

SVG Sanitization Guide

SVG Security: Preventing XSS & Injection Attacks

About This Document

This reference accompanies the article: SVG Security: Preventing XSS & Injection Attacks

Read the full article at: <https://svgeneration.com/docs/svg-security-best-practices>

Article Summary

How to safely handle user-supplied SVG, prevent cross-site scripting via SVG vectors, and sanitize pattern inputs.

The SVG SSRF Risk

Server-Side Request Forgery (SSRF) via SVG: if your server processes uploaded SVG files (e.g., to generate thumbnails), a malicious SVG can reference internal services via `<img href="http://169.254.169.254/latest/meta-data/">` (AWS metadata endpoint). Always process SVG files in a sandboxed environment (containerized, no network access) and strip all external references before processing.

Secure Pattern Generation Pipeline

Build SVG patterns programmatically from whitelisted components never via string interpolation of user input. Accept only primitive values (colour hex, numeric scale, pattern type identifier), validate each input individually, build the SVG using a templating system with proper escaping, and base64-encode the result. User input should never reach the SVG markup level directly.

Free Resources

Visit SVGeneration.com for 600 free SVG background patterns. No attribution required.

License: Modified MIT License. Use freely in personal and commercial projects.