Application security assessment: Hugging Face Gradio

Hugging Face hired Trail of Bits to assess Gradio's security before releasing version 5.0 of their popular machine-learning platform.

The assessment included:

4	engineer-weeks of review
27	identified security issues across Python, JavaScript, and Go codebases
	Evaluated local deployments, server implementations, and sharing infrastructure
	Validated remediation of all findings before public release

> The Trail of Bits security team was fantastic and the review exceeded our expectations in speed and depth.
>
> Within 2 weeks, they not only got up-to-speed with our relatively large codebase, which spans Python, JavaScript, and Go, but they identified many security issues that required a deep understanding of how Gradio and Hugging Face are used in practice to build machine learning apps"
>
> **Hugging Face** on working with Trail of Bits

The assessment focused on security across four critical scenarios:

- Local development environments
- Production deployments on Hugging Face Spaces
- Built-in share link functionality
- CI/CD pipeline security

Why Trail of Bits for securing AI/ML systems

AI/ML security expertise

Vulnerabilities in AI/ML systems differ significantly from traditional software bugs, and you need a team with specialized expertise to find them.

"From the outset, Trail of Bits demonstrated a deep understanding of Gradio, the machine learning ecosystem, and the nuances of web security. They asked thoughtful questions about Gradio's use cases and were transparent about the scope of their audit."

Practical security solutions

Trail of Bits understands that security recommendations must work within our clients' real-world constraints and user expectations. Our solutions balance strong security controls with practical implementation, considering how teams and their users will interact with the system.

"The Trail of Bits team worked closely with us to devise effective mitigation strategies, ensuring that our security enhancements did not compromise the ease of use that is core to Gradio's appeal. This collaborative approach validated our choice and resulted in a productive and rewarding partnership."

Building trust in open-source

Independent security assessments help open-source projects establish a security baseline as they grow to serve more users and use cases.

"The comprehensive review of Gradio's architecture by Trail of Bits significantly influenced our overall security design. Their findings and recommendations allowed us to make informed decisions that enhanced the robustness of the platform."

About Gradio

Gradio is an open-source platform that allows developers to quickly build and scale web applications for machine learning use cases.

- **6M+** monthly PyPI installs
- **470k+** Gradio apps on Hugging Face Spaces
- **35k** GitHub stars

> Over the years, we've prioritized improving our internal security processes and standards. The audits by Trail of Bits are a consequence of this larger commitment to security"
>
> Hugging Face on working with Trail of Bits

Learn from our Gradio audit: Security reports, blogs & tools

PUBLIC REPORTS:

- Hugging Face Gradio report
- Hugging Face Safe Tensors report

BLOGS:

- Auditing Gradio 5, Hugging Face's ML GUI framework
- A Security Review of Gradio 5

TOOLS:

- SARIF Explorer
- Semgrep
- WeAudit
- CodeQL
- Burp Suite Professional
- Regexploit

gradio

Empowering ML innovation with security-minded development, informed by Trail of Bits' independent assessment.