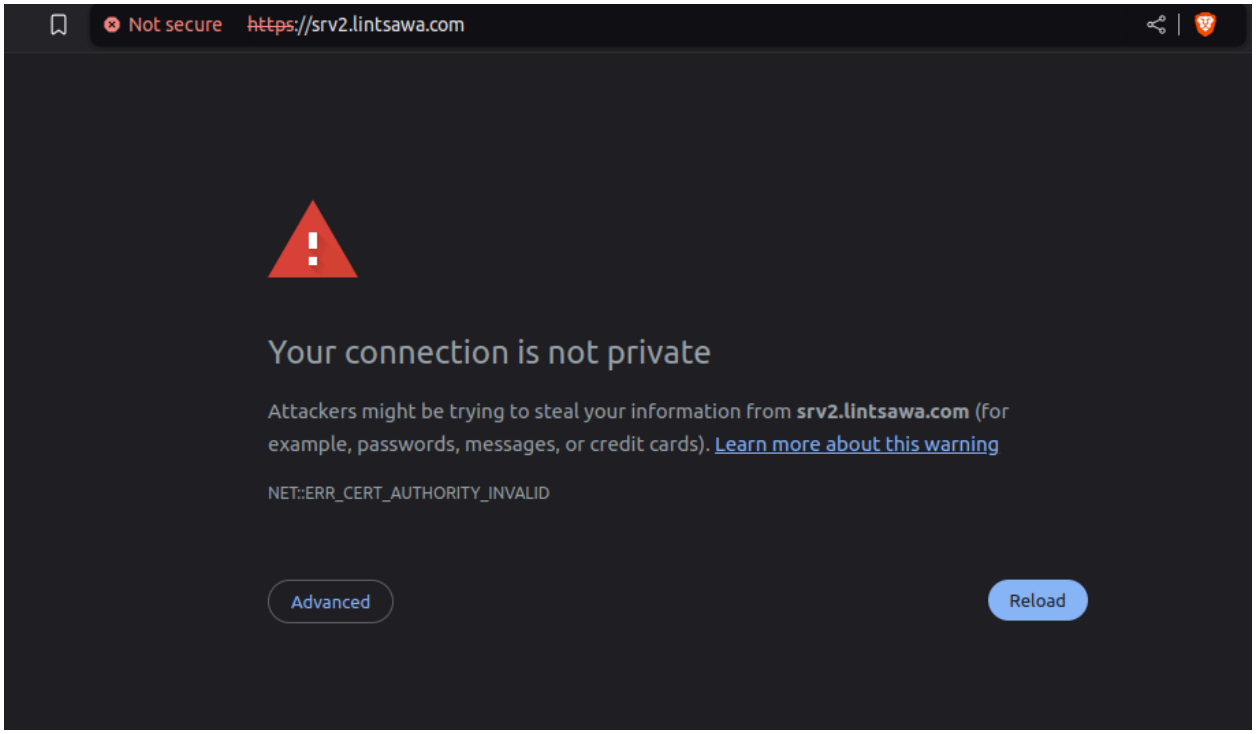
Module 1: Understanding SSL Fundamentals

