INFOSEC Skills

LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

# OWASP Top Ten Boot Camp

Infosec's two-day OWASP Top Ten Boot Camp includes a mix of expert instruction and hands-on secure coding lab activities designed to provide web developers, web administrators and other IT and information security professionals with an overview of the ten most critical web application security risks.

## Course description

The Open Web Application Security Project (OWASP) Top Ten is widely recognized as a powerful awareness document that represents a broad consensus among security experts about the most critical security risks to web applications.

This boot camp is designed to educate those who develop, administer and secure web applications about the most common web application security vulnerabilities, the potential impact of exploiting these weaknesses and basic approaches to mitigating web application security risks.

## Who should attend

Infosec's OWASP Top Ten Boot Camp applies to a broad audience. Primarily designed for professionals whose job function includes creating web applications, it will also be highly beneficial for other IT and information security professionals, as well as managers who want to know more about web application security risks and what they mean to an organization.

## Boot camp at a glance

### Get certified

- ✓ Methods for discovery and exploitation of common issues
- ✓ Causes of common coding errors
- ✓ Protecting web applications from the top 10 risks

### Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

### Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 2-day boot camp
- ✓ 90-day extended access to all boot camp materials

### The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

#### Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

#### Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

#### Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

#### 700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

# What's included

- Two days of expert, live OWASP Top Ten training
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Pre-study learning path
- Knowledge Transfer Guarantee

### Pre-class preparation

Signing up for Infosec's OWASP Top Ten Boot Camp means more than just attending a two-day training. The program starts with quality custom pre-study course, an interactive self-learning experience that combines reading materials, videos, practice questions, and other types of resources and guidance.

## OWASP Top Ten objectives

This training follows the structure of the OWASP Top Ten list of the most critical web application security risks. For each risk, it provides its description, common examples of vulnerabilities and ways the attackers can use to exploit them, and explains potential consequences of a successful attack.

Basic guidance on how to avoid each risk is also provided, which is delivered in engaging, seminar-style lecture format with hands-on lab exercises for you to complete. This hands-on approach keeps you engaged and ensures the knowledge transfer of critical secure coding techniques.

## Experienced instructors

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. We've helped tens of thousands of students like you get certified and advance their careers.

## What you'll learn

After successfully completing this boot camp, you will:

- Recognize the causes behind and
- the consequences of common
- coding errors and mistakes
- Understand the methods for discovery
- and exploitation of these issues
- Understand the basic practices that help
- prevent the most common mistakes
- and lead to more secure software

## Hands-on labs

The OWASP Top Ten Boot Camp features several hands-on labs, including:

- Exploiting SQL injection
- Attacking authentication
- Cross-site scripting exploitation
- Source code auditing
- CMS identification
- Attacking web services
- Client-side attacks
- Open source analysis & Google hacking
- Exploiting web application with w3af

## Skill up and get certified, guaranteed

### 100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

### Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

# What our students are saying

“Amazing experience! The methods of teaching the material are right on spot. The presentation of the material made it easy for everyone in class to understand and the instructor’s knowledge and practical experience supported all aspects of the training.”

**Kurt Kopf**

Freddie Mac

“I went to West Point for my bachelor’s, Columbia for my master’s and had multiple Army-led courses and this ranks as one of the best, most engaging courses that I have ever had.”

**William Jack**

US Army

“I have been in this industry for over 10 years, and I have never seen or heard anyone explain complex ideas and systems in such an easy-to-digest manner.”

**Antonio Roberto Garcia**

GRA Research

# OWASP Top 10 Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions!

This boot camp is sectioned into ten modules, based on the latest release of the OWASP Top 10 list. The material is constantly being revised and is subject to change.

### A1 - Injection

Injection flaws, such as SQL, OS, XXE and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. Attackers send simple text-based attacks that exploit the syntax of the targeted interpreter. Injection can result in data loss or corruption, denial of access or lead to complete host takeover.

### A2 - Broken authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently). Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.

### A3 - Sensitive data exposure

The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm usage is common, particularly weak password hashing techniques. Attackers typically don't break crypto directly. They break something else, such as stealing keys, performing man-in-the-middle attacks, or stealing clear text data off the server, while in transit or from the user's browser. Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive data such as health records, credentials, personal data and credit cards.

### A4 - XML external entities (XXE)

By default, many older XML processors allow specification of an external entity, a URI that is dereferenced and evaluated during XML processing. Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies or integrations. These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks.

### A5 - Broken access control

Applications and APIs don't always verify the user is authorized for the target resource. This results in an access control flaw. Attackers, who are authorized users, simply change a parameter value to another resource they aren't authorized for. Such flaws can compromise all the functionality or data that is accessible.

### A6 - Security misconfiguration

Good security requires having a secure configuration defined and deployed for the application,frameworks, application server, web server, database server and platform. Attackers access default accounts, unused pages, unpatched flaws, unprotected files and directories to gain unauthorized access to or knowledge of the system. Occasionally, such flaws result in a complete system compromise.

### A7 - Cross-site scripting (XSS)

XSS flaws occur when an application updates a web page with attacker controlled data without properly escaping that content or using a safe JavaScript API. Attackers can execute scripts in a victim's browser to hijack user sessions, deface websites, insert hostile content, redirect users, hijack the user's browser using malware and more.

### A8 - Insecure deserialization

Applications and APIs will be vulnerable if they deserialize hostile or tampered objects supplied by an attacker. This can result in object- and data-structure-related attacks or data-tampering attacks, such as access-control-related attacks where existing data structures are used but the content is changed. Exploitation of deserialization is somewhat difficult, as off-the-shelf exploits rarely work without changes or tweaks to the underlying exploit code. The impact of deserialization flaws cannot be overstated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible.

### A9 - Using components with known vulnerabili-ties

Many applications and APIs have these issues because their development teams don't focus on ensuring their components and libraries are up to date. In some cases, the developers don't even know all the components they are using, never mind their versions. Attackers identify a weak component through scanning or manual analysis. They customize the exploit as needed and execute the attack. The impact could range from minimal to complete host takeover and data compromise.

### A10 - Insufficient logging & monitoring

Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected. Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%. One strategy for determining if you have sufficient monitoring is to examine the logs following penetration testing. The testers' actions should be recorded sufficiently to understand what damages they may have inflicted.

## After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

## About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC