XBOW

Customer Story

How XBOW Transformed PuppyGraph's Approach to Pentesting

April 2025

Before working with XBOW, we relied on a different pentest provider. Their findings lacked depth. Key vulnerabilities remained undetected, leaving us with a false sense of security.
Additionally, while we explored other security tools like SAST and DAST solutions, they didn't provide the same level of real-world attack simulation that a strong pentest should deliver.

PuppyGraph

Weimo Liu
CEO — PuppyGraph

Background

On January 31st, 2025, XBOW identified and reported a critical authentication bypass and remote code execution vulnerability in PuppyGraph. The PuppyGraph team promptly acknowledged the issue and released a patch—one that had gone unnoticed by their previous pentest provider.

The vulnerability had gone undetected because it existed in an unusual authentication edge case where failed login attempts returned both an error message and a valid JWT token in the same response payload.

XBOW's systematic approach thoroughly parsed JavaScript source maps to identify the token validation logic flaw in the authentication middleware where response formatting occurred before token invalidation checks. Impressed by the technical depth and autonomous nature of the assessment, PuppyGraph took notice and explored XBOW capabilities further.

Challenge

As a developer-first product with a modern attack surface, PuppyGraph operates at a rapid development pace while maintaining the highest security standards—an ongoing and complex challenge.

PuppyGraph serves customers such as Coinbase, Clarivate, Prevalent AI, and more who are in highly regulated, security- critical industries. These organizations handle sensitive data, making security a top priority for both PuppyGraph and its customers.

Solution

As proof-of-concept testing continued, XBOW identified and reported two critical RCE vulnerabilities to PuppyGraph on March 7, 2025. XBOW's findings reinforced the effectiveness of its approach, leading to a pivotal decision for PuppyGraph:

"After working with XBOW, it was clear that their approach to security was a much better fit for our needs. The depth of their testing, their expertise, and the clarity of their findings made them an invaluable security partner. As a result, we've decided to move all our pentesting needs to XBOW and shift from periodic assessments to a more continuous testing approach aligned with our release cycles."
— Danfeng Xu, CTO, PuppyGraph

This shift marked a fundamental change in PuppyGraph's security strategy—moving from traditional, point-in-time testing to a model that ensures vulnerabilities are continuously identified and addressed in sync with development. To further validate this model, PuppyGraph engaged with XBOW for a pentest ahead of one of their releases. In less than 2 days a full penetration test was conducted and a report was delivered.

Future

The speed of the pentest exceeded expectations, proving that security testing no longer needs to be a slow process. Looking ahead, PuppyGraph plans to expand its use of XBOW, making continuous pentesting a core pillar of its security strategy.

“With XBOW’s ongoing support, we’re confident in maintaining a strong security posture as we scale.” — Danfeng Xu, CTO, PuppyGraph

By adopting XBOW’s always-on testing, PuppyGraph is not only strengthening its own security posture but also reinforcing trust with its customers—ensuring their sensitive data remains protected as they scale.

About

XBOW is the autonomous offensive security company redefining cyber defense for the AI era. Combining AI reasoning with offensive security workflows, the XBOW platform delivers expert-level security testing at machine speed. XBOW empowers security teams to transform from reactive to proactive defense at AI scale. For XBOW customers, autonomous offense is the best defense. → xbow.com

PuppyGraph is the first and only real time, zero-ETL graph query engine in the market, empowering data teams to query existing relational data stores as a unified graph model in under 10 minutes, bypassing traditional graph databases' cost, latency, and maintenance hurdles. Capable of scaling with petabytes of data and executing complex 10-hop queries in seconds, PuppyGraph supports use cases from enhancing LLMs with knowledge graphs to fraud detection, cybersecurity and more. → puppygraph.com

Get Pentesting that keeps up with your development

Visit xbow.com/pentest to learn more