1. What is SSL?

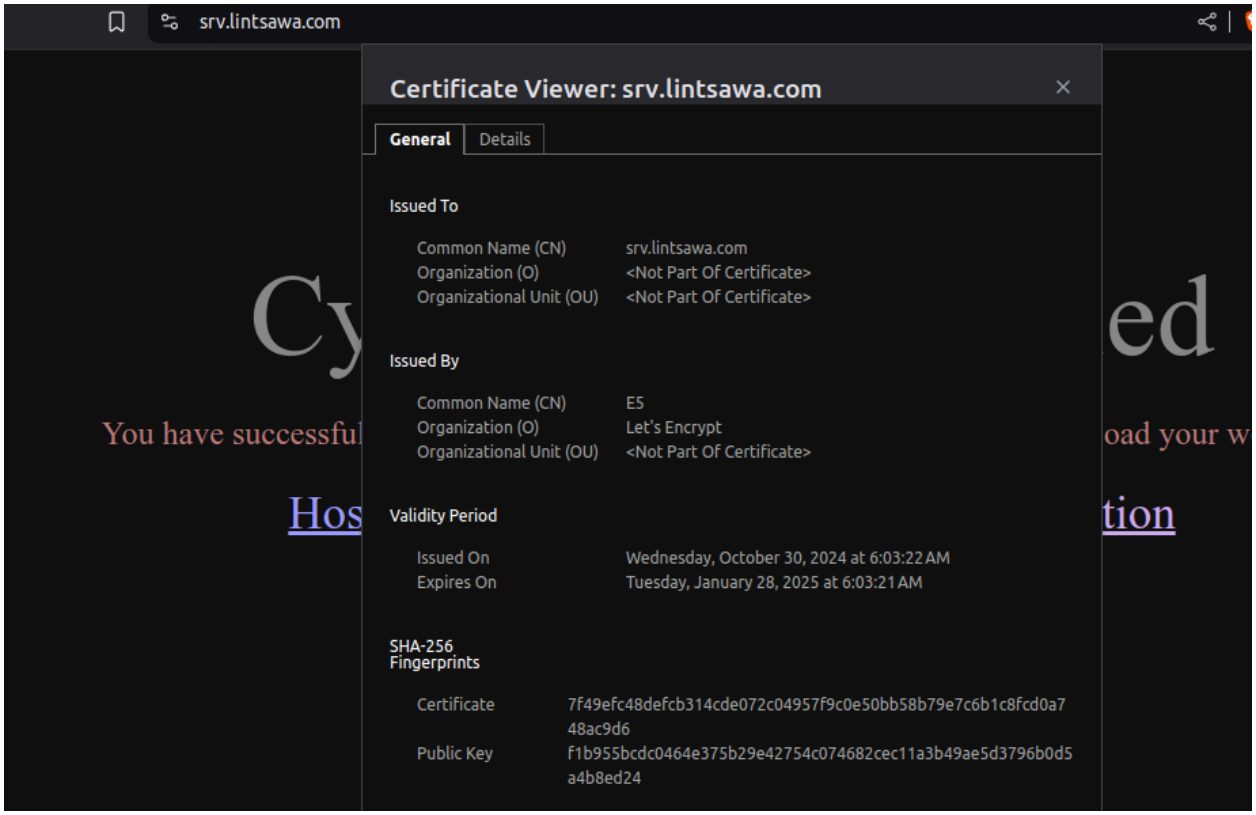
- **Definition and Importance:**
  Secure Sockets Layer (SSL) is a technology used to establish an encrypted link/connection between a web server and a browser, ensuring that data passed between them remains private and secure.
- **How SSL Works:**
  - Encryption: Protects data by converting it into a secure format.
  - Authentication: Verifies the identity of the website.
  - Data Integrity: Ensures transmitted data is not tampered with during transit.
- **Evolution from HTTP to HTTPS:**
  - HTTP is unencrypted, making data vulnerable.
  - HTTPS adds a secure layer through SSL/TLS, making websites safer and more trustworthy.

Example of Non Secure Site and Secure Site.

Non Secure


Not secure
https://srv2.lintsawa.com
Your connection is not private
Attackers might be trying to steal your information from srv2.lintsawa.com (for example, passwords, messages, or credit cards). Learn more about this warning
NET::ERR_CERT_AUTHORITY_INVALID
Advanced
Reload

Secure.


srv.lintsawa.com
Certificate Viewer: srv.lintsawa.com
General
Details
Issued To
Common Name (CN) srv.lintsawa.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) E5
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Wednesday, October 30, 2024 at 6:03:22 AM
Expires On Tuesday, January 28, 2025 at 6:03:21 AM
SHA-256 Fingerprints
Certificate 7f49efc48defcb314cde072c04957f9c0e50bb58b79e7c6b1c8fcd0a748ac9d6
Public Key f1b955bcdc0464e375b29e42754c074682cec11a3b49ae5d3796b0d5a4b8ed24

