Can your web apps withstand the onslaught of modern advanced attack techniques? Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

Are you ready to put your web apps to the test with cutting-edge skills? This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course section culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five sections in a fun environment based on real-world technologies.

Hands-on Learning Of Advanced Web App Exploitation Skills
We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We’ll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We’ll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

You Will Learn:

- How to discover and exploit vulnerabilities in modern web frameworks, technologies, and backends
- Skills to test and exploit specific technologies such as HTTP/2, Web Sockets, and Node.js
- How to evaluate and find vulnerabilities in the many uses of encryption within modern web applications
- Skills to test and evaluate mobile backends and web services used in an enterprise
- Methods to recognize and bypass custom developer, web framework, and Web Application Firewall defenses

“SEC642 is quality content for senior penetration testers – a nice extension of standard WAPT courses!”
— Caleb Jaren, Microsoft
## Section Descriptions

### SECTION 1: Advanced Attacks

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We’ll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQLi server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help us learn to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

**TOPICS:** Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploiting Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

### SECTION 2: Web Cryptography

Cryptographic weaknesses are a major area of web application vulnerabilities, yet very few penetration testers have the skill to investigate, attack, and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer. However, they often do not protect encrypted data from being attacked, or they enable the developer to use cryptography only weakly. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and how this can be done insecurely. Students will learn techniques ranging from identifying types of encryption to exploiting various flaws within encryption or hashing techniques.

**TOPICS:** Identifying the Cryptography Used in the Web Application; Identifying and Exploiting Hash-length Extension Attacks; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Collisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

### SECTION 3: Alternative Interfaces AND XML

Web applications are no longer limited to the traditional HTML-based interfaces. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. We will explore various techniques to discover flaws within the applications and backend systems. These techniques will make use of tools such as Burp Suite and other automated toolsets. We’ll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them. We’ll then examine a mobile backend, Representational State Transfer (REST) and Simple Object Access Protocol (SOAP) Application Programming Interfaces (APIs), Graph Query Language (GraphQL), XML XPath injection, and XML External Entity (XXE) attacks.

**TOPICS:** WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 and HTTP/3 Protocol Issues and Penetration Testing

### SECTION 4: Modern Web Frameworks, Part I

In this section we start exploring the underlying infrastructure of our frameworks and languages. It all begins with an exploration of the architecture of popular frameworks. There is coverage on architectural vulnerabilities found in frameworks even today, such as Mass Assignment. Newer frameworks such as server-side JavaScript frameworks with NodeJS show us some different exploitation options. Students will explore how to abuse vulnerabilities to append our JavaScript code blocks within these frameworks, leading to full system takeover. Next, we’ll explore Modern PHP, and while it is a much-maligned language, it is still hugely popular. Our exploration of Modern PHP takes us into types-inference bugs and how these issues can be abused and lead to system manipulation or bypassing controls. We’ll then turn to PHP deserialization bugs. Students will get to discover and build custom PHP deserialization payloads. We end the section with a lab that walks the student through building a PHAR payload that causes deserialization to occur, allowing us to exploit the underlying system. The topics covered in this section help us connect to the concepts that will be valuable in the next section, when we’ll be dealing with much more complex frameworks.

**TOPICS:** Web Architectures; MVC and its Architecture Components; JavaScript and JavaScript Frameworks; Server-Side JavaScript; Modern PHP; PHP Deserialization Bugs; Deserialization Through PHAR

### SECTION 5: Modern Web Frameworks, Part II

This course section continues the topics of the previous section with web frameworks. We start with Ruby- and Rack-based applications such as Sinatra and Ruby on Rails. Developers can improperly set up the Rack-based applications, and as part of that misconfiguration, we explore the abuse of the middleware layer using Ruby deserialization techniques. Next we’ll look at the Java Language and all its complexity. Some maintain that the Java language is a mature, enterprise language, while others claim it to be a complete security failure. Students will review Java’s security features and its security failings to discover, assess, and exploit Java Applications. The section features a walkthrough on how to construct Java attacks through Reflection, Serialization Issues, RMI, and the use of Java-Jar-based payloads.

**TOPICS:** Ruby and Rack Applications; Java, Java Gadgets, and Java Payloads; Java Payload Weaponization; Java Serialization; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPEs, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall’s Best-Defended Vulnerabilities, XSS and SQLi Bypassing Application Restrictions

### SECTION 6: Capture the Flag Challenge

In this final course section you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise is for you to explore the techniques, tools, and methodology you will have learned over the last five sections. You’ll be able to use these skills against a realistic extranet and intranet. At the end of the section, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF). You will be able to use this both in the class and after leaving and returning to your job.

---

**Who Should Attend**
- System administrators and IT professionals
- Developers, QA testers
- Security consultants
- Vulnerability assessment personnel
- Red team members
- Web and network penetration testers
- System architects
- System administrators and IT managers