CHICAGO BOOTH

The University of Chicago Booth School of Business

AI and Financial Information
BUSN 30135-01 (Winter 2025)

Neural Strike

Bohren, Christian
Fernandes, Terence
Lupercal, Caesar
Saygaonkar, Prathamesh

Humorous Judicious Cobra Launches AI Powered Cybersecurity Automation Platform

Online Press Release [FOR IMMEDIATE RELEASE]

Chicago, Mar 13 2025 — Neural-Strike, an innovative AI-driven cybersecurity platform developed by Chicago Booth MBA students, is now live. This cutting-edge solution integrates offensive and defensive security operations into a unified ecosystem powered by advanced AI models. Neural-Strike empowers organizations to automate penetration testing, simulate cyberattacks, and enhance defensive strategies with unprecedented efficiency. By bridging offense and defense workflows, Neural-Strike aims to streamline vulnerability detection, reduce manual effort, and improve security response capabilities for organizations of all sizes. Its fully automated process yields incredible efficiency gains, allowing your organization to grow faster, in a more secure way, the Neural Strike way.

AI is revolutionizing the way attackers can exploit vulnerabilities across your organizations. Can you *really* afford to use outdated methodologies to protect against those?

Let us show you how we can help by contacting us at hello@neuralstrike.ai.

What is Neural-Strike?

Neural Strike is the first platform to seamlessly unify offensive (Red Team) and defensive (Blue Team) security operations through AI-driven automation. Unlike traditional tools, it dynamically generates tailored penetration testing methodologies and actionable scripts using cutting-edge cybersecurity tools, aligning with industry standards like OWASP, ATT&CK, and NIST. Its modular architecture supports integration with multiple AI providers—including OpenAI, Anthropic, and local LLMs—ensuring adaptable, high-precision security testing, even in isolated environments.

Available on Mac, Windows, and Linux, Neural Strike delivers a truly customizable, next-generation approach to cybersecurity.

Core Features

Unified Offense and Defense
Gone are the days of siloed red and blue teams. Neural Strike brings them together on a single platform, enabling faster, more efficient, and truly collaborative security operations. It can simultaneously assess vulnerabilities on the offensive side while generating a tailored defensive strategy based on your organization's unique environment and assets. With Neural Strike, cybersecurity teams can focus on identifying and responding to threats faster than ever before.

Always Up-to-Date
Cybersecurity testing no longer relies on static knowledge requiring cumbersome updates and long ramp-up training. With its flexible architecture supporting the latest LLM models through an intuitive API key management interface, Neural Strike ensures continuous access to the most accurate methodologies and tools.

Integrated RAG-Powered Chatbot
Neural Strike includes an interactive assistant leveraging Retrieval Augmented Generation (RAG) to provide instant responses to user queries regarding functionalities, security recommendations, and implementation guidance.

Interactive Training Platform
Neural Strike reduces training costs and ramp-up times by adapting to user expertise—breaking down cryptography for entry-level analysts while supporting advanced scripting and edge cases for senior professionals. Every resource gets exactly the insights they need, right when they need them.

Compliance Guru
Neural Strike automates compliance audits, aligning with the latest regulatory requirements (GDPR, CCPA, PCI DSS, HIPAA) while generating auditor-ready reports. Security Compliance teams can operate more efficiently, reducing operational costs by at least **35%**.

Why Trust Neural-Strike?

Security Talent Shortage Means Automation is Key
The 2024 ISC2 Workforce Study highlights a 5.4M global shortage of security specialists. Neural Strike mitigates this by offering intelligent automation, reducing onboarding costs, and enabling teams to focus on high-priority threats. Beta tests showed analysts saving **60-90%** of assessment time.

Expanding Attack Surface Requires a Smarter Approach

Cloud services, IoT, and AI-driven attacks have exponentially increased security risks. Neural Strike evolves with these threats, providing *continuous, adaptive security* while empowering employees to focus on complex challenges.

Competitive Differentiation: More Than Just Another Security Tool

Unlike traditional vendors that separate offensive and defensive security, Neural Strike unifies both within a single AI-powered workflow. This enables seamless collaboration across cybersecurity analysts, developers, and DevOps teams while ensuring security decisions are informed by real-time offensive and defensive data points.

Neural Strike isn't just another security tool—i*t's an **entirely new way** of thinking about cybersecurity*!

