

Is AI-Generated Code Secure?

Key Findings from the 2026 GenAI Code Security Report



HOW SECURE IS THE CODE GENERATED BY AI?

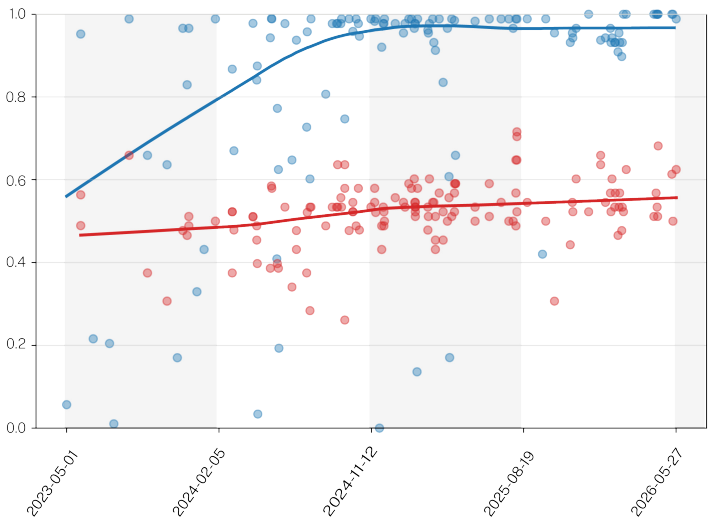
AI is writing far more code than ever before.
Security is not improving at the same pace.

Across our testing,
44% of AI code generation tasks produced code with a risky vulnerability.



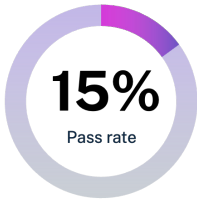
That rate has barely moved since this research began. What has changed is the scale. The risk isn't theoretical, and now it's entering production at much higher volume.

Syntax Pass Rate • Security Pass Rate



WHAT KIND OF VULNERABILITIES ARE BEING GENERATED, AND HOW BAD ARE THEY?

85% of the time, AI failed to secure code against Cross-Site Scripting (CWE-80).



15% pass rate against Cross-Site Scripting (CWE-80)

This is one example; read the report for more.

CWE	Type	Severity	Common Threats	Remediation Priority
CWE-80	XSS Injection	High	User session theft, malware delivery	Critical

ARE NEWER, BIGGER AI MODELS MORE SECURE?

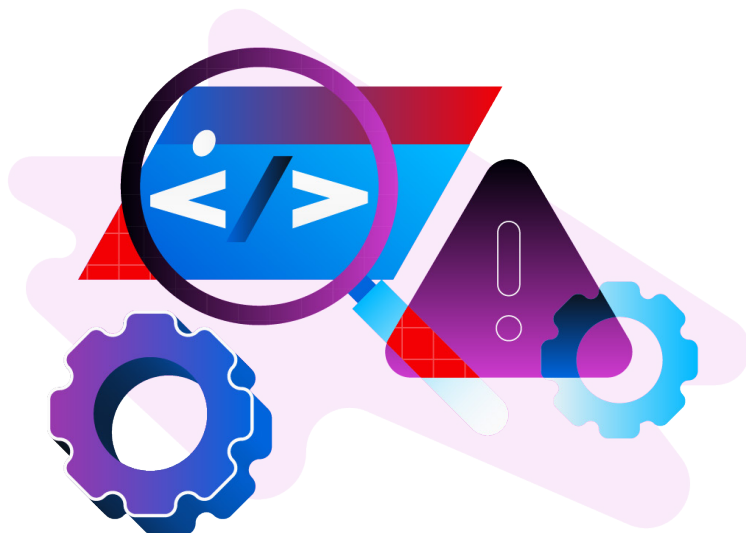
No. Size has essentially no effect: large 53%, medium 51%, small 51%.

DOES IT MATTER WHICH MODEL YOU PICK?

Yes. GPT-5.5 leads at 68%; six of eleven models cluster at 50–53%.

- Reasoning models edge ahead: 56% vs. 51%
- Coding-specialized ≠ safer: 51% vs. 52%
- Even the best got worse: last year's leader was 72%

Model selection has quietly become a security decision.



Secure adoption is not about shutting AI down. It is about making safe use repeatable, visible, and provable.

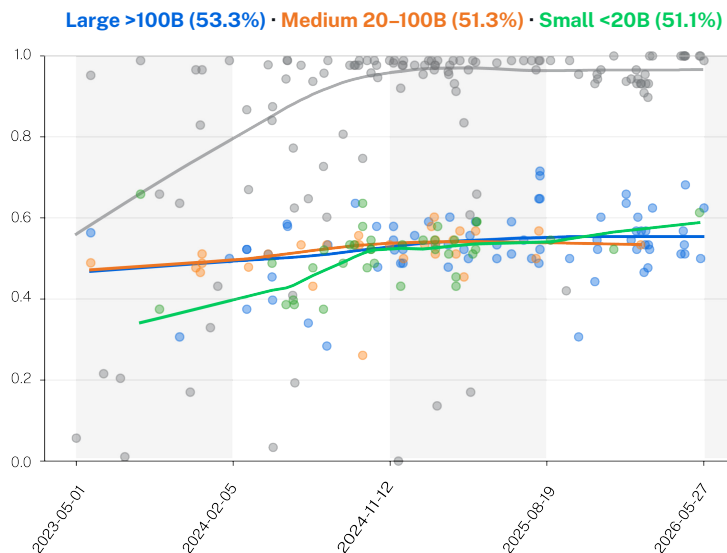
READ THE REPORT

See which models performed best, where the biggest risk gaps remain, and what it takes to build trust into AI-assisted software delivery.

Download the full report at: veracode.com/ai-report

VERACODE

This report is for informational purposes only and does not constitute legal, technical, or other professional advice. The information contained herein is based on data available to Veracode as of the date of publication and is subject to change without notice. © Veracode 2026. All rights reserved.



WHAT DOES ALL THIS MEAN?

AI now authors roughly **half of all committed code**. The same 44% failure rate applies to half a codebase, at a pace no security team can match. Syntax is solved at 99.9%. Security is not.

WHAT LEADERS SHOULD DO NEXT

- Enable AI coding with controls, not caution tape.
- Choose models with security performance in mind.
- Verify AI-generated code before it moves downstream.
- Prioritize findings so teams focus on what matters most.
- Build traceability into the workflow.
- Strengthen governance across developers, security, and risk teams.

