Why this topic?

Most enterprises, regardless of size, run their own web applications. Vulnerabilities in these web applications make them prime targets for hackers – and hackers succeed at a very high cost both to enterprises and their customers.

Web application security is essential mainly because of the scale of impact. Millions of people interact with web applications every day to do everything from reading the news to shopping for groceries to planning their finances, and many of these applications store personal data such as addresses and credit card information. A single vulnerability is all a hacker needs to retrieve all of this.

No pentester can be truly effective without a working understanding of web application security. In the following sections, you'll learn to systematically dissect the inner mechanics of an application, chalk out the threatscape, identify possible attack vectors and then use various tools and techniques to launch the attack.

Prerequisites

- Basic knowledge of computers and networking
- Familiarity with the Linux operating system

What will you learn?

These labs will familiarize you with the basics of **Web Application Pentesting**. To start with, we'll take a look at some key concepts of web applications, followed by methods of uncovering and exploiting the OWASP TOP 10 vulnerabilities. We will also take a look at manual exploitation techniques using popular open-source attack tools.

Overall, these labs and techniques are technology-stack agnostic and will use a combination of simulated and real-world applications.

References:

- Web Application Pentesting
- WAP Challenges
- Pentesting Challenges

While the lab sections have been designed to be used independently of each other, we recommend that beginners tackle them in this order:

Web Application Basics

At the start, it is important to understand how web applications work and how various components interact with each other. This section will cover various web application concepts and protocol basics.

The infosec community has done a wonderful job creating a variety of open-source pentesting tools. Tools are available to enumerate web applications and gather the information that can be useful in identifying vulnerabilities and creating application/platform-specific payloads for attacks such as LFI and Command Injection. In this section, we will take a look at how to use popular open-source tools for reconnaissance and the automation of attacks.

OWASP Top 10

OWASP Top 10 is an awareness document that outlines the most critical security risks to web applications. Pentesting is performed according to the OWASP TOP 10 standard to reduce/mitigate security risks. In this section, we will take a look at how to identify and exploit OWASP Top 10 vulnerabilities.

Webapp CVEs

Common Vulnerabilities and Exposures (CVE) is a list of all publicly disclosed vulnerabilities. In this section, we will take a look at how to search for a publicly available exploit for a vulnerability and use it to compromise the target machine.