Go-To-Market Approach

Sales Strategy

Neural Strike will be distributed through:

- **Strategic Partnerships**: Google Cloud, AWS, and DigitalOcean enable scalable, integrated security solutions.
- **Government Contracts**: Designed for high-security environments, with user-controlled local models ensuring total agency control.
- **Direct Online Sales**: A lead-driven model ensures seamless integration for businesses of all sizes.

Market Expansion Plan

Neural Strike will be launching first in the US and Canada, expanding to Asia and Europe within two years to achieve full global support. This focused strategy allows for rapid growth while building a strong customer foundation.

Revenue Model

Neural Strike follows a subscription-based pricing model, with tiers based on features and support level. Unlike traditional penetration testing services costing $30K+ per engagement, Neural Strike provides unlimited testing at a fraction of the cost.

Benchmarking and Evaluation of AI Models

We benchmarked multiple AI models to ensure Neural Strike delivers the most effective security solutions.

Our evaluations included OpenAI 4o mini, Ollama 3.3, and Claude 3.7, with Claude 3.7's thinking model producing the most actionable results, as judged by the two cybersecurity experts on our team. Since Neural Strike allows users to choose their preferred AI models, flexibility remains a cornerstone of our approach so benchmarking is informative in terms of showcasing the viability of our product but customers will tailor it to their needs.

It's worth noting however, that Ollama 3.3 struggled with script generation, a limitation we are actively investigating with potentially system prompt changes and the addition of a model-specific additional training with OS-specific scripting best-practices.

FAQ

How does Neural Strike ensure its AI models stay up-to-date?
Neural Strike continuously integrates new cybersecurity threat intelligence and supports API-based model updates from OpenAI, Anthropic, and other providers.

Can Neural Strike operate in air-gapped or highly regulated environments?
Yes, Neural Strike supports local LLM deployment, ensuring full control and compliance for organizations handling sensitive data.

What industries can benefit the most from Neural Strike?
Neural Strike is designed for finance, healthcare, critical infrastructure, and government organizations, where real-time security adaptation is critical.

How does Neural Strike compare to traditional consulting-based security assessments?
Unlike Accenture or KPMG's point-in-time audits, Neural Strike provides continuous, automated security testing, reducing cost and response times.

