Web Application Security Assessment

Key Benefits

- Real-world testing: Evaluate your web applications against modern attacker tactics, techniques, and procedures (TTPs)
- Risk reduction: Identify unknown gaps in your web application's infrastructure and configurations
- Improved defenses: Receive threat prevention, detection, and remediation recommendations tailored to your organization's needs

Identify zero-day vulnerabilities and misconfigurations in your web application before attackers do

Service overview

Web applications are traditionally used by an organization to meet specific business needs through a custom design. To protect the security of web applications, reduce business risk, and ensure stakeholder confidence, custom applications require tailored assessments to identify security weaknesses and improve existing security processes for better prevention and detection against the latest cyber threats.

The Mandiant Web Application Security Assessment analyzes your web application to identify design weaknesses and insecure coding patterns, along with the discovery of security concerns unique to your application's attack surface. Once identified, Mandiant experts provide remediation recommendations to strengthen the overall security posture of your application throughout its lifecycle.

This assessment can be conducted in one of two ways:

- Closed box test (without application source code provided): Authenticated, dynamic testing of the application without prior information. This is typically used to model common, opportunistic threat actors.
- Open box test (application source code provided): Authenticated, dynamic testing of the application with source code static analysis. This allows for better coverage, more efficient testing, and optimized findings.

Service methodology

Mandiant experts work closely with an organization's internal engineers to understand their web application's existing threat model. This collaboration helps to determine the application's real-world attack surface and identify unique security risks that affect the specific application and its related components.

Next, Mandiant assesses the web application by probing for vulnerabilities and searching for misconfigurations found on web servers, backend applications, and frontend applications. This assessment goes beyond automated scanning with manual testing and validation to ensure coverage of your application.

This includes the discovery of business logic and authorization weaknesses based on industry-leading evaluation techniques and enhanced testing of the following application elements:

- Configuration and deployment management
- Identity management
- Authentication
- Authorization
- Session management
- Input validation
- Error handling
- Client-side handling

Once the vulnerabilities of these application components are identified, Mandiant experts develop a simulated, targeted attack scenario to exploit multiple vulnerabilities combined together, known as a vulnerability chain, to better demonstrate the real-world impact of an attack on the application, aligned with TTPs used by advanced threat actors.

Mandiant experts use the observations obtained from each phase of the assessment to provide strategic and technical guidance to help enhance your security approach through defense-in-depth solutions that improve the prevention, detection, and mitigation of your application's vulnerabilities and reduce overall risk.

Deliverables

Mandiant provides a full report that contains the following:

- Executive-level summary of findings to help senior-level management understand the current security posture of their application
- Technical details with step-by-step information to recreate the assessment for validation of remediation recommendations after implementation
- Vulnerability prioritization ratings identified through fact-based risk analysis based on exposure of the web application, ease of exploitation, and overall vulnerability impact
- Tactical guidance for long-term improvement of your application's security throughout its lifecycle