# Module 3: Troubleshooting and Managing SSL

### 1. Common SSL Issues

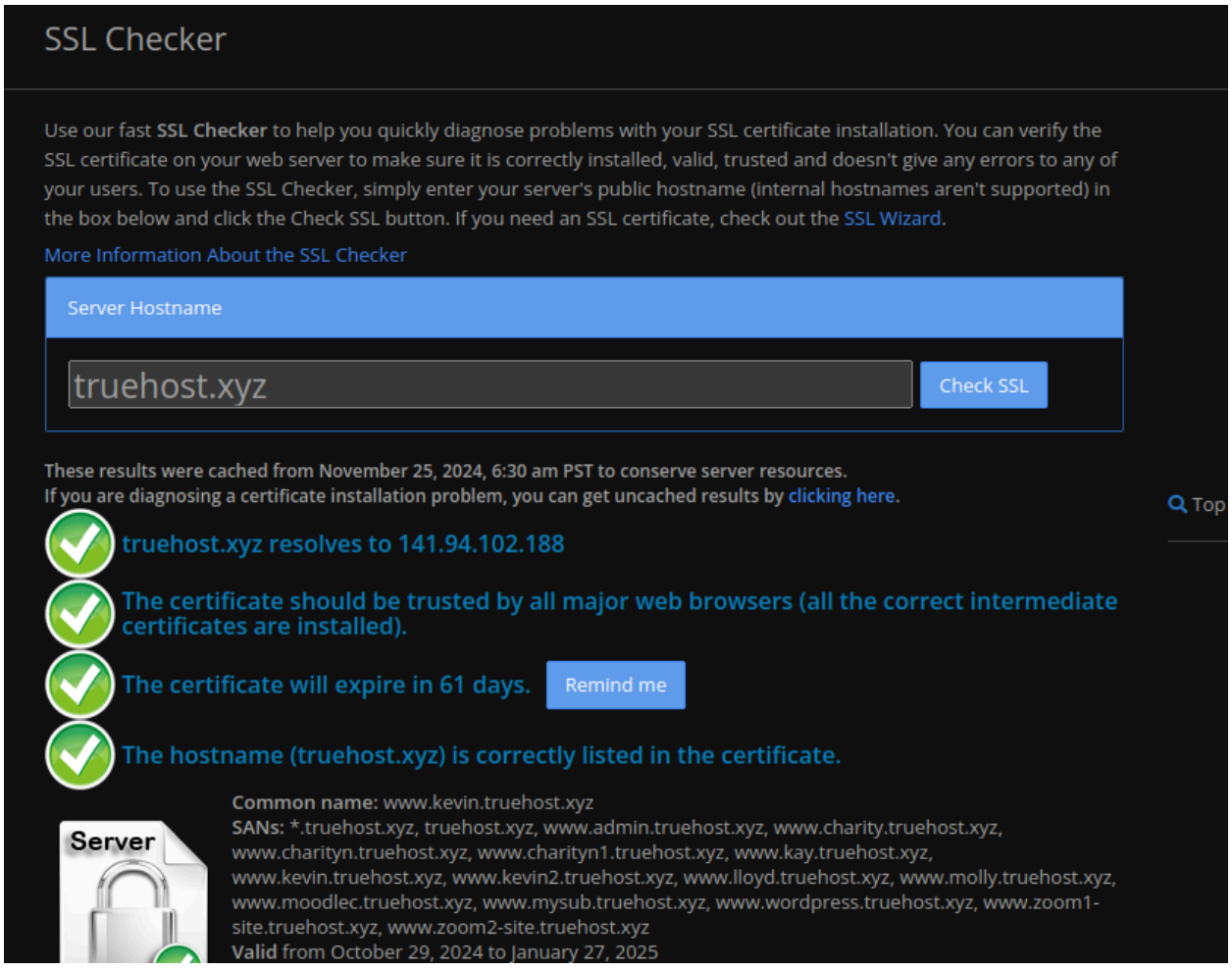
- **Mixed Content Errors:**
  - Occurs when some resources on a page (e.g., images, CSS, or JavaScript) are served over HTTP while the page itself is served over HTTPS.
  - **Solution:**
    - Update URLs in the code or database to use HTTPS.
    - Use browser developer tools to identify non-secure elements.
- **Certificate Chain Issues:**
  - Incomplete or incorrect certificate chain causes browsers to distrust the website.
  - **Solution:**
    - Ensure the intermediate certificates are correctly installed.
    - Use tools like SSL Checker to verify the chain.
    - https://www.sslshopper.com/ssl-checker.html
    -
- **Expired Certificates:**
  - Certificates not renewed before expiry result in browser warnings and site inaccessibility.
  - **Solution:**
    - Regularly monitor expiration dates and enable automated renewal for Free SSL where possible.
    - For Paid SSL, ensure the SSL has been re-issued manually.
- **Browser Warnings:**
  - Can result from incorrect certificate installation, domain mismatch, or outdated browser settings.
  - **Solution:**
    - Verify certificate installation and domain coverage.
    - Encourage users to update their browsers.