---

2. Why is SSL Critical?

- **Benefits:**
  - **Security:** Encrypts sensitive information, protecting it from interception.
  - **Trust:** Provides visual cues like the padlock icon, boosting customer confidence.
  - **SEO:** HTTPS is a ranking factor in Google, helping websites rank higher.
- **Compliance:**
  - SSL helps meet regulatory requirements like GDPR, PCI DSS, and others by ensuring secure data handling.
  - PCI DSS - https://www.pcisecuritystandards.org/standards/
  - GDPR - https://gdpr-info.eu/issues/personal-data/

---

3. Types of SSL Certificates

- **Free SSL (e.g., Let's Encrypt):**
  - Cost-effective but may have limitations like shorter validity periods or reduced features.
  - At Truehost, all our shared hosting servers come with Free SSL(s) provided by Let's Encrypt.
  - The validity period for this SSL is 90 days and is automatically renewed on the server.
  - For this SSL to work, the domain or subdomains in question must be pointed to Truehost Default Nameservers for both the cPanel Shared Hosting Environments and the Windows Shared Hosting Environments.

- **Paid SSL Certificates:**
  - **Based on Validation Level:**

- **Domain Validation (DV):** Verifies domain ownership. Ideal for personal websites or small businesses.

  Benefits of DV SSL:

  - Validates control of a domain
  - Enables https and the padlock icon in browsers
  - Issued within minutes

  Use cases

  Since the legitimacy of the organization is not vetted, DV SSL certificates work best on websites that don't collect any personal data or credit card transactions.

  Common use cases are blogs and personal websites. They can also be ideal for internal sites, test servers, and test domains.

- **Organization Validation (OV):** Verifies domain ownership and organization identity. Suitable for medium-sized businesses.

  Details including organization name, phone number, and location will be verified during this step.

  Benefits of OV SSL:

  - Validates control of the domain
  - Enables https and the padlock image
  - Authenticates the legitimacy of an organization, adding a level of trust
  - Shows organization details in the certificate information

  Issued in 1-3 days after all required documents are received

  Use cases

Since OV SSL certificates can only be issued to a registered organization and not individuals, this makes them more suitable for commercial and public-facing websites, though still not ideal for websites that collect any type of sensitive information.

- **Extended Validation (EV):** Provides the highest level of validation, displaying the organization's name in the address bar. Best for e-commerce and financial sites.

  To receive one, website owners must meet the authentication requirements for an OV SSL but also go through a stricter vetting process performed by a human specialist.

  Benefits of EV SSL:

  - Validates control of the domain
  - Enables https and the padlock image
  - Authenticates the legitimacy of an organization, adding an additional level of trust
  - Verifies the applicant has the right to request an EV SSL and is in good standing with the organization
  - Shows organization details in the certificate information

