

Forum:[Hack Forums](#)

Thread: [XSS with SVG file upload](#)

0xcitizen - February 20, 2023, 11:34 am

Hi everyone.

I have been hacking on a bug bounty program on HackerOne and on this particular program there is a functionality to create your team.

When you create your team you can upload a logo for that team. The web app does not allow SVG uploads, so I made the file with SVG content added some javascript to it and saved it as JPG and I uploaded it.

Then I went to Burp and sent that request to the Repeater changed the extension of the file from JPG to SVG and sent the request again it was accepted I got back 201 Created.

The photo cannot be opened by just clicking on the photo like on Facebook for example but if you want to open a photo you have to open it in new tab or click onto the image link and when the user does that my javascript code executes.

Now the problem is that this photo opens on a "randomtext/cloudfront.net/randomtext/mypayload.svg" there is no cookies on that website so I can't steal the session.

Then I wrote javascript code that redirects the user to a "malicious" website when he opens a photo or clicks on image link and everything works, the user gets redirected.

My question is if I can report this as a Open Redirect vulnerability, or if any of you guys have any suggestions how I can escalate this any other way.

Thanks.