What integrations does Neural Strike support?
Neural Strike seamlessly integrates with CI/CD pipelines, cloud providers (AWS, Azure, GCP), and major SIEM solutions.
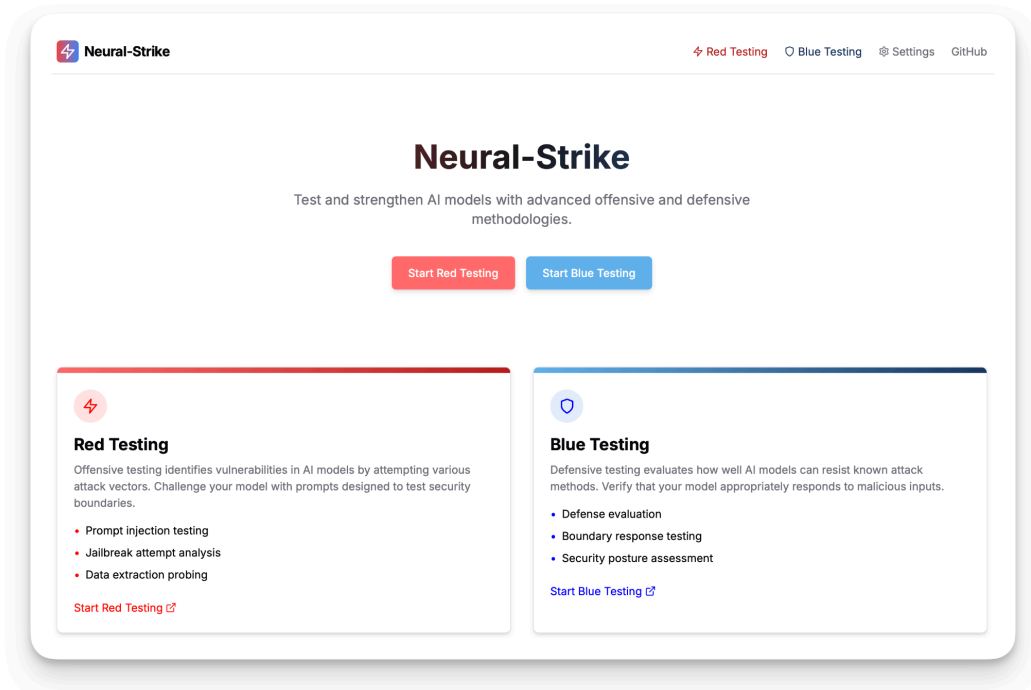
Example Outputs:
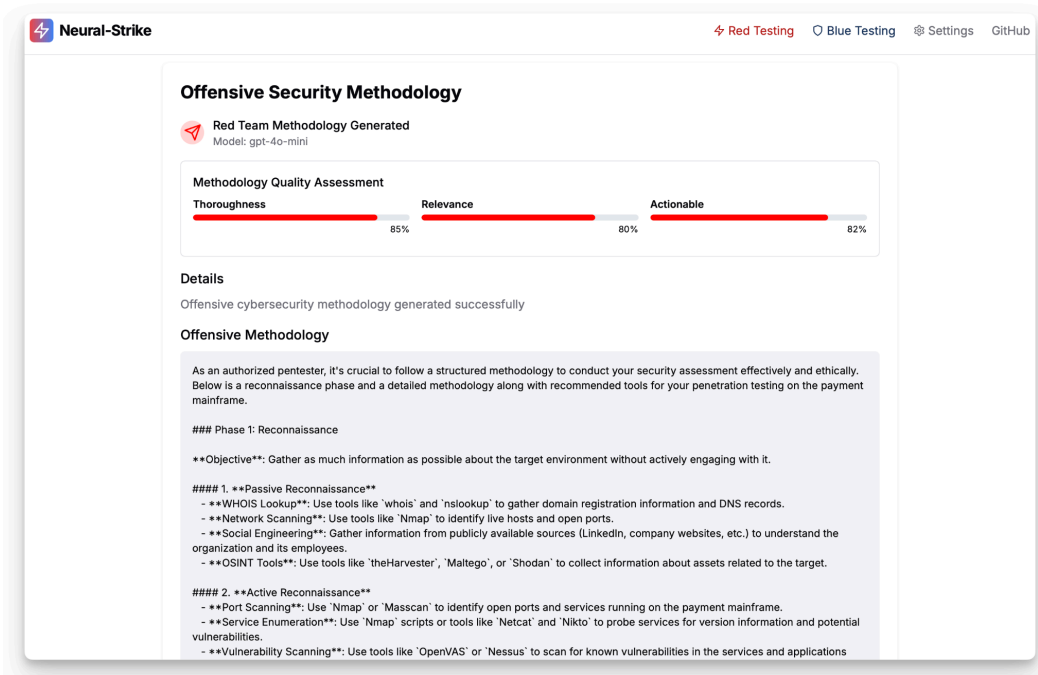

