WEB APPLICATION TESTING

Find and Address Application Security Flaws

The evolution of highly dynamic, interactive web applications has changed the way we interact with the web - and brought additional security risks with it. Additional user input, connected databases, and rapidly deployed code bring new attack vectors into existence - from simple injection flaws to complex, multi-staged attacks.

With decades of combined experience, Rhino Security Labs is at the forefront of application security and penetration testing. With a veteran team of subject matter experts, you can be sure every resource is an authority in their field.

APPLICATION TESTING BEYOND THE OWASP TOP 10

Application security issues are not only the most common type of vulnerability, they're also growing in complexity. While the OWASP Top 10 is used as the standard for identifying application security flaws, that's just a start - many advanced vulnerabilities are not included in that list. Automated vulnerability scanners and penetration testers focused on OWASP will fall behind new threats, leaving the application exposed to unknown risks.

At Rhino Security Labs, we go far beyond the OWASP Top 10, constantly pushing the boundaries of application security and detailing the way unique architectures can be abused – and how to fix them.

CODE REVIEW – IDENTIFY FLAWS EARLIER IN DEVELOPMENT

While 'blackbox' application assessments provide good insight to the capabilities and techniques of external attackers, particularly sensitive applications require a more robust audit. Secure code reviews identify bugs before they get pushed to production apps – and found by attackers.

With Rhino Security's penetration testing and Code Review assessment reports, you can ensure your apps are production ready. In addition to technical vulnerability and remediation details, each report provides an executive summary for non-technical management.

> *"Rhino Security Labs has a history of revealing how trust relationships between and among online services can be abused."*
>
> **– Brian Krebs, krebsonsecurity.com**

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122

ASSESSMENT DETAILS AND METHODOLOGY

At Rhino Security Labs, our application penetration testing targets the entire range of vulnerabilities in your webapp or API. Using the same techniques as sophisticated hackers, we providing unique visibility into security risks automated tools often miss. To ensure high quality, repeatable engagements, our penetration testing methodology follows these steps:

Information gathering on target environment

1. Reconnaissance

As with malicious hackers, each penetration test begins with information gathering. Collecting, parsing, and correlation information on the target is key to identifying vulnerabilities.

Identify and map vulnerabilities

2. Vulnerability Detection

Once the target has been fully enumerated, Rhino Security Labs uses both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find

Safe and controlled exploitation of vulnerabilities

3. Attack and Post-Exploitation

At this stage of the assessment, our consultants review all previous data to identify and safely exploit identified application vulnerabilities. Once sensitive access has been obtained, focus turns to escalation and movement to identify technical risk and total business impact.

During each phase of the compromise, we keep client stakeholders informed of testing progress, ensuring asset safety and stability.

Detailed, risk-prioritized report with remediation steps

4. Assessment Reporting

Once the engagement is complete, Rhino Security Labs delivers a detailed analysis and threat report, including remediation steps. Our consultants set an industry standard for clear and concise reports, prioritizing the highest risk vulnerabilities first.

The assessment includes the following:

- Executive Summary
- Strategic Strengths and Weaknesses
- Identified Vulnerabilities and Risk Ratings
- Detailed Risk Remediation Steps
- Assets and Data Compromised During Assessment

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122