Module 8: SSL Certificates

8.1 Importance of SSL in Website Security

SSL (Secure Sockets Layer) is crucial for ensuring that data transmitted between your website and its visitors is encrypted and secure. SSL certificates are used to:

- **Encrypt Data**: SSL encrypts sensitive information such as login credentials, credit card numbers, and personal data, protecting it from being intercepted by malicious actors.
- **Authenticate Identity**: SSL certificates verify that the website belongs to the organization it claims to represent, protecting against phishing attacks.
- **Improve SEO**: Search engines like Google prioritize secure websites in search rankings, improving your site's visibility.
- **Build Trust with Visitors**: An SSL-secured website displays a **padlock** icon in the browser, signaling to visitors that the site is trustworthy and secure.

Without SSL, websites are flagged as "Not Secure" by browsers, which can deter users from engaging with the site.

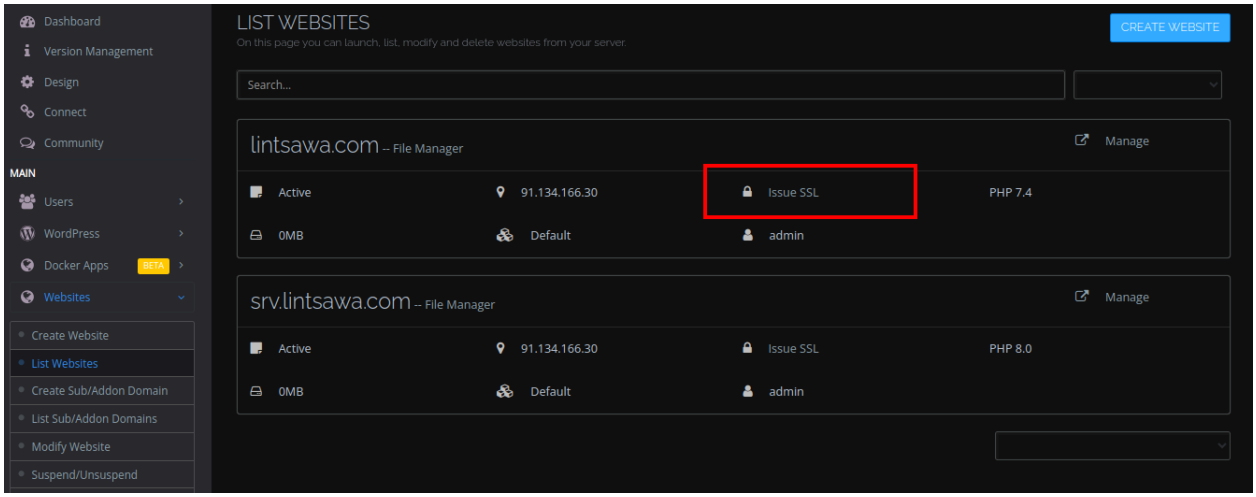
8.2 Issuing SSL Certificates: Setting up Free SSL with Let’s Encrypt

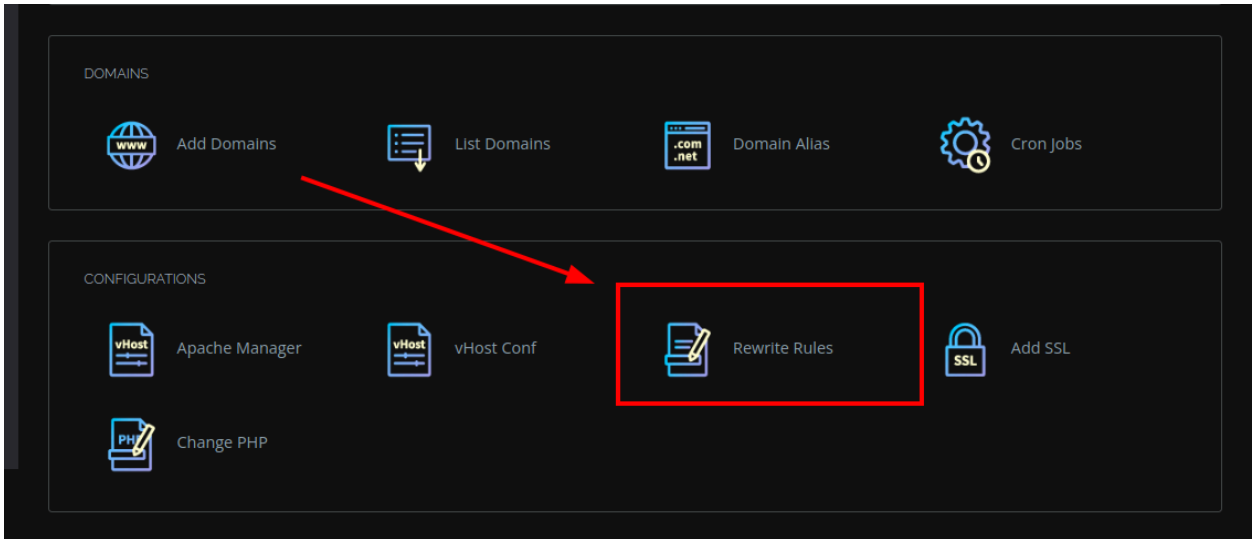
CyberPanel provides a simple way to issue SSL certificates for websites using **Let’s Encrypt**, a free, automated, and open certificate authority.