Fig 1: Neural Strike Main Interface
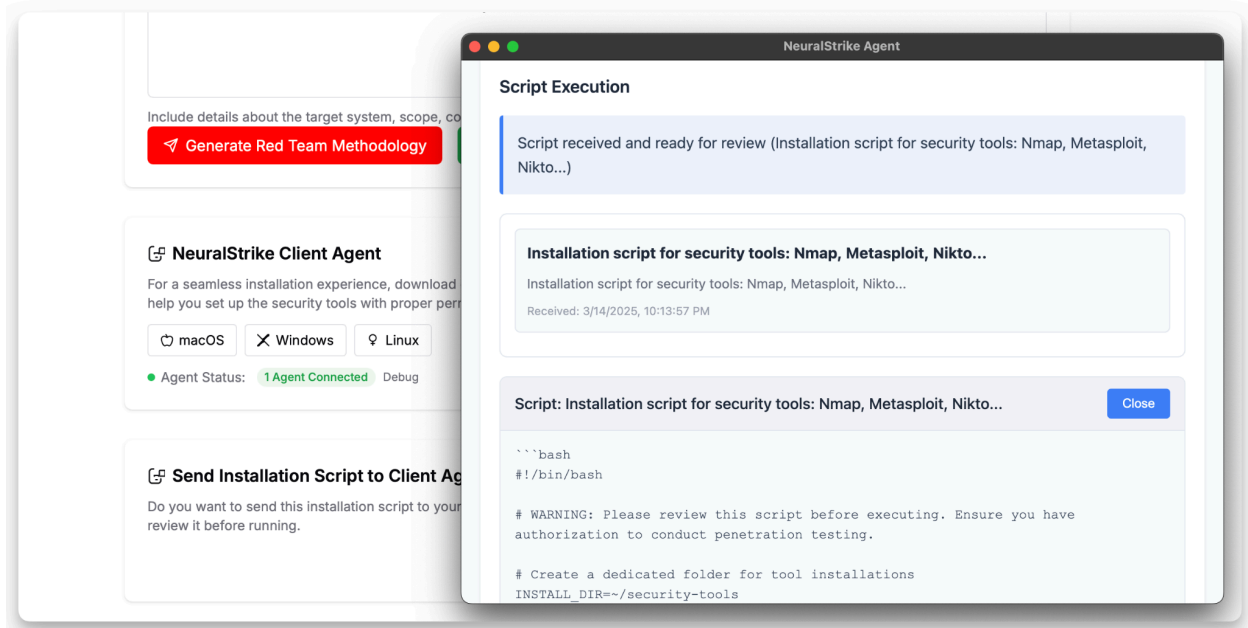

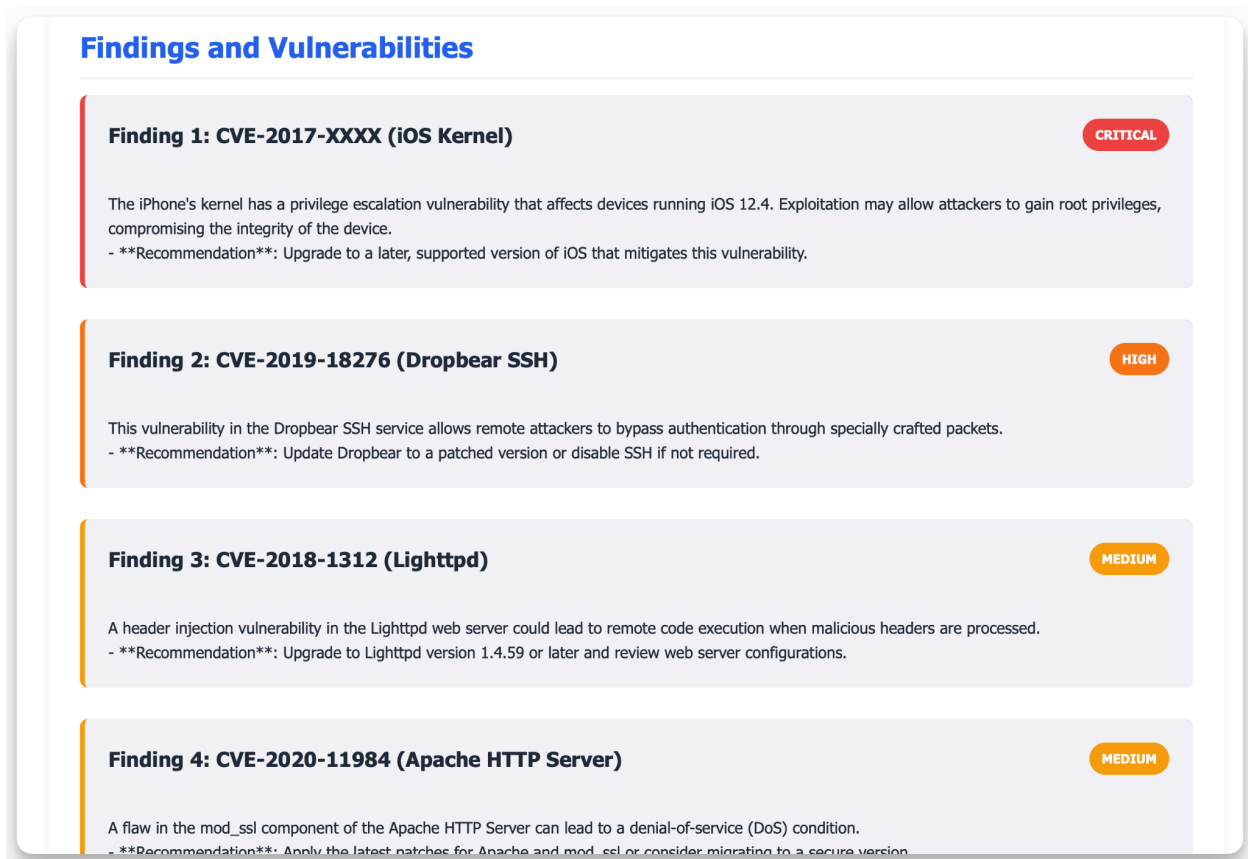Fig 2: Methodology Generation

Fig 3: Script Generation & Local Agent Execution

Fig 4: Tailored & Actionable Report Generation