Web Security Components (CS107)

40 Hours

Outline

This course including the top 10 web application attacks (OWASP ranking) and understood drill-down the attacks, including codes examples, lab and exercises. In the end of the course the students understand how to attack, and how to defense own code. And get best practice of web attacks and defense.

Prerequisites

- Experienced web developers.
- Experienced in Jscript programming
- Experienced basic SQL queries and database structure.

Contents

Introduction of web application hacking

In this section we talk about biggest attacks scenarios in the world, and explain the attack vectors, and how is work.

Client side restrictions and parameter tempering

In this section we talk about Burp suite program, and another proxies to intercept band width. We talk about the concept and how is help us to penetrate applications (Mobile and Web)

Types of Injection Flaws attacks and prevention

OS Injection - explanation, wrong code example, secured code and labs

SQL Injection - explanation, wrong code example, secured code and lab

Offline and online password attacks

In this section we talk about brute-force attacks, online and offline, and do labs and exercise

Cross-site scripting - attacks and prevention

In this section we talk about HTML attacks vector in real life, do a labs and exercises

Cross-Site Request Forgery attacks

We talk about CSRF attacks in real life, and demonstrate banking attack(via labs)

File inclusion attacks

File inclusion attacks

Unrestricted File Upload

Client side attacks and Java applets

Real-life hacking attack scenario