

## Actividades

1. Para esta actividad, es importante que en el vídeo mostréis la conexión HTTPS y que cuando hacéis la petición a HTTP os redirija a HTTPS.

DEAW reverse proxy [Corriendo] - Oracle VirtualBox

Oct 29 1:48 PM

elshin\_vadim@vbox: /etc/apache2/ssl

GNU nano 8.4 /etc/nginx/sites-enabled/test-ssl.conf

```
server{
    listen 8080 default_server;
    server_name www.myexamplevadim.com;
    return 301 https://10.100.0.106$request_uri;
}

server{
    listen 443 ssl;
    server_name www.myexamplevadim.com;

    ssl_certificate /etc/nginx/ssl/server.crt;
    ssl_certificate_key /etc/nginx/ssl/server.key;
    ssl_protocols TLSv1.3;

#    ssl_ciphers ECDH+AESGCM:DH+AESGCM:E

    access_log /var/log/nginx/https_access.log;

    location / {
        root /var/www/html/example.com;
        index index.html;
    }
}
```

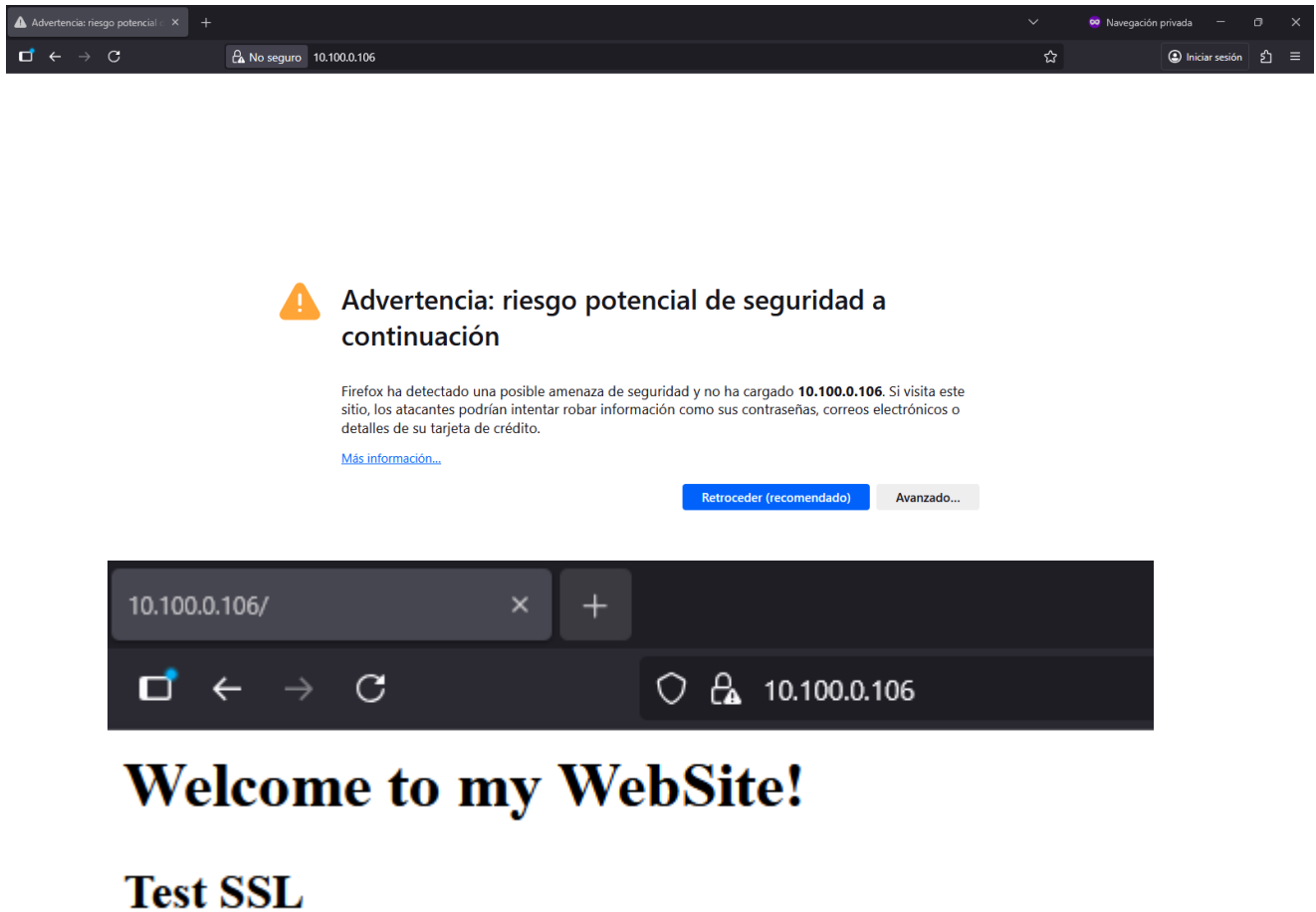
[ Read 24 lines ]

^G Help    ^O Write Out    ^F Where Is    ^K Cut    ^T Execute    ^C Location  
 ^X Exit    ^R Read File    ^\ Replace    ^U Paste    ^J Justify    ^\_ Go To Line

2. Hemos configurado nuestro proxy inverso con todo lo que nos hace falta pero no nos funciona y da un error del tipo This site can't provide a secure connection, ERR\_SSL\_PROTOCOL\_ERROR

The image displays two side-by-side browser windows. The left window shows a security warning from the address 10.100.0.106, indicating that the certificate is self-signed and not trusted. It offers a 'Retroceder (recomendado)' (Go back) button and a 'Ver certificado' (View certificate) link. The right window shows the details of a certificate issued to 'Vadim'. The certificate information includes the subject (Nombre del asunto) and issuer (Nombre del emisor) details, such as country (ES), state (Alicante), and organization (IES Doctor Balmis). It also shows the validity period (Validade) from October 2025 to October 2026 and the public key information (Información de clave pública).

3. Imaginad que intentamos acceder a nuestro sitio web HTTPS y nos encontramos con el siguiente error:



Investiga qué está pasando y cómo se debe solucionar

Para que un certificado SSL sea válido, los dominios deben obtenerlo (previo pago) de una autoridad certificadora (CA). Una CA es una organización externa, un tercero de confianza, que genera y emite certificados SSL. La CA también firma digitalmente el certificado con su propia clave privada, lo que permite a los dispositivos cliente verificarlo.