# SSL

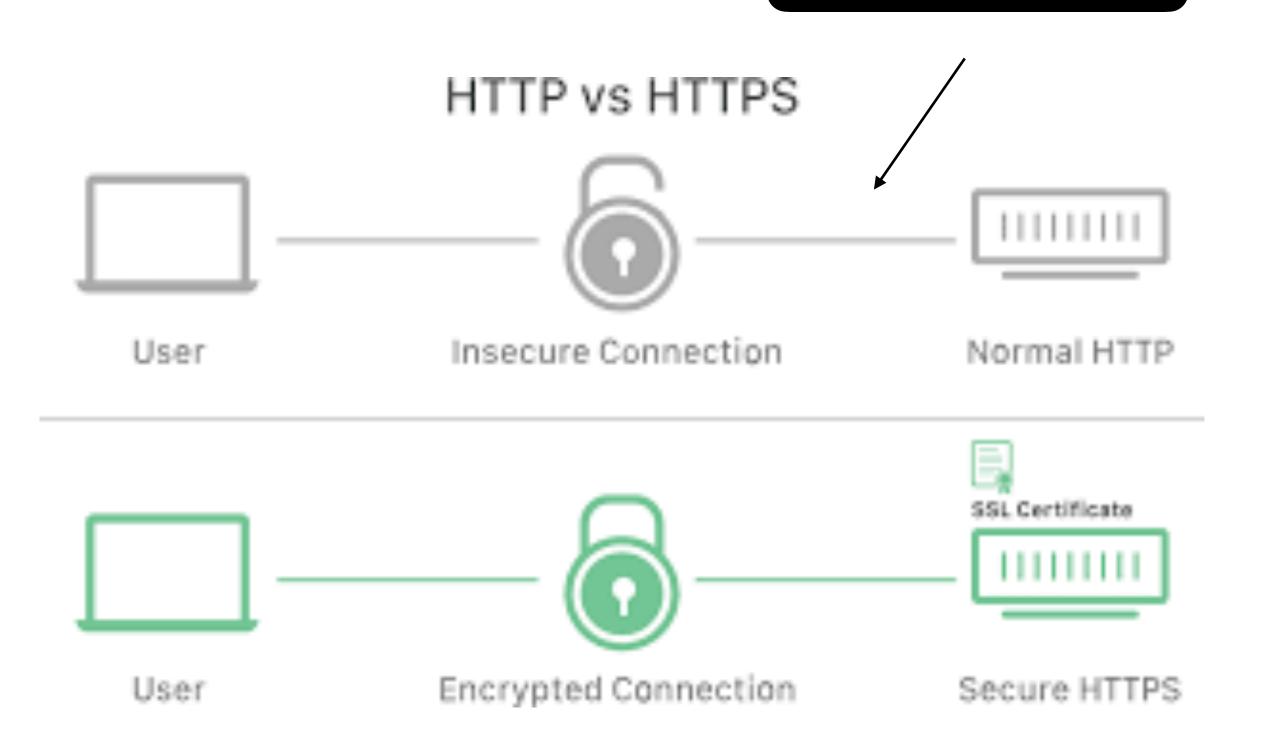
Clase



8 https://

Sin SSL Con SSL

# Robo de información



#### Como funciona



Client messages server to initiate SSL/TLS communication











Server sends back an encrypted public key/certificate. Client checks the certificate, creates and sends an encrypted key back to the server (If the certificate is not ok, the communication fails)



Server decrypts the key and delivers encrypted content with key to the client



Client decrypts the content completing the SSL/TLS handshake

## SSL

#### **Auto Generado**

Se generan por el servidor sin la autorización de una empresa certificadora.

Ventajas: Sin costo

Desventaja:



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de (por ejemplo, contraseñas, mensajes o tarjetas de crédito). <u>Más información</u>

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

Ayuda a mejorar la Navegación Segura enviando <u>datos del sistema y contenido de las páginas</u> a Google. <u>Política de Privacidad</u>

## SSL

#### Por empresa certificador

Se generan en el portal de una empresa certificadora, se descargan y se instalan en el servidor.

Ventajas: No requiere de autorización por parte del usuario.

Desventaja: Costo anual.

# SSL Let's Encrypt

Let's Encrypt es una autoridad de certificación gratuita, automatizada, y abierta traida a ustedes por la organización sin ánimos de lucro Internet Security Research Group (ISRG).

Ventajas: No requiere de autorización por parte del usuario. Sin costo

Desventaja: Se renueva cada tres meses.

# NGINX/DJANGO/CERBOT

Reverse Proxy & SSL

Instancia EC2 SSL claseweb2.pikit.mx Puerto Puerto interno 8000 público 80 y 443 android Users Request's

3.134.106.77

Conexión pública segura