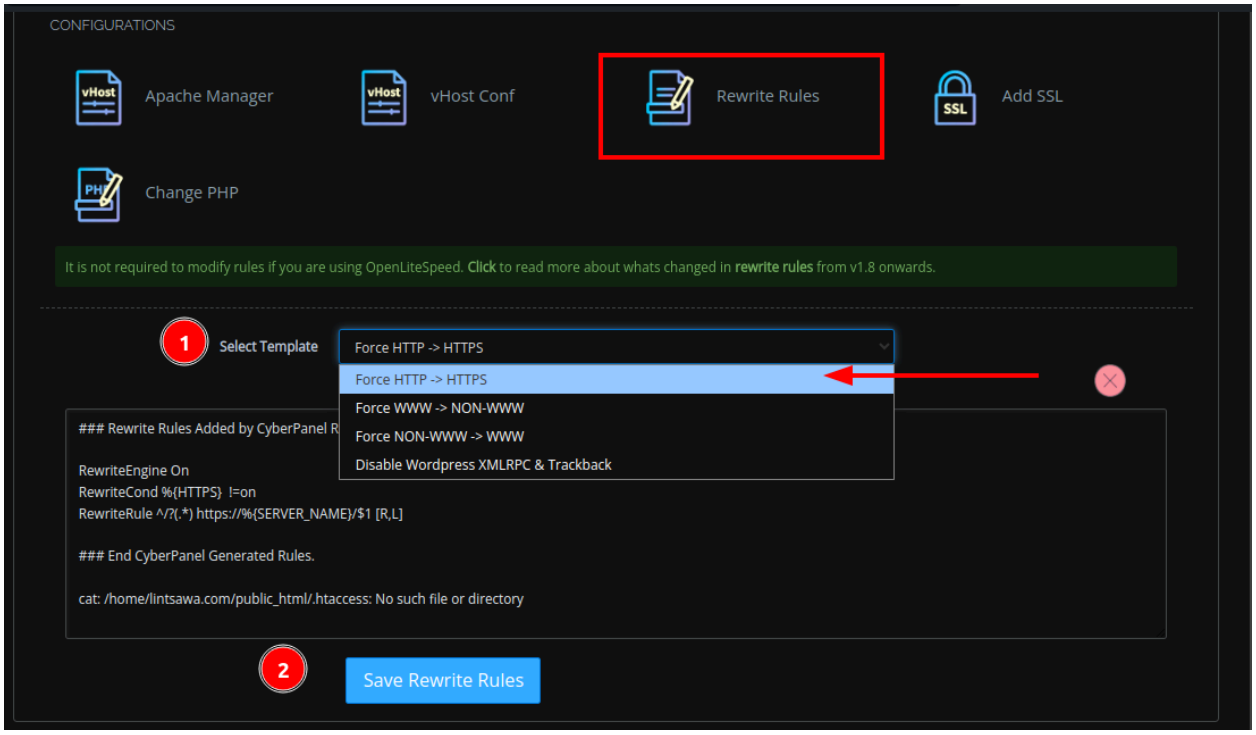
8.2.1 Setting up SSL with Let’s Encrypt

1. **Navigate to Websites Section**: In CyberPanel, go to the **"Websites"** section.
2. **Choose the Website**:
    - Select the website you want to issue the SSL certificate for.
3. **Access SSL Settings**:
    - Under the website management options, find and click on the **"Issue SSL"** option.
4. **Enable SSL**: Click **"Issue SSL"** to generate and install the certificate.
    - After successful installation, your website will have an active SSL certificate.
    - To redirect visitors to https, Click on Manage
    - Go to **Configurations** -> **Rewrite Rules**

- Select Template : Force **HTTP -> HTTPS**







8.2.2 SSL for Subdomains

1. If your website includes subdomains, repeat the SSL issuance process for each subdomain.
2. Alternatively, you can issue a **Wildcard SSL** that secures both the primary domain and all subdomains. Wildcard SSL is often a premium feature. Not covered in this course.

8.3 Auto-Renewal: Managing SSL Renewals

CyberPanel simplifies SSL certificate management by offering auto-renewal features for Let’s Encrypt certificates. However, you may need to verify that the

auto-renewal is properly set up and troubleshoot any renewal issues.

8.3.1 Setting Up Auto-Renewal for SSL

1. **Automatic Renewal Setup**:
    - Let’s Encrypt SSL certificates are valid for 90 days. CyberPanel automatically attempts to renew them before expiration.
2. **Manual Renewal**:
    - If auto-renewal fails or you wish to renew manually, click on the **"Issue SSL"** button for the specific domain.

8.3.2 Monitoring SSL Expiration

. You can also monitor SSL expiration dates from the SSL Manager.

8.3.3 Troubleshooting SSL Renewal Issues

Sometimes, SSL renewal might fail due to various reasons, such as DNS misconfigurations or connection issues. Here are some common steps for troubleshooting:

1. **Check Domain DNS**: Ensure the domain's **A records** point to the correct server. Misconfigured DNS can prevent SSL issuance or renewal.

2. **Check Server Connectivity**: Let’s Encrypt requires access to your website for verification. Ensure that your server is publicly accessible.
3. **Fix Mixed Content Issues**: If the SSL is working but your site still shows a "Not Secure" message, you may have **mixed content** (HTTP links or assets). Update any HTTP resources to HTTPS.

8.4 Troubleshooting SSL Issues

SSL certificate issues can result in users being blocked from your site, which can harm user trust. Some common SSL issues include:

1. **SSL Not Installing**: Ensure DNS settings are correct, and the server can access Let’s Encrypt’s servers. Try reinstalling the SSL certificate if necessary.
2. **Certificate Expiration**: If the SSL certificate expires, manually renew it and check that auto-renewal is enabled for future updates.
3. **Mixed Content Errors**: Use browser developer tools to identify non-HTTPS resources and update them accordingly.