Threat Management: Web Application Security Assessment
An adversarial perspective of web applications and supporting environments

Vulnerabilities in web applications are one of the most significant threats to critical business system environments because many web application vulnerabilities are due to an application's logic and design and are not readily identified by automated scanning software programs.

By utilizing real-world adversarial tactics and techniques, Optiv enables you to identify and prioritize the highest severity risks affecting your web application and its supporting infrastructure.

The Optiv Approach

**Develop a Profile**
Optiv leverages a targeted approach, starting with developing a profile of your application and conducting a threat assessment of the application before performing dynamic testing of the application. If the application environment is a cloud environment, Optiv conducts testing of the cloud environment.

**Data Storage and Controls**
During the security assessment, Optiv documents the locations where sensitive information is stored and tests the security controls used to secure it. Optiv also tests and documents the security channels used to communicate data, including sensitive data, and monitors the results to detect information disclosure issues.

**Manual Testing**
Optiv conducts manual testing involving customized and complex attacks against the application during the assessment. This type of testing is crucial to perform to identify vulnerabilities that can be identified by real-world adversaries.

**Network Testing**
Optiv also conducts network testing against the applications supporting environments to identify potentially exploitable vulnerabilities that could be exploited by adversaries to gain access or control of the applications supporting the environment.

**Static Analysis of Source Code**
If provided with source code, Optiv can perform static analysis of source code (SAST) as well as manually portions of the source code to identify vulnerabilities in the application that represent security risks in the application.
**Why Clients Choose Optiv**

The advantages of the Optiv approach to web application security testing:

**Socially Distanced Testing**
Optiv’s security professionals are proficient in performing the required security testing with no need for in-person or face-to-face contact.

**Comprehensive Assessments**
To ensure you’re meeting security requirements, not just in compliance, we leverage internally developed as well as leading third-party applications to do manual and automatic scanning of your application security program.

**Clear Continuous Communication of Testing Status and Findings Identified**
Optiv’s approach to performing testing provides clients with daily communication of progress and testing results.

**High-Quality Technical Reports**
Optiv’s refined process results in the consistent delivery of security testing reports of the highest levels of quality and technical content. They are both peer-reviewed and edited by professional technical writers before delivery.

**Expertise**
Our team of application security experts has extensive knowledge and experience in web applications, as well as as-a-service architecture and penetration testing. We have an in-depth knowledge of dynamic application and code scanning tools and methods and use these in conjunction with manual testing performed by expert security analysts.

---

**How We Do It**

**Pre-Engagement Knowledge Transfer:**
Optiv builds an understanding of web applications and their supporting environments before the commencement of testing.

**Profiling:**
Starting from the corporate environment, Optiv will identify the attack surface, which could lead an attacker to the web application and its environment.

**Attack Chain:**
Optiv will exploit applications, hosts, APIs, communication channels and platform vulnerabilities to attain access to sensitive application data and to modify application content and inject attack payloads to emulate real-world attack scenarios in the way an adversary could.

**Assisted Discovery/Vulnerability Scanning:**
Optionally, to ensure the integrity and operational state of the entire application environment, Optiv has the tools and capability to conduct broad vulnerability scans of the application environment. This can aid with asset discovery, the discovery of patching needed, and third-party component vulnerabilities. The scanning can be conducted during the profiling phase.

**Application Threat Assessment:**
Optiv can evaluate the security controls associated with both the application and its environment, completing the picture of both platform or environment-based and application-based attacks.