



REDFOX

CYBER SECURITY PVT LTD

 1-800-917-0850

 info@redfoxsec.com

 redfoxsec.com

Application Security

Why Redfox Security

Redfox Security is a fast-growing cyber security consulting firm, spread across 4 countries. With over 9 years of global security consulting experience, we help businesses strengthen their security posture. Our mission is to help businesses grow securely with our top-line cyber security consulting services – and that’s exactly what we do.

We leverage our insightful understanding of the threat landscape to identify and resolve security risks. We believe in establishing a company culture that disrupts the status quo of security testing. With an undying passion for improving security, we continue to hire innovative talent while continually upgrading our penetration testing methodologies.

Application Security

Modern organizations significantly depend on the smooth and secure functionality of web applications.

Unfortunately, both small and large-scale organizations don’t prioritize security testing of their web applications. As a result, attackers can easily compromise these applications, disrupt business functionality, and gain unauthorized access to sensitive data. As numerous organizations falsely trust in the accuracy of automated web application security scanners, they’re left with unidentified loopholes in their application’s functionality, source code, and infrastructure.

Web application penetration tests are security assessments curated to analyze the architecture, design, and configuration of web applications. Our team makes use of advanced web application security skills necessary to perform a manual and thorough penetration test against modern web applications. Further on, we offer code-assisted penetration tests to explicitly understand the application, detect deep-seated issues in source code, and reduce the number of false-positive findings.

Benefits

-  Improve your overall security posture.
-  Find out about your application vulnerabilities.
-  Investigate any security flaws that may allow data theft.
-  Establish robust authentication and authorization controls.
-  Develop strong access control.
-  Find the most susceptible attack vectors via which an attack can be carried out.



What to Expect?

We deliver an in-depth report that displays all technical findings in detail, with the relevant risk ratings, descriptions, recommendations, and reproduction steps. Every report follows a strict QA process to ensure quality, accuracy, and correctness. At a high-level, our reports include the following sections:

- **Executive Summary:** Summary for executive- and senior-level management.
- **Strategic Recommendations:** Recommendations for longer-term improvement.
- **Detailed Findings:** Technical details that include enough information to reproduce the findings.
- **Recommendations:** Tactical recommendations for immediate improvement.
- **Risk Analysis:** Fact-based risk analysis to confirm a critical finding is relevant to the environment.

Our Engagement Process





Our Accreditations



Our Offices

Toronto Office

3080 Yonge Street,
Suite 6060, Toronto,
Ontario M4N 3N1,
Canada

London Office

Kemp House,
Unit 2446, 152 City Road,
London EC1V 2NX,
United Kingdom

Mumbai Office

A-201, Sunrise, Lokhandwala
Market, Andheri West,
Mumbai,
MH 400053, India

Santa Clara Office

4500 Great America Parkway,
Unit 190, Santa Clara,
CA 95054,
United States