MIT WORLD PEACE UNIVERSITY

Information and Cybersecurity
Second Year B. Tech, Semester 1

SECURED WEB APPLICATIONS

LAB ASSIGNMENT 9

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

May 1, 2023

Contents

1 Aim

Demonstration of secured web applications system using SSL certificates and its deployment in Apache tomcat server

2 Objectives

To learn different vulnerability scanning.

3 Theory

3.1 SSL Certificate

An SSL (Secure Sockets Layer) certificate is a digital certificate that verifies the authenticity of a website and encrypts data transmitted between the website and the user's web browser. SSL certificates ensure that all sensitive information, such as usernames, passwords, and credit card numbers, are transmitted securely over the internet.

3.2 How does an SSL certificate work?

When a user visits a website that has an SSL certificate, the website's server sends the user's web browser a copy of the certificate. The browser then verifies the certificate with the Certificate Authority (CA) that issued it. If the certificate is valid, the browser establishes a secure connection with the website using SSL/TLS encryption.

3.3 Types of SSL certificates

There are different types of SSL certificates based on the number of domains or subdomains they cover, the level of validation, and the warranty offered by the Certificate Authority (CA). Some common types of SSL certificates include:

1. Domain Validated (DV) SSL Certificate: This type of SSL certificate only validates the domain name of the website, ensuring that it belongs to the entity requesting the certificate. DV SSL certificates are the most common type of SSL certificate and are suitable for personal websites or blogs.

2. Organization Validated (OV) SSL Certificate: This type of SSL certificate validates both the domain name and the identity of the organization or business requesting the certificate. OV SSL certificates are suitable for e-commerce websites and other online businesses.

3. Extended Validation (EV) SSL Certificate: This type of SSL certificate provides the highest level of validation and requires extensive documentation to prove the identity of the organization requesting the certificate. EV SSL certificates are suitable for large businesses and financial institutions.

4. Wildcard SSL Certificate: This type of SSL certificate covers multiple subdomains of a single domain name. For example, a wildcard SSL certificate for the domain example.com would cover subdomains such as blog.example.com and shop.example.com.

3.4   Benefits of SSL certificates

There are several benefits of using an SSL certificate for a website, including:

1. Data encryption: SSL certificates encrypt all data transmitted between the website and the user's web browser, ensuring that sensitive information is secure.

2. Authentication: SSL certificates provide authentication, verifying that the website is legitimate and belongs to the entity requesting the certificate.

3. Trust and credibility: SSL certificates display trust indicators, such as the padlock icon in the web browser's address bar, which can increase a website's credibility and reputation.

4. SEO benefits: SSL certificates can improve a website's search engine ranking, as search engines prefer secure websites.

5.

3.5   Example

Suppose you want to create an e-commerce website where users can purchase products and enter their personal information, such as name, address, and credit card details. To ensure that the website is secure and trustworthy, you decide to obtain an SSL certificate.

You choose to purchase an OV SSL certificate, which will validate your domain name and your business's identity. You submit your company's legal documents and undergo a validation process to prove your identity.

Once the CA verifies your documents and identity, they issue the SSL certificate, which you install on your website's server. Now, when users visit your website, their web browsers will establish a secure connection using SSL/TLS encryption, ensuring that their personal information is protected.

4   Platform

Operating System: Arch Linux x86-64
IDEs or Text Editors Used: Visual Studio Code

5   Input and Output

```
The Given Signature is Valid
```

6   Conclusion

Thus, we have successfully implemented

7 FAQ

1. **What type of encryption does SSL use?**

   Secure Socket Layer (SSL) uses a combination of symmetric and asymmetric encryption to secure data transmitted over a network. SSL uses asymmetric encryption during the initial handshake process, where the client and server exchange public keys to establish a secure communication channel. Once the secure channel is established, SSL uses symmetric encryption to encrypt the data being transmitted between the client and server.

   Symmetric encryption uses a single secret key to encrypt and decrypt data, while asymmetric encryption uses a pair of keys, one private and one public. The public key can be freely shared, while the private key is kept secret. In SSL, the public key is used to encrypt the data, and the private key is used to decrypt the data.

   SSL supports a variety of symmetric encryption algorithms, including AES, DES, and 3DES. It also supports a variety of asymmetric encryption algorithms, including RSA, DSA, and ECDSA.

2. **How safe is SSL?**

   SSL is generally considered to be a secure protocol for transmitting sensitive data over a network. SSL has undergone multiple revisions over the years, with the latest version being Transport Layer Security (TLS). TLS version 1.3 is the latest and most secure version of SSL/TLS, which has been designed to provide strong encryption and better security features.

   However, SSL can be vulnerable to various types of attacks, such as Man-in-the-Middle (MITM) attacks, where an attacker intercepts the communication between the client and server and eavesdrops on the conversation or alters the data being transmitted. SSL is also vulnerable to attacks that exploit weaknesses in the encryption algorithms or the SSL protocol itself.

   To mitigate these risks, SSL implementations must be properly configured and maintained to ensure they are up-to-date with the latest security patches and best practices. It is also recommended to use SSL/TLS certificates from trusted Certificate Authorities (CA) and to use strong passwords and multi-factor authentication to protect the private keys used for encryption.

3. **What are the benefits of SSL?**

   The benefits of SSL include:

   (a) Data encryption: SSL encrypts the data transmitted between the client and server, which helps to protect the data from unauthorized access and eavesdropping.

   (b) Authentication: SSL uses digital certificates to authenticate the identity of the server and ensure that the client is communicating with the intended server.

   (c) Trust: SSL/TLS certificates are issued by trusted Certificate Authorities (CA) that verify the identity of the server and ensure that the SSL/TLS certificate is valid.

(d) Compliance: SSL is required by many industry regulations and compliance standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

(e) Improved search engine ranking: Google has confirmed that HTTPS is a ranking factor, and using SSL/TLS can help to improve search engine rankings.