  Issued in 1-5 days after all required documents are received

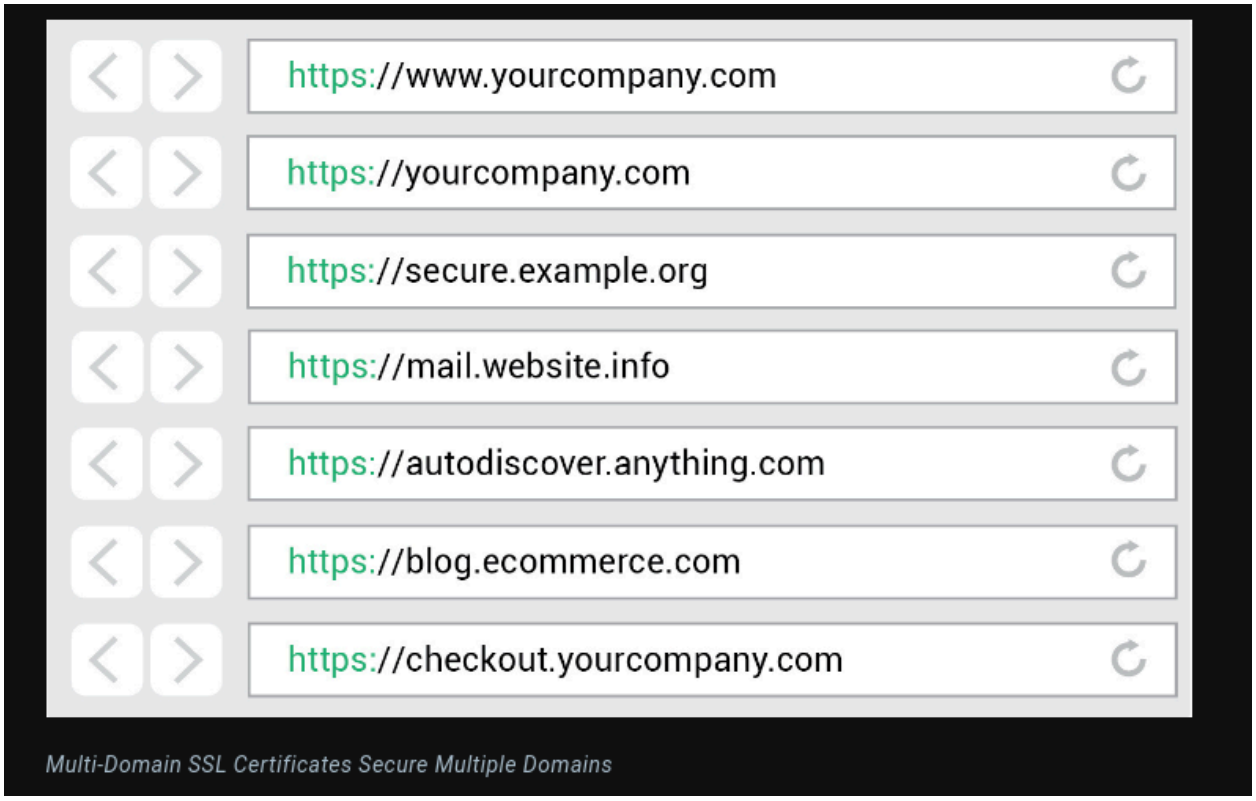
  Use cases

  EV SSL certificates are recommended for all business and enterprise websites but are especially important for

any site that requests personal information from users (eCommerce, financial, legal and otherwise).

- **Based on Certificate Variations:**
  - **Single Domain SSL:** Secures one domain. Examples for Truehost
    - Ask Starter SSL - One domain Only.
    - Sectigo SSL - One domain Only

  - **Multi-Domain SSL (MD/SAN):** Secures multiple domains under one certificate. Example
    - Ask Starter Multi Domain SSL - Covers 3 main domains - 1 main and 2 additional SANS. For additional domains, the client will pay.
    - Sectigo Multi Domain SSL - Covers 3 main domains - 1 main and 2 additional SANS. For additional domains, the client will pay.
    - Subdomains are not included in this SSL. However, if the subdomain in question is the main domain, then SSL can be issued.



- **Wildcard SSL:** Secures a single domain and its unlimited subdomains. Example
  - Ask Starter Wildcard SSL- Covers 1 main domain and it's sub-domains
  - Sectigo Wildcard SSL - Covers 1 main domain and it's subdomains

- **Wildcard Multi-Domain SSL:** Combines Multi-Domain and Wildcard features to secure multiple domains and their subdomains. Example
  - Ask Starter Wildcard Multi Domain SSL. - Covers 3 Main Domains and their Sub-domains.
  - Sectigo Wildcard Multi Domain SSL - Covers 3 Main Domains and their Sub-domains.

---

4. Choosing the Right SSL

- **Matching SSL Types to Use Cases:**
  - Personal blogs or small businesses: Free SSL or DV SSL.
  - Corporate websites: OV SSL for added identity verification.
  - E-commerce platforms: EV SSL for maximum trust.
  - Managing multiple sites: Multi-Domain or Wildcard SSL.
- **Balancing Cost and Security Needs:**
  - Evaluate the value of the data being protected versus the cost of the SSL.

- Consider the long-term benefits of Paid SSL for critical applications.