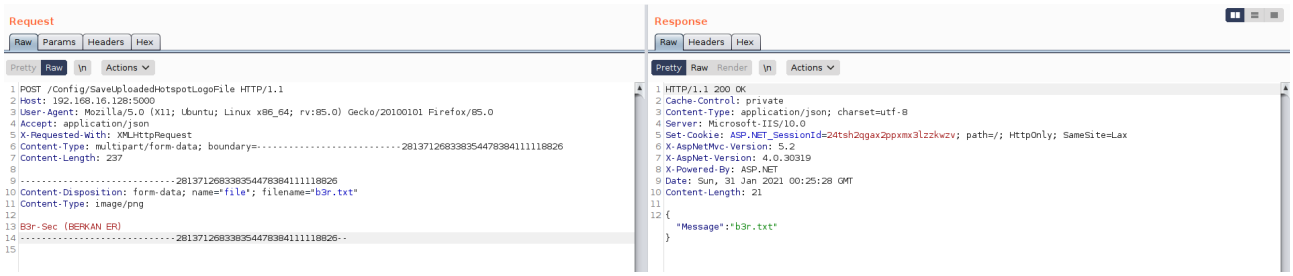
FortiLogger | Log and Report System - Unauthenticated Arbitrary File Upload (Metasploit)

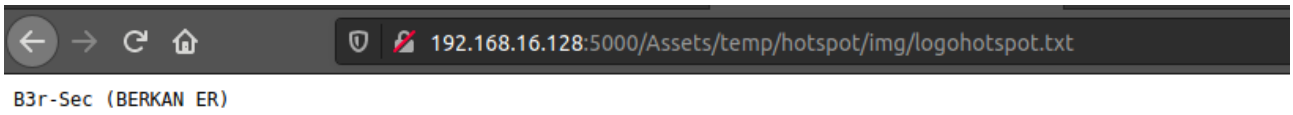
Berkan ER (b3rsec@protonmail.com)- 30/01/2021

This vulnerability found on upload a company logo under “Hotspot Settings” (http://192.168.16.128:5000/config/hotspotsettings).

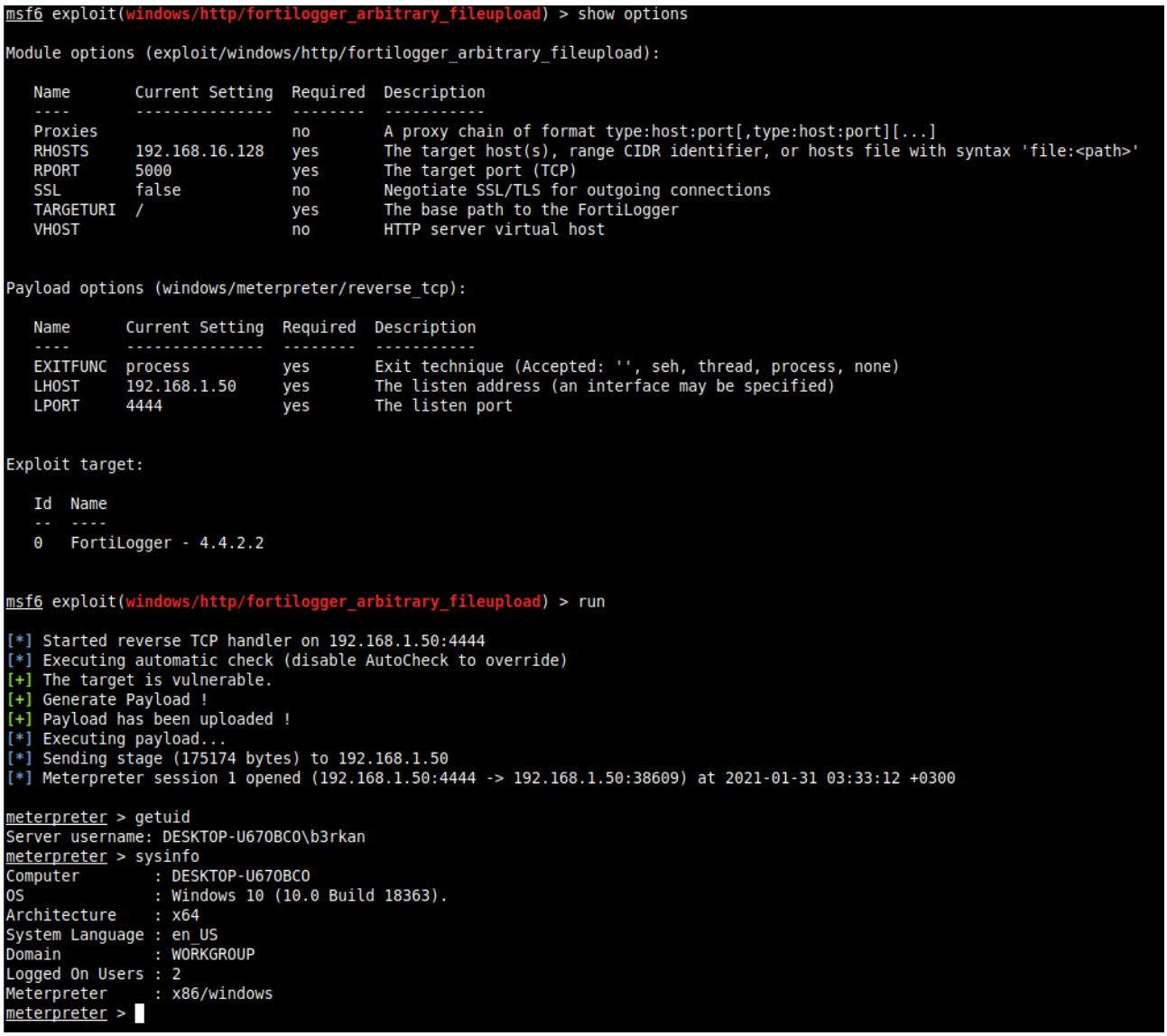
An anonymous user can be send a file without any authentication or session header with POST request to “/Config/SaveUploadedHotspotLogoFile”



This file is upload under “C:\Program Files\RZK\Fortilogger\Web\Assets\temp\hotspot\img” destination with “logonhotspot” name without controlling file extention or content.



Using this vulnerability, I uploaded a malicious file and accessed the remote server where the application was running.



POC:

https://asciinema.org/a/388098