Atumcell

Web App Penetration Testing

A Must for Private Equity Portfolio Companies

Contact

David E. Williams, CEO

d@atumcell.com

(617) 671-8810

atumcell.com

April 2025

Executive Summary

1. **Web applications power modern business workflows,** allowing users to manage sales pipelines, submit expense reports, and access dashboards directly through a browser.
2. **Private equity-backed companies invest heavily in web apps** for digital transformation. Web apps are quick to deploy and help companies scale rapidly.
3. **Web apps often contain severe cybersecurity vulnerabilities**—like privilege escalation—that let malicious users trigger fraudulent payments or expose business secrets and sensitive personal information.
4. **PE firms encourage portfolio companies to sell tools and platforms to one** another, making an insecure web app a point of entry into the entire portfolio, and multiplying the impact of an attack.
5. **Regular web application penetration testing** by expert providers can uncover and mitigate these risks before attackers exploit them.

Introduction: The Digital Transformation Trap

Portfolio companies are rapidly adopting web applications to modernize operations, improve customer experience, and support digital transformation. But inexperience with web technologies, reliance on third-party developers, and limited awareness of application-layer security risks create fertile ground for vulnerabilities.

Many IT teams are comfortable managing network and infrastructure security, but web applications present a different set of challenges, which are often overlooked until it's too late.

This white paper explores why web application penetration testing is essential for portfolio companies. It provides examples of the most common and severe risks and demonstrates how to get ahead of attackers with the right testing approach.

Web Apps: A Double-Edged Sword

Web applications are browser-based software tools that do more than display static content. They facilitate real-time, dynamic interactions such as e-commerce transactions, data input, and internal workflows. For portfolio companies, these tools are attractive because they:

- Are cost-effective to develop and deploy
- Can scale massively
- Are accessible across devices and platforms
- Support automation and customer self-service

But web apps also introduce significant risks, especially when built by outsourced or inexperienced teams. Web app security is often an unfamiliar domain, and vulnerabilities can remain hidden until exploited.

Portfolio-Wide Risk: A Single Point of Failure

PE firms encourage their portfolio companies to cross-sell, so they often use one another's CRMs, financial apps, and HR systems like timesheet or payroll apps. While efficient and synergistic, this practice introduces systemic risk. One vulnerable app can expose the entire network of companies to devastating consequences, ironically counteracting the diversification that is the underlying logic behind portfolios.

Consider a financial, communications or HR tool built by one company in the portfolio and adopted by ten others. If it contains an access control flaw or vulnerable component, a breach in one company could cascade to all.

Attackers are increasingly targeting mid-sized firms with limited defenses but strong business ties and deep pockets—making lateral movement between companies easier and more lucrative.

Real-World Examples: What Can Go Wrong

The following are recent examples of issues identified in web app pentestests of mid-market portfolio companies conducted by Atumcell.

Privilege Escalation to Super Admin

- A user modified a hidden isSuperAdmin flag in an API request and gained full admin access.
- Impact: Full system compromise, data manipulation, and unrestricted access to corporate resources.

Privilege Escalation to Super Admin

- The password reset link was exposed in the HTTP response instead of being emailed, allowing attackers to hijack any account, including administrators.
- Impact: Complete account takeover, access to sensitive dashboards, and potential internal fraud.

Unauthenticated Access to Sensitive Employee Data

- A timecard management tool failed to enforce backend authentication, exposing employee PII and HR data via unauthenticated requests.
- Impact: Data breach, regulatory non-compliance, and reputational damage.

Broken Object-Level Authorization (BOLA)

- Users could manipulate object IDs in API requests to view or modify other users' records.
- Impact: Confidential data exposure, customer impersonation, and business logic abuse.

These incidents can result in:

- Regulatory fines (e.g., GDPR, HIPAA)
- Stalled M&A or IPO activity
- Depressed valuations

Why Penetration Testing Is Essential

A thorough web application penetration test replicates the behavior of real-world attackers to expose vulnerabilities that static code review or automated scans can miss. For portfolio companies, it's a critical layer of due diligence and risk mitigation.

Key benefits:

- Identify critical vulnerabilities and business-specific threats
- Prioritize remediation based on impact
- Demonstrate security maturity to boards and buyers
- Build a security-first culture across the organization

What to Look for in a Penetration Testing Partner

- Deep experience in web application penetration testing—not just general cybersecurity
- Mastery of OWASP Top 10 and real-world attack techniques
- Actionable reporting with clear remediation guidance
- Flexibility to test apps at different stages of development
- Collaborative engagement model that supports DevOps cycles

At Atumcell, we specialize in in-depth web application penetration testing tailored to the needs of fast-growing, digitally transforming companies in private equity portfolios. Our team embodies the hacker’s perspective, focusing on meaningful findings. And we work directly with your developers to resolve them.

Typical pricing for a standalone web app penetration test ranges from $10,000 to $25,000, depending on app complexity and testing depth.

Take the Next Step:

Secure Your Investments

Web apps are central to modern business operations, but they're also among the most common entry points for attackers. With digital transformation accelerating, now is the time to ensure your applications—and your company—are protected.

Contact Atumcell CEO, David Williams d@atumcell.com or (617) 671-8810 to schedule a web application penetration test with Atumcell and get ahead of the next breach.

atumcell.com