1. For privacy and identification

b.2. For faster websites

[✓ b.3. For privacy, integrity, and identification]

b.4. For identification only

c) In the context of HTTPS, what does integrity mean?

c.1. That my browser has ethics

[✓ c.2. That communication is not being tampered with]

c.3. That the website I am visiting is honest

c.4. That the internet is strong and durable

d) How many keys are necessary in the symmetric key algorithm?

d.1. Two. One public and one private

[✓ d.2. One]

d.3. Zero.

e) Should you keep your public key private and hidden from everyone?

e.1. Yes

[✓ e.2. No]

e.3. Not telling you. It's private.

f) When speaking about HTTPS, what's a handshake?

f.1. A ritual when we all shake hands

f.2. A process to ensure private communication between a browser and a server

f.3. A gang sign. Don't go into that neighborhood

g) Is SSL 3.0 deprecated?

g.1. Of course yes

g.2. Of course no

h) Who maintains and improves the TLS protocol?

h.1. Netscape

h.2. Microsoft

h.3. IETF (Internet Engineering Task Force)

h.4. Apple

i) When is it OK to self-sign SSL certificates?

i.1. For internal testing sites

i.2. For public web sites

j) What does SSL/TLS stand for in the context of HTTPS?

j.1. Secure Socket Layer / Transport Layer Security.

j.2. Server Side Language / Transmission Line System.

j.3. Secure System Login / Transfer Log Service.

j.4. Static Site Layout / Telecommunication Link Setup.

k) Which component is responsible for encrypting data in HTTPS communication?

k.1. Browser settings.

k.2. Digital certificates.

k.3. SSL/TLS protocols.

k.4. Internet Service Provider (ISP).

l) Why is it important to avoid websites that do not use HTTPS?

l.1. They load slower than HTTPS sites.

l.2. They may not display images properly.

l.3. Data transmitted can be intercepted and read by attackers.

l.4. They cannot be accessed on mobile devices.