

In today's rapidly evolving digital landscape, web application penetration testing is more critical than ever. Trace3's Web Application Penetration Test is your urgent solution to uncover and address vulnerabilities before they become catastrophic breaches. Our experts simulate real-world attack scenarios to expose weaknesses that could lead to unauthorized access, privilege escalation, or service disruptions. By leveraging cutting-edge techniques, we provide actionable insights to fortify your defenses immediately. Don't wait for a breach to happen—invest in Trace3's services now to safeguard your critical assets and ensure robust web application security.



OVERVIEW

Our Web Application Penetration Test simulates the actions of a malicious actor who has targeted your website through open source intelligence, compromised credentials, or an insider threat. The goal is to identify and validate vulnerabilities that could lead to website defacement, privilege escalation, unauthorized access to sensitive data, or disruption of services. Trace3's offensive security experts utilize real-world attack techniques within a controlled and authorized environment to assess your website's resilience. Our web application testing services are designed for organizations looking to assess the effectiveness of their secure coding practices, implementation, and overall website security posture.



Testing Duration: Typically conducted over 2-4 weeks (depending on scope) via secure VPN

Rules of Engagement: Clearly defined scope, including URLs, credentials (if required), and authorized hours

Attack Surface Coverage:

- Web application (all exposed functions/features)
- Application APIs and endpoints
- Web server(s) hosting the app
- Application authentication & session management
- Application-level authorization controls
- Third-party integrations (if applicable)
- Business logic
- Client-side code (JavaScript, DOM manipulation, local storage)
- Data in transit (TLS/SSL)
- Client-specified areas of focus

Communication & Collaboration:

- Real-time updates available via client's specified communication method
- Coordination with the development and security teams to minimize disruption
- Access to a reporting platform to see findings in near real-time

Deliverables

Upon completion of the assessment process, Trace3 will review the vulnerabilities in depth with the client to ensure the risk information is conveyed clearly. The final report will include an executive summary, detailed vulnerability descriptions, risk ratings, and remediation recommendations. If requested, a one-page Letter of Attestation can also be provided.

Retesting

Following the final report delivery, Trace3 offers a single complimentary retest within a 90-day retesting window. This service ensures vulnerabilities marked as remediated have been properly addressed.

Retesting includes:

- Validation of previously identified issues
- Updated report showing risk reductions or remaining gaps
- Confirmation of website hardening and secure coding practices

VALUE

Trace3's Web Application Penetration Test is designed to identify and address security vulnerabilities that could compromise your web applications and the data they handle. Our specialists utilize industry-leading methodologies—including dynamic application testing, code review, vulnerability identification, and exploit validation—to thoroughly assess your applications from authenticated and unauthenticated perspectives. This engagement is suited for organizations seeking to evaluate the security posture of their web-based services, test input validation controls, evaluate authentication and session management, identify access control flaws, and validate the effectiveness of implemented security solutions. We maintain clear communication throughout the process, providing real-time updates and collaborating with your IT and development teams to minimize operational impact. Clients receive access to a live reporting platform with ongoing findings. After the engagement, a detailed report outlining vulnerabilities, business risk impact, and actionable remediation guidance is provided. A complimentary retest is provided within 90 days to verify that remediations are effective and risks are mitigated. By partnering with Trace3, you can proactively secure your web applications and safeguard your organization's critical digital assets against emerging threats.

Elevate your organization's security posture with Trace3's Web Application Penetration Test, pinpointing vulnerabilities and fortifying defenses against zero days, privilege escalation, and unauthorized data access, ensuring resilient protection and uninterrupted operations. For more information, contact your Trace3 Security expert or find us at [Trace3.com](https://www.Trace3.com).