BEGINNER’S GUIDE TO WEB SECURITY

Gokul

Gokulakrishnan
Kalaikovan

Table of Contents

1. Introduction

2. How does the web works

3. Web Application Security

Table of Contents

Table of Contents

3.

Web Application Security

3. What Is Web Application Security?

Before we talk about web application security, let's talk about software development in 2020. The software development in 2020 is very different from how it was ten years ago. We often find ourselves writing code for requirements and keep adding more code to the codebase. And as an engineer or software developer, we often forget that security is a crucial part of the development both during and after the development.

Most of us keep security as a flexible part of the development which as in needed. Whenever a security issue is found and then at the time, we fix the issue and move forward with development. This is how most of the software development happens in many companies. The main reason for this is that security is a vague topic and many of us don't know what web security is or think it as in needed work. Let me tell you why you are wrong, why I was wrong by seeing some statistics below.

According to internet live stats, close to 30-60k websites are hacked per day, and according to NCSC's UK cyber survey, more than 23 million people use the password as "**123456**" in 2019.

Wordpress is one of the most popular ways to a create website even in the year 2020, and it accounts for over **~35%** of all the webpages on the World Wide Web (WWW). WordPress's 98% vulnerability is related to its plugins, and wordPress has around **~50k+** plugins. According to CVE report, wordpress's most popular vulnerabilities are Cross Site Scripting (XSS) and SQL Injection.

What is Web Application Security?

Web Application Security (Web AppSec), in a nutshell, is a process of protecting the web application from accessing or modifying or destroying the data by an un-authorised user. So let's understand, what type of security attacks are there, when and how it can happen.

Two types of security attacks

1. Passive Attack
2. Active Attack

Passive Attack

A passive attack is when the attacker attempts to monitor or eavesdrop or retrieve information sent from one website to another. The attacker's intention here is to steal the data but not to attack the website.

A passive attack is possible when a website uses a non-secure (HTTP) connection for transferring the data or any information from web server to client or vice verse. Any data transferred to or from application to server is susceptible to security attacks.

Examples

1. Listening to a message or an email sent from Person A to Person B.
2. Monitoring the traffic data to find the information such as location of a person.
3. Release of the contents like message conversions or sensitive information on the internet which can damage the reputation of an individual or an entity.

