# Web Application Security

***In this course, you will explore web application threats and countermeasures focused on Fortinet solutions. Comprised of theory lessons and hands-on labs, this course will guide you from the very motivations of attacks on web applications through to understanding and executing attack techniques. You will gain insight into recognizing such attacks, and, finally, configure Fortinet solutions to mitigate them.***

## Product Version

- FortiGate 7.2.1
- FortiWeb 7.2.1

## Course Duration

- Lecture time (estimated): 3 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated):7 hours/1 day

## Who Should Attend

Networking and security professionals involved in the architectural design, implementation, and monitoring of solutions to address web application security based on FortiGate and FortiWeb devices should attend this course.

This course assumes advanced knowledge of networking and web application security concepts, and extensive hands-on experience working with FortiWeb and FortiGate devices.

## Certification

There is no certification for this course at this time.

## Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure

It is also recommended that you have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 6 FortiWeb
- NSE 7 Advanced Threat Protection

## Agenda

1. Contextualization
2. Attack Procedures
3. Software and Tools
4. Incident Detection
5. Threat Mitigation

## Objectives

After completing this course, you will be able to:

- Identify adversary motivation and opportunities to attack web applications
- Identify the top security risks associated with web applications and the common challenges faced when addressing these risks
- Identify various attacks on web applications by examining real-world examples
- Identify how adversaries exploit web application vulnerabilities using attacks, such as SQL injection, local and remote file inclusion, cross-site scripting, cross-site forgery, and so on
- Use popular software and tools used for web application security testing
- Detect security incidents targeting web applications
- Improve mitigation capabilities related to threats against web applications using methods, such as layered architecture, machine learning, solution integration, secure software development life-cycle, and so on

## Delivery Options and SKUs

### Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-CST-WAS

### Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- Purchase order (PO), through Fortinet Resellers or Authorized Training Partners

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-CST-WAS-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

## (ISC)2

- CPE training hours: 3
- CPE lab hours: 4
- CISSP domains: Security Operations

## Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.