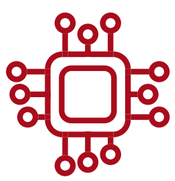
OFFENSIVE® security

WEB APPLICATION SECURITY

Is your organization protected?

INTRODUCTION

—Web Application Security



ARE ORGANIZATIONS DOING ENOUGH TO STAY SECURE?

What if someone was able to access and steal your company’s intellectual property or customer data? These are the types of concerns Chief Information Security Officers lose sleep over. Despite conducting frequent and independent security audits, even the most security focused organizations can remain susceptible to the latest vulnerabilities and attacks.Today, most organizations handle sensitive personal and business data in web based applications, and as a result, allocating resources towards vulnerability mitigation isn’t a choice anymore, it’s a must.

As more and more organizations transition their business operations to these web applications, security in the development process can no longer be an afterthought. Whether it’s a code injection, privilege escalation, DDoS attack, or a vulnerable element, bad actors are constantly looking for creative ways to manipulate exploits for personal gain. Each hack costs an organization in reputation, time, and money – and customers are increasingly aware of the fallout.

We've all put in the work to be secure, but has it been enough?

92%

OF WEB APPS HAVE SECURITY WEAKNESSES

An overwhelming amount of web applications contain exploitable security vulnerabilities

Source: ImunniWeb

OFFENSIVE® security

WHO SHOULD BE CONCERNED?

—Everyone

If your company has a web app, you need to worry about its security. This isn't an area to be left to the security analysts or the IT team. Web developers need to take a hand, too. Privacy by design is a good start, but it's really just the first step.

Hackers will be targeting scripts, file extension filters, cross-site requests, and character restrictions and more. They'll be looking for ways to bypass restrictions on file uploads, RegEx, and characters. And these vulnerabilities are just the beginning.

What measures can be taken to reduce the risk of a hacked web app?

OFFENSIVE security

BEST PRACTICES FOR WEB APPLICATION SECURITY

NEVER TRUST USER INPUT

Bad actors will attempt to submit malicious inputs through available entry points. Sanitizing this input against well thought-out requirements and restrictions is a critical first step.

DISABLE UNUSED FUNCTIONALITY

If a feature, theme, plugin, or service isn’t used by your web application, disable it. Leaving unused functionality available increases the attack surface of an application.

CONDUCT REGULAR SAFETY ASSESSMENTS

Contract with an independent firm unfamiliar with your infrastructure and systems. They’ll think differently and test vulnerabilities you might have glossed over.

INVEST IN ONGOING CYBERSECURITY TRAINING

Anyone who works on web apps, including security analysts, software engineers, or web developers, should receive training and education to understand how attacks can manipulate code.

CREATE A BUG BOUNTY PROGRAM

By offering monetary or other rewards to researchers who privately disclose application vulnerabilities, your team can be ahead of the curve in preventing potential attacks.

OFFENSIVE® security

BUT NOT EVERYONE HAS THE SKILLSET TO FOLLOW THESE BEST PRACTICES

Offensive Security's AWAE course can help.

OFFENSIVE® security

WHAT IS AWAE?

—Advanced Web Attacks and Explotation

Advanced Web Attacks and Exploitation (AWAE) is an advanced web application security review course. We teach the skills needed to conduct **white box web app penetration tests.**

Students learn how to:

- Perform a deep analysis of decompiled code
- Identify logical vulnerabilities many scanners aren't equipped to find
- Exploit vulnerabilities by chaining them into complex attacks

Students who complete the course and pass the exam earn the Offensive Security Web Expert (OSWE) certification. Certified OSWEs have a clear and practical understanding of the web application assessment and hacking process. They've proven their ability to review advanced source code in web apps, identify vulnerabilities, and exploit them.

OFFENSIVE® security

WHITE BOX

—What is it and why is it important?

A penetration tester's objective is to uncover vulnerabilities in a client system and determine how to exploit them. With web application pentesting, this doesn’t always mean cracking a system from the outside. Sometimes, the best way to discover how to break in is to start from the inside.

In a traditional web application penetration test, the tester might spend a couple of weeks working to access the client's systems with no previous knowledge: the black box approach. While black box testing has its place, it usually only manages to scratch the surface. This is particularly true with the limits often imposed by time and scope.

White box web application pentesting offers a different approach. For a comprehensive web app pentest, assessing the source code provides opportunities to go deeper. Many of the more dangerous bugs and vulnerabilities discovered in the field aren't simple syntax errors or other traditional vulnerabilities. They're the result of creatively chaining vulnerabilities together into an attack.

A white box approach has a greater chance of uncovering these smaller vulnerabilities within the limits of an engagement.

OFFENSIVE® security

WHO SHOULD TAKE AWAE?

—Security begins at the design stage

Investing in ongoing cybersecurity training for your team is likely one of the most valuable actions you can take to protect your web application's security. Anyone who works on the application front, whether they are security analysts, software engineers, or web designers should receive training and education. They need to understand how attacks can manipulate the code they write. Web applications are handling increasing amounts of sensitive personal and business data; as a result, security needs to be top of mind for every employee working on the application.

Job titles where web application security training may be particularly useful include:

- Software engineer
- Web application developer
- Full-stack web developer
- Quality assurance analyst or tester
- Information security analyst or engineer
- Cybersecurity consultant
- Penetration tester

OFFENSIVE® security

BENEFITS

—What's the ROI?

TRAIN AND RETAIN

Investing in training is a smart way to develop and retain in-house cybersecurity talent. AWAE offers an invaluable education on the protection of your web application. With the rapidly changing nature of the infosec space, it's critical that your team receives up-to-date training on the latest attacks and exploitation techniques.

PEACE OF MIND

Trust that your company's data, reputation and financial stability are protected, because your employees are prepared to take on challenges. They have received training from the experts who defined the standard of excellence in penetration testing training.

OFFENSIVE® security

INTERESTED IN LEARNING MORE?

Contact us at offensive-security.com

OFFENSIVE® security

ABOUT OFFSEC

WE TRAIN THE TOP SECURITY PROFESSIONALS

Offensive Security was founded in 2006 by and for information security professionals. Today, we're best known for the Offensive Security Certified Professional (OSCP) certification, the Kali Linux security distribution platform, and our motto: “Try Harder." With courses available in penetration testing, wireless security, and web application security, OffSec offers training in key information security areas. Course levels range from foundational to expert. Each course teaches not only the skills needed to succeed in information security, but also the mindset.

OFFENSIVE® security