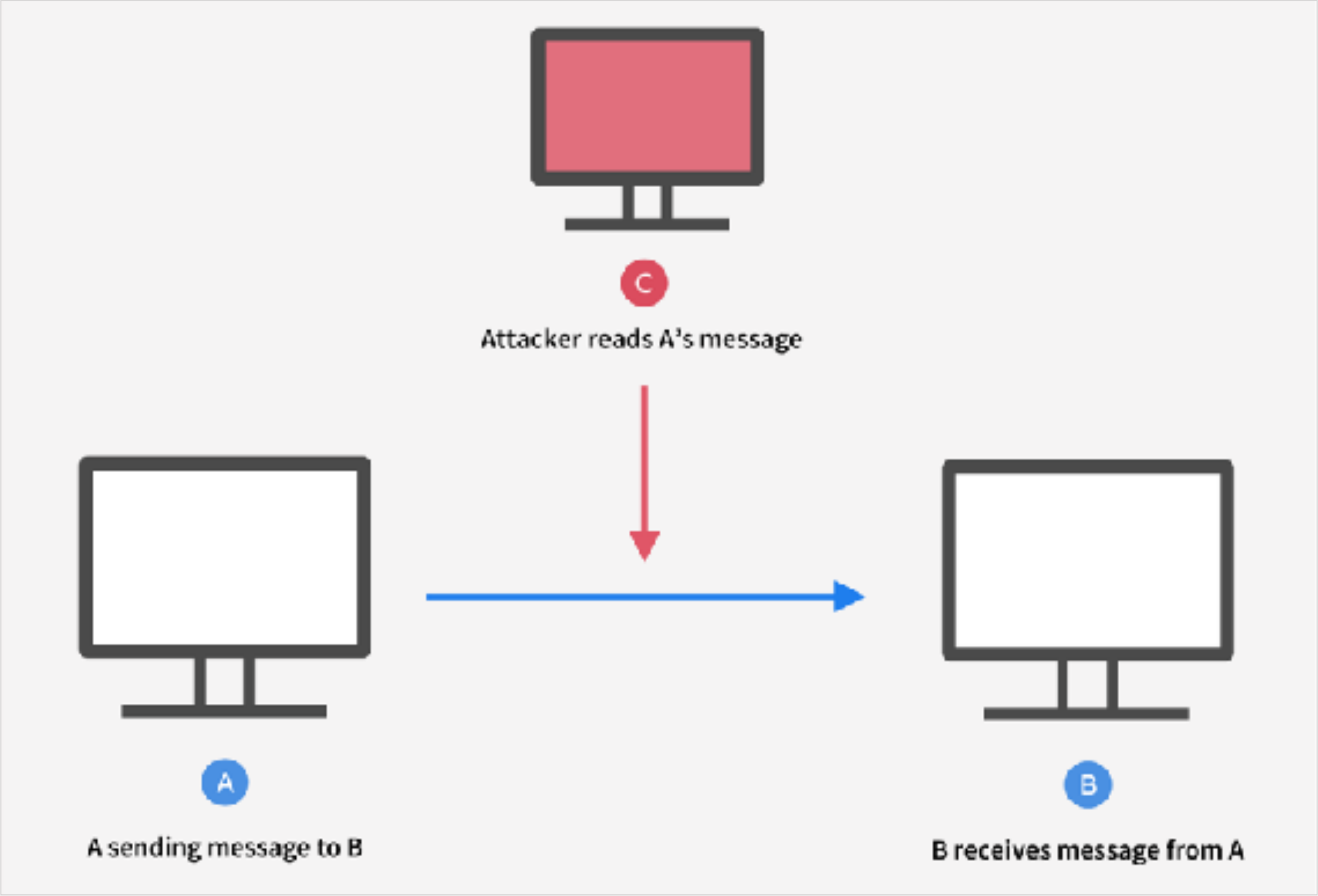

Figure 6: Passive Attack illustration

Active Attack

An active attack is when the attacker wants to take down or destroy the application or web server. This kind of attack involves modification or removal of data from the web server.

Examples

1. Person A is chatting with Person B, and the attacker (Person C) pretends to be Person B is called masquerading.
2. Person A sends a message to Person B, but the attacker (Person C) modifies the data in the middle before received by the Person B.

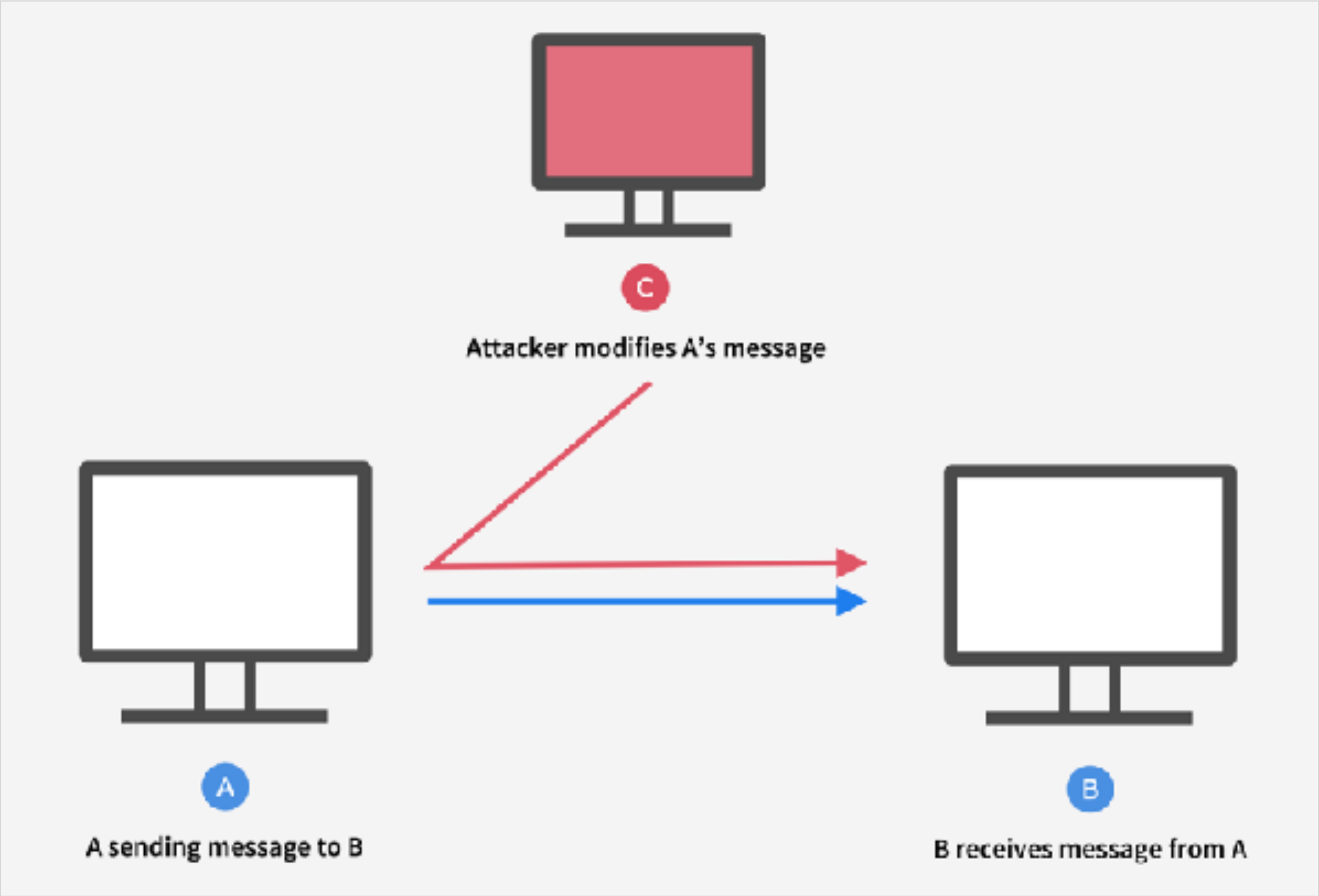

Figure 7: Active Attack illustration

Software Development Lifecycle (SDLC)

It is a common practice before, and even now, many companies follow security related activities as part of testing the application at the end of the development. By doing so, there is a higher chance of discovering a significant number of risks at the end, or there is a chance the security risks might not be discovered at all.

Two approaches to security in SDLC

1. Shift Right Approach
2. Shift Left Approach

Shift Right Approach

Shift right security means moving the security testing to the very end of the software development lifecycle.

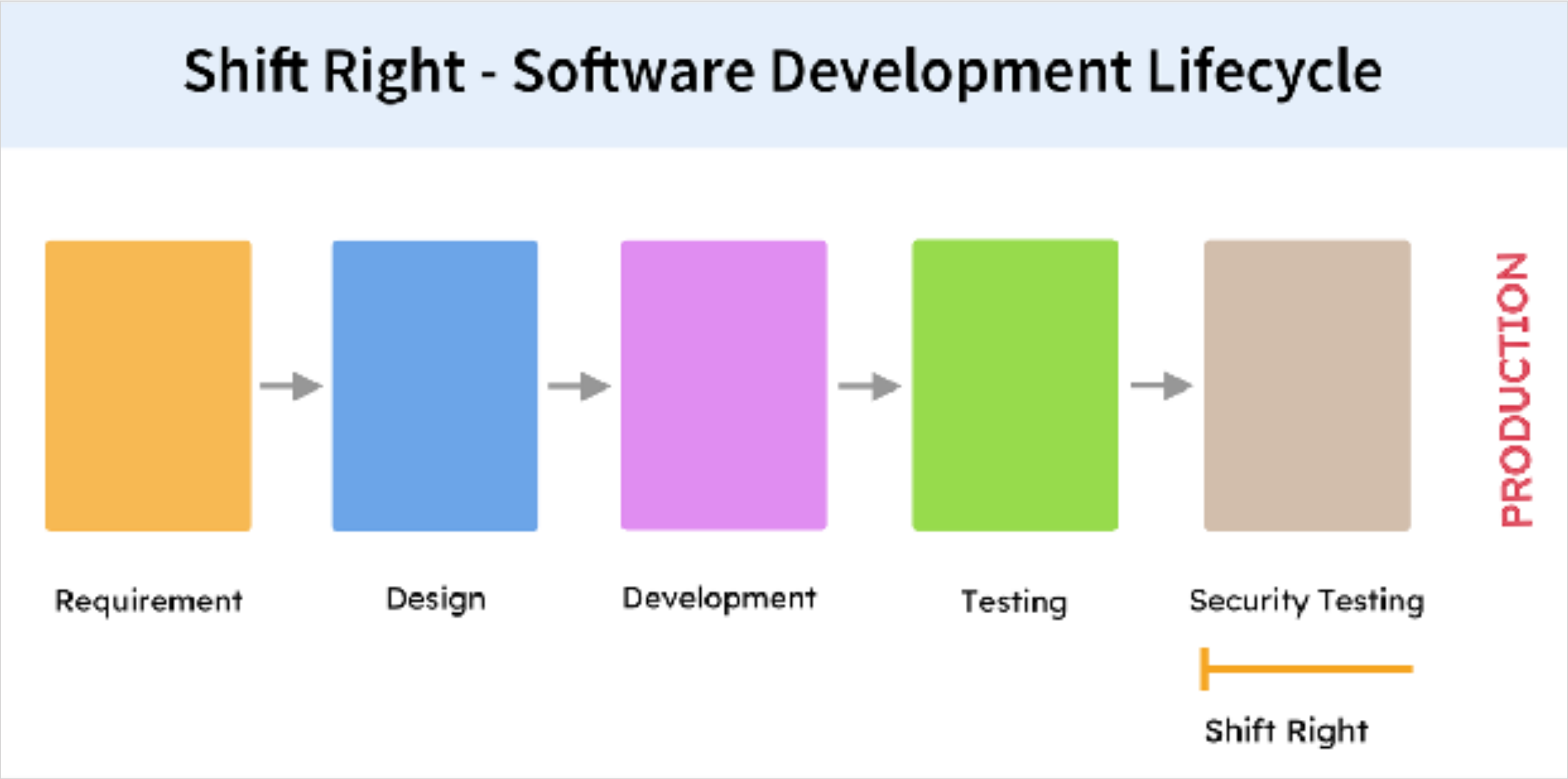

Figure 8: Shift Right approach in Software Development Lifecycle (SDLC)

