Module 4: SSL Best Practices

1. SSL and SEO

- **HTTPS as a Ranking Signal:**
  - Search engines like Google prioritize secure websites in search rankings.
  - HTTPS enhances user trust, reducing bounce rates and improving engagement metrics.
- **Planning and Executing a Seamless HTTP to HTTPS Migration:**
  - **Preparation:**
    - Acquire an SSL certificate suitable for the website.
    - Update all internal and external links to use HTTPS.
  - **Implementation:**
    - Redirect HTTP traffic to HTTPS using 301 redirects.

      Example code to use for redirects.

```
RewriteEngine On

RewriteCond %{HTTPS} off

RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

    - Update the canonical tags to reference HTTPS versions.

      Example, for domain.com, the canonical name www.domain.com should also have SSL.

    - Update your sitemap and resubmit it to search engines.
  - **Post-Migration Check:**
    - Test for mixed content errors using tools like browser developer tools or online scanners.

For more details:
https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

        - Monitor traffic changes via analytics platforms.

---

2. SSL Compliance and Security

- **Certificate Lifecycle Management:**
    - Ensure timely renewals of SSL certificates to avoid expiration.
    - Regularly review certificate configurations to ensure alignment with the latest standards.
- **Advanced Security Features:**
    - **Perfect Forward Secrecy (PFS):**
        - Uses ephemeral keys for encryption, ensuring past communications cannot be decrypted even if the private key is compromised.
        - Configurable in modern web servers like Nginx and Apache.
        - Docs: https://www.sectigo.com/resource-library/perfect-forward-secrecy
        - May not be implemented currently on cPanel.
    - **OCSP Stapling:**
        - Reduces the overhead of real-time certificate validation by allowing servers to "staple" the OCSP response.
        - Enhances performance and security.
        -
- **Understanding Certificate Revocation:**

    - **Certificate Revocation List (CRL):**
        - A list of certificates that have been revoked by the Certificate Authority.
    - **Online Certificate Status Protocol (OCSP):**
        - Enables real-time checking of a certificate's status.
        - OCSP Stapling provides this information without additional client requests.
        - Docs : https://knowledge.digicert.com/quovadis/ssl-certificates/ssl-general-topics/what-is-ocsp-stapling

---

3. Best Practices for SSL Optimization

- **Ensuring Consistent HTTPS Implementation:**
    - Redirect all HTTP traffic to HTTPS with server-level rules (e.g., **`.htaccess for Apache and Litespeed`**, Nginx configurations).
    - Update all resources (images, CSS, JS) to use HTTPS to avoid mixed content warnings.
- **Maintaining Secure Access to Certificates:**
    - Limit access to private keys and SSL configuration files.
    - Regularly audit SSL configurations for vulnerabilities.

---

4. Final Project

- **Objective:**
  Implement and optimize SSL for a Truehost-hosted domain, applying all the knowledge acquired in the course.
- **Steps:**
    - Acquire an SSL certificate (Free, Trial or Paid) through Truehost.

    - Install the certificate on a chosen platform (e.g., cPanel, Plesk, [Apache or Nginx] via SSH).
    - Validate the installation using tools like SSL Checker.
    - Optimize the configuration and enabling HTTPS redirects.
    - Diagnose and resolve any mixed content errors.
- **Deliverables:**
    - A fully functional and secure HTTPS-enabled website.
    - A report documenting the process, challenges, and solutions.

The END.