---

## 2. SSL Diagnostics

- **Checking Validity and Expiration:**
  - Tools:
    - SSL Checker: Verifies certificate installation, chain validity, and expiration date.
    - Browser security panels (e.g., Chrome DevTools).
  - Regular checks to avoid service interruptions.

Sample:




- **Debugging SSL Configurations:**

- **CSR Decoder:**
  - CSR Decoder: Validates Certificate Signing Requests (CSR) and ensures correct details.
- **Certificate Decoder.**

  **https://www.sslshopper.com/certificate-decoder.html**

- **Command-line Tools:**
  - OpenSSL: Validate and debug certificates

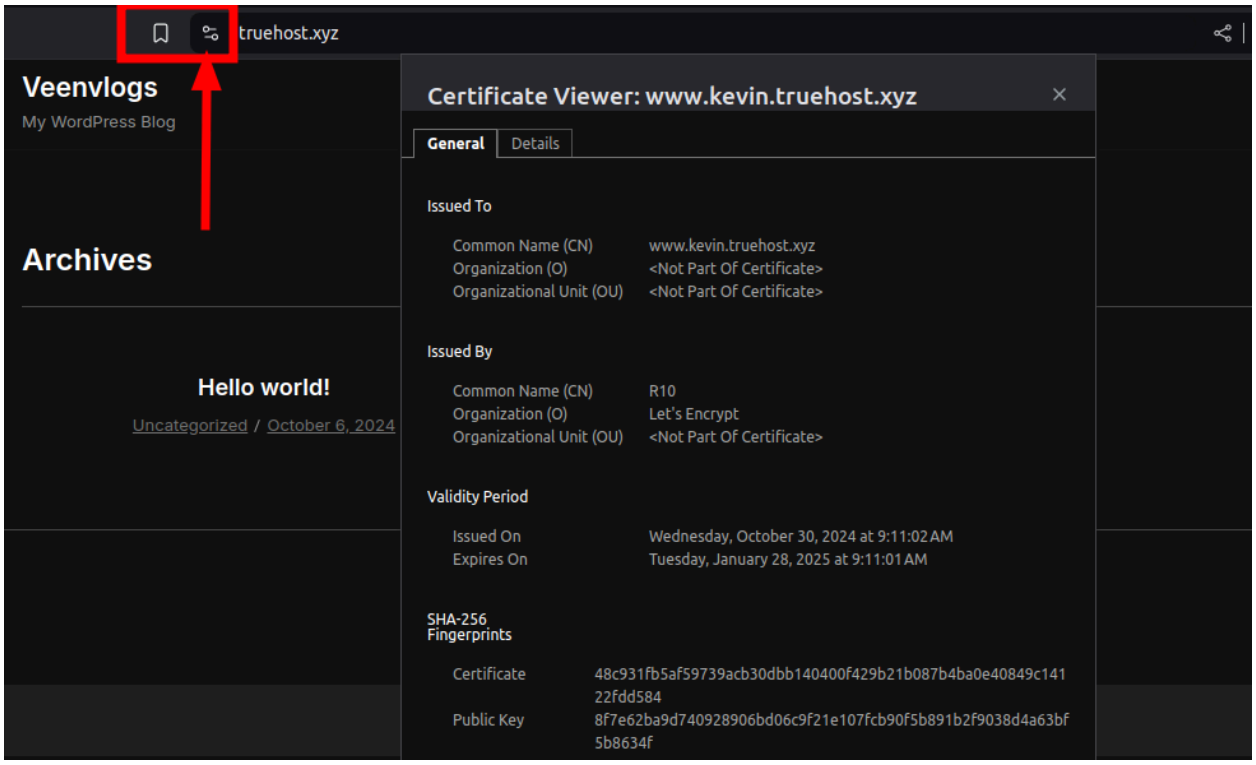
    **`openssl s_client -connect domain.com:443`**

```
dann@homelab:~$ openssl s_client -connect truehost.xyz:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R10
verify return:1
depth=0 CN = www.kevin.truehost.xyz
verify return:1
---
Certificate chain
 0 s:CN = www.kevin.truehost.xyz
   i:C = US, O = Let's Encrypt, CN = R10
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Oct 30 06:11:02 2024 GMT; NotAfter: Jan 28 06:11:01 2025 GMT
 1 s:C = US, O = Let's Encrypt, CN = R10
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
---
Server certificate
```

```
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 3436 bytes and written 394 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
```

- **Browser Tools:**

- Use browser developer tools to inspect certificate details and error logs.




---

### 3. Migrating SSL Certificates

- **Exporting and Importing Certificates:**
  - **Converting Certificates:**
    - Convert formats if needed (e.g., .pem to .pfx for IIS).
- **Re-Keying SSL Certificates:**
  - Required when the private key is compromised or needs to be updated.
  - **Steps:**
    - Generate a new CSR on the server.
    - Reissue the certificate through the certificate authority.
    - Install the reissued certificate on the server.
- **Managing Domain Migrations with SSL:**
  - **Steps:**

- Backup the existing SSL certificate and private key.
- Update DNS records to point to the new server.
- Reinstall the certificate on the new server.
- Test the SSL configuration post-migration to ensure proper functionality.
- Migration scripts usually assist to restore SSL certificates from backups generated.

---