Cross Site Scripting (XSS) via Malicious File Upload

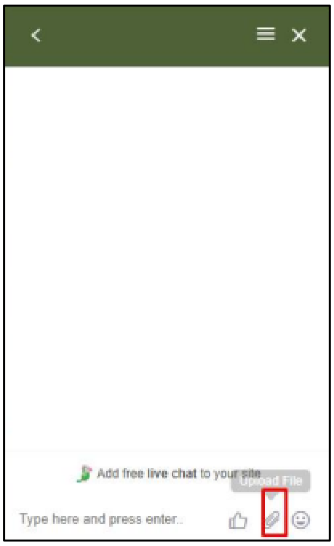
File upload is a function used to allow users to interact with a specific web page and upload various data/files. But instead of uploading the actual file an attacker uploads some malicious file which result in total compromise of the system . Many client side and server side attacks can happen due to unrestricted file upload.

Client-side attacks like Cross Site Scripting (XSS) or Cross Site Content Hijacking and Server-side attacks includes File Inclusion attacks, Remote code execution etc.

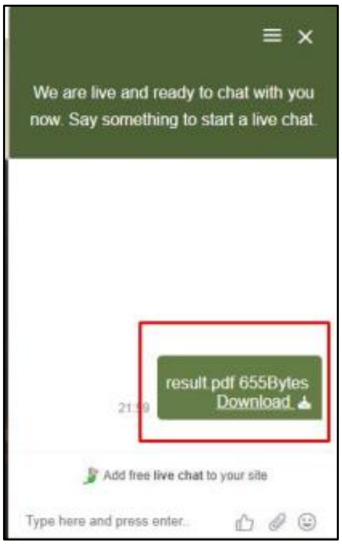
The impact of Malicious File Upload vulnerability is high.

Proof of Concepts

Step 1: - Observe the highlighted part there is an Upload button.



Step 2: - Upload a Malicious file named as result.pdf

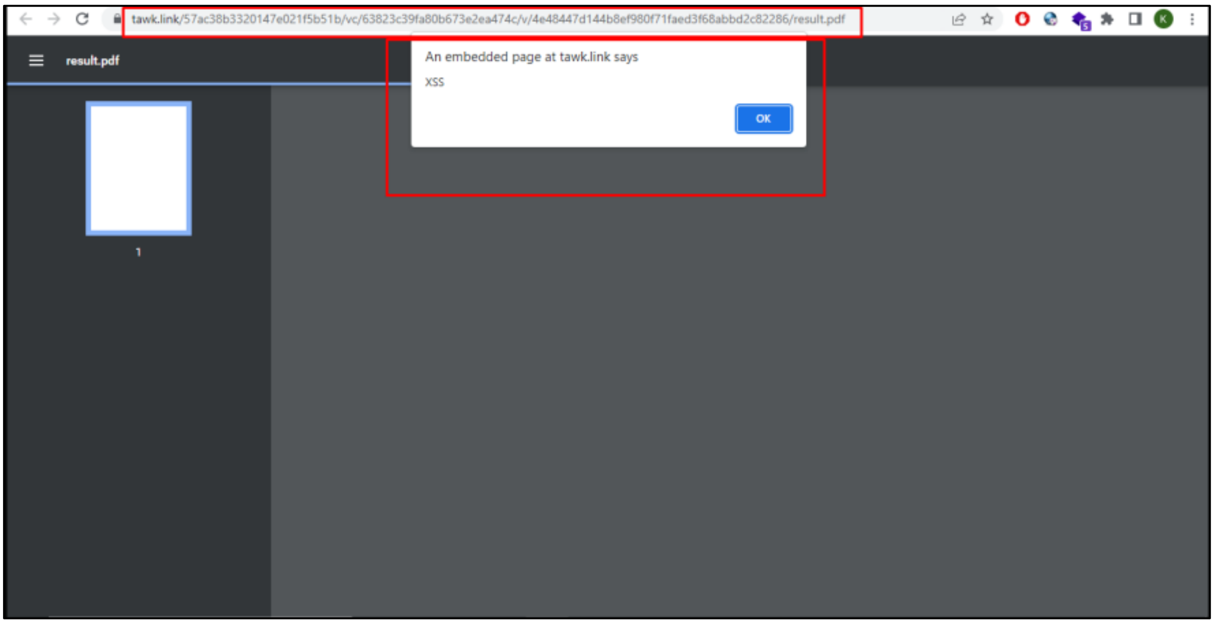


We are live and ready to chat with you now. Say something to start a live chat.

result.pdf 655Bytes
Download

21:59

Step 3: - Click on download and as shown below Cross Site Scripting (XSS) payload executed successfully.



tawk.link/57ac38b3320147e021f5b51b/vc/63823c39fa80b673e2ea474c/v/4e48447d144b8ef980f71faed3f68abbd2c82286/result.pdf

An embedded page at tawk.link says

XSS