SEC102 - DEFENDING WEB APPLICATIONS

Course Learning Objectives

By the end of this course, you will be able to describe the most common web application vulnerabilities and familiarize yourself with defending them using best practices.

Description

This course will explore the most common security concepts for web application developers who are new to application security. You'll learn how to address general web application security issues by incorporating defense mechanisms in your code.

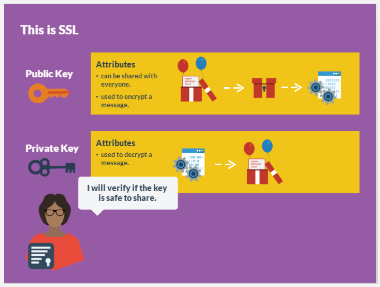
This course is for developers with little to no experience with cybersecurity.

Audience

Software Developers

Time Required

Tailored learning - 75 minutes total



This is SSL

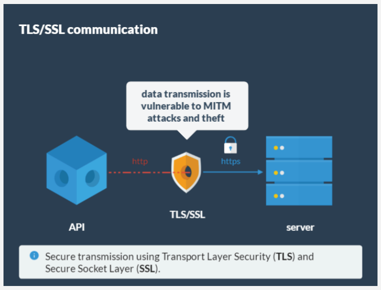
Public Key

Attributes
- can be shared with everyone.
- used to encrypt a message.

Private Key

Attributes
- used to decrypt a message.

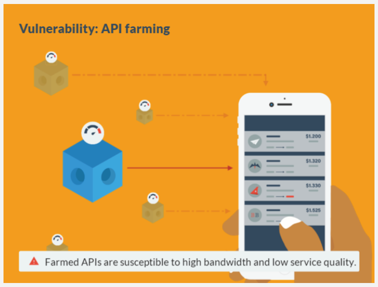
I will verify if the key is safe to share.



TLS/SSL communication

data transmission is vulnerable to MITM attacks and theft

Secure transmission using Transport Layer Security (**TLS**) and Secure Socket Layer (**SSL**).



Vulnerability: API farming

Farmed APIs are susceptible to high bandwidth and low service quality.

SEC102 - DEFENDING WEB APPLICATIONS

Course Outline

1. Authentication and authorization

- Three authentication factors
- Sequential brute force attacks
- Dictionary attacks
- Newsflash: Sony gets hacked by brute force
- 2-Factor authentication
- Account lockout
- Password complexity
- Increasing time delay
- CAPTCHA
- About authorization
- About roles
- Privilege escalations
- Newsflash: Binary.com
- Proper access control mechanisms
- Server-side validation of roles

2. Session management

- HTTP
- How HTTP requests look
- About session tokens
- Sessions as tickets
- Cookies
- Security concerns
- Client and server side issues
- Sequential tokens
- Repeating or exhausted tokens
- Time-driven generation
- Predictable sessions
- Session fixation example A
- Session fixation example B
- How do users get fooled?
- Newsflash: ColdFusion Server
- Assign a new session token
- HTTP verb tampering and cookie attributes
- Preventing verb tampering and cookie vulnerabilities

3. Secure account management

- User enumeration
- Implement account management features securely
- Password storage
- Registration
- Remember Me
- Password reset
- Cross-Site Request Forgery
- Defending against CSRF
- Newsflash: Coursera

4. Data validation

- Code versus data
- Trustworthy user data
- Data validation example
- Malicious input example
- Risks of data validation
- Newsflash: Shopify
- Client and server side validation
- Blacklisting and whitelisting
- Output encoding
- Bind variables and stored procedures

5. Insecure logging

- Log and error messages
- Information disclosure scenario - error message
- Information disclosure scenario - set up
- Information disclosure scenario - attack
- Monitoring of events
- Storage of sensitive data
- Newsflash: Mariott
- Generic error messages
- Logging frameworks
- Sanitizing data

6. Understanding SSL

- Problem 1: Safely sharing a key
- Problem 2: Who sent the box?
- This is SSL
- How SSL works
- User opens certificate details
- User checks certificate
- User asks CA if site is legitimate
- User creates shared key and encrypts it
- Both use a shared key
- About Trusted CAs
- Newsflash: Root CA hacking

SecurityCompass

SEC102 - DEFENDING WEB APPLICATIONS

Course Outline

7. Insecure web services

- Public and private APIs
- Authentication & authorization in Web APIs
- Vulnerability: API farming
- Defense: API keys
- Best practices for using API keys
- Defense: Perform authorizations checks
- Improper input validation in Web APIs
- Validate input and incoming data for REST services
- Missing or incorrect XML validation
- Use an XML schema
- Sanitize data
- Do not accept DTDs from users
- Secure transmission in Web APIs
- TLS/SSL communication
- Best practices for securing TLS/SSL communication
- Best practices for choosing a secure cipher

Security Compass