

Introduction

CVE-2026-5026 is a recently disclosed vulnerability (2026) that highlights a critical security issue in modern web applications: the unsafe handling of **SVG (Scalable Vector Graphics)** files during upload and rendering.

SVG files are **XML-based documents** that can contain active content, such as JavaScript code and event handlers, in contrast to conventional picture formats like JPEG or PNG. These files may serve as a vector for **Cross-Site Scripting (XSS)** attacks if they are not properly verified.

In affected systems, applications allow users to upload SVG files and subsequently render them in the browser without sanitizing their contents. As a result, attackers are able to inject malicious scripts inside the SVG file. When another user or an administrator views the uploaded image, the embedded script is run within the web application.

This vulnerability is classified as **Stored XSS**, since the malicious payload is permanently stored on the server and automatically executed when accessed. Such attacks may have serious consequences, including:

- Session hijacking through cookie theft;
- Sensitive data exposure;
- Full compromise of user accounts (especially administrative accounts);

CVE-2026-5026 reflects a broader class of vulnerabilities where developers mistakenly treat all image formats as passive content. It emphasizes the importance of **strict input validation, content sanitization, and secure file handling practices** in web applications. The goal of this lab is to demonstrate how this vulnerability can be exploited in practice. By completing it, students will:

- Understand how XSS attacks work in non-traditional contexts;
- Learn how file upload features can introduce security risks;
- Perform a real attack to extract sensitive data (flag);
- Propose and implement mitigation strategies.