Shift Left Approach

Shift left security means moving the security testing to the beginning of the software development lifecycle. Also called as Secure Software Development Lifecycle (SSDLC). Having the security aspect of application at the beginning of the software development lifecycle (shift left) will save a lot of time and money, if the risks were found during the development process instead of at the time of an attack or before going to production.

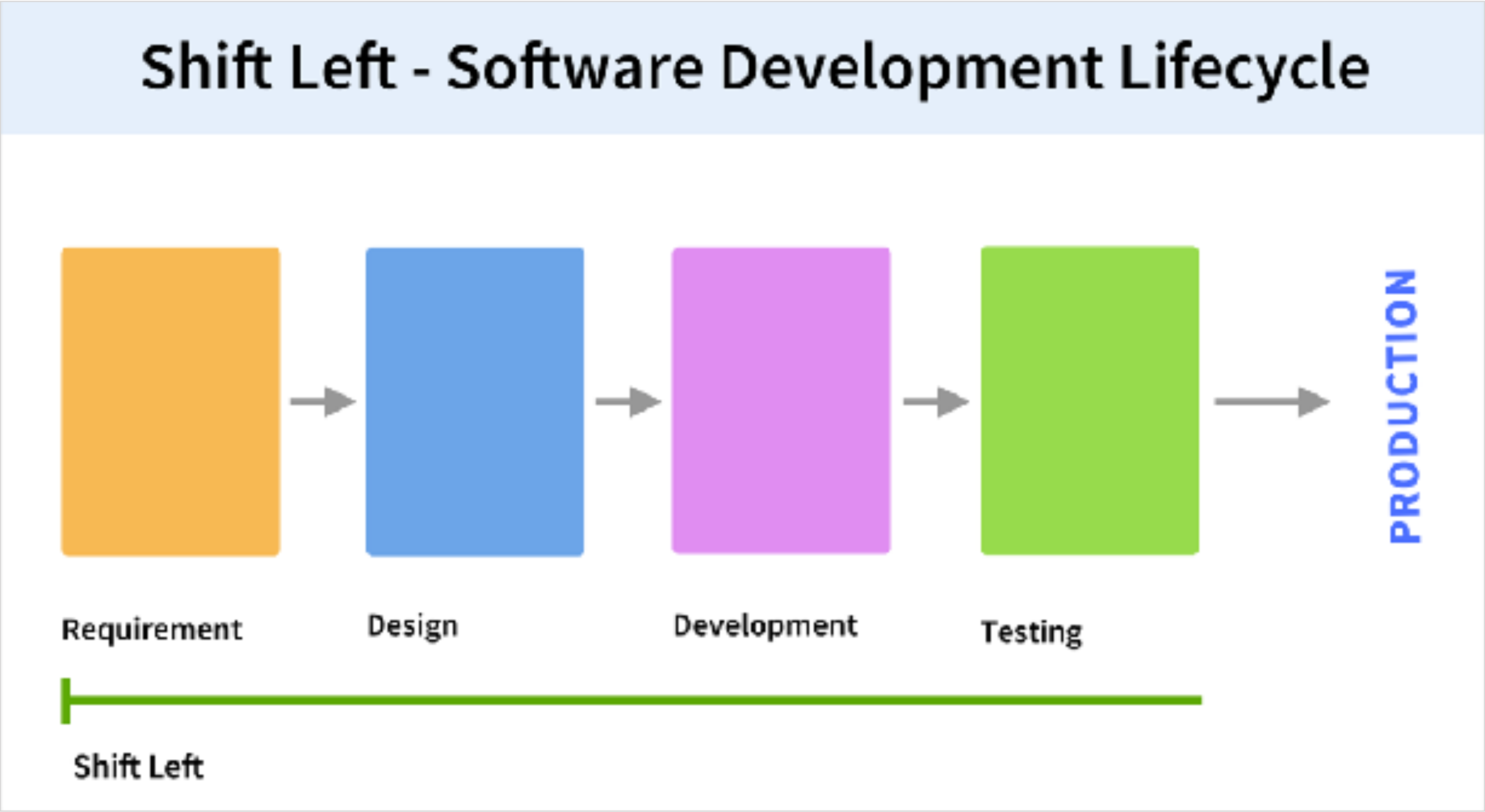

Figure 8.1: Shift Left approach in Software Development Lifecycle (SDLC)