RootMe Try Hack Me Walkthrough

This is a simple machine to hack for beginners too.

- ***Step 1:*** Enumeration

  We get two ports open ie. 22 and 80 with their common services running. There is a website on port 80 which gives us nothing significant

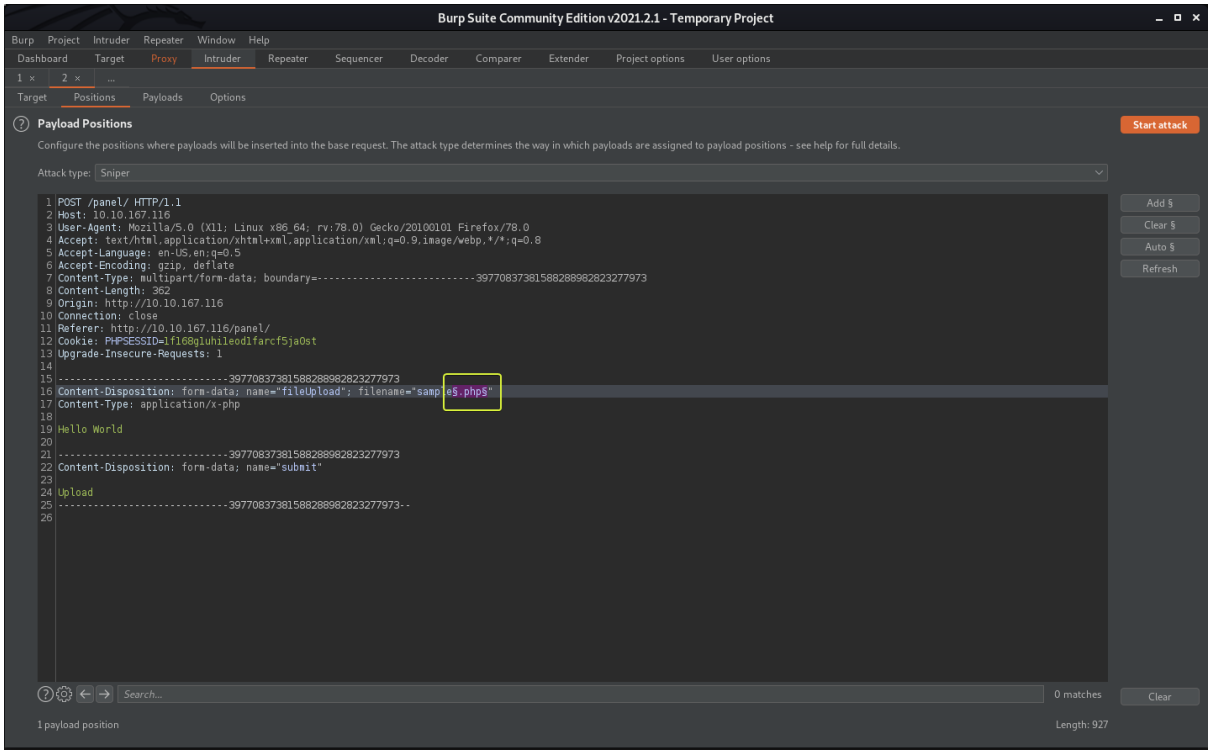
- ***Step 2:*** Directory Bruteforcing

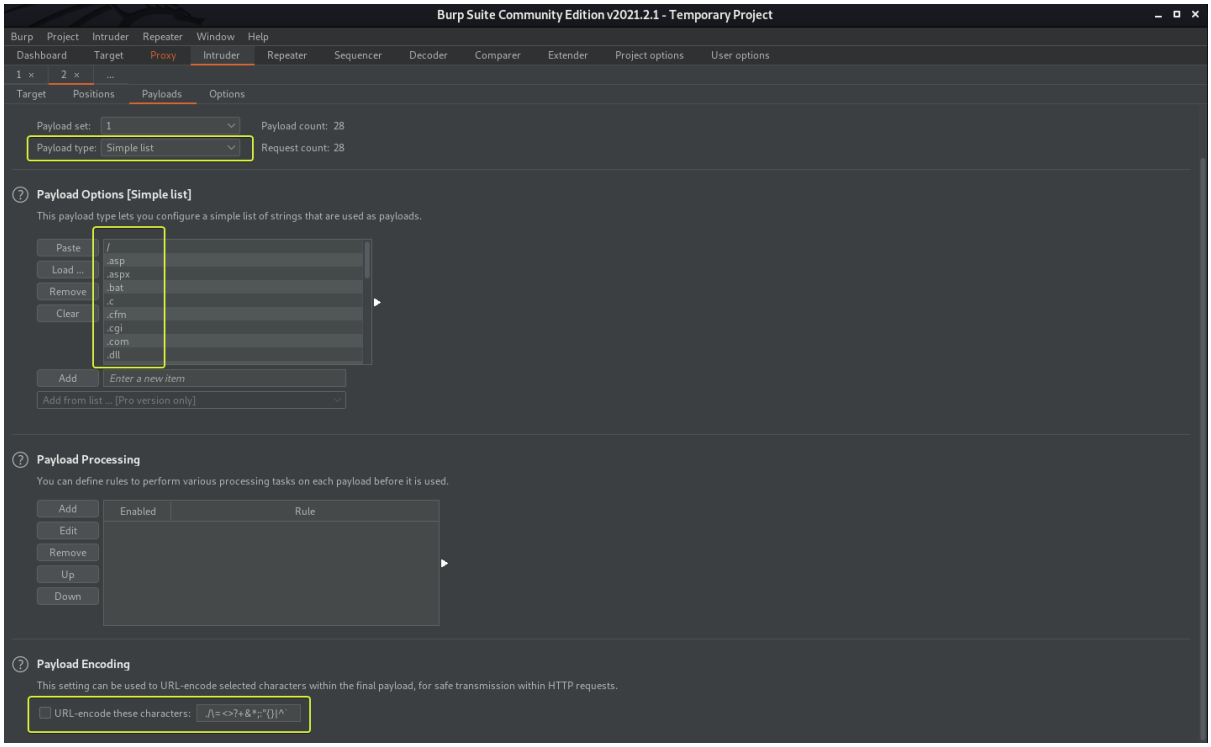
  Using gobuster we bruteforce directories and get a */panel/* directory in which upon navigating to it we get a file upload service shown. This is a good scenario to check for a reverse shell upload.

- ***Step 3:*** Reverse Shell

  Here we can try the various file extensions possible and try to get a connection back to our kali machine. We can manually test the different file extensions but it would become tedious after some point, so we will be using Burpsuite for this. Capture the upload request made to the website using burpsuite and send it to the Intruder. We will now test the various file extensions by fuzzing.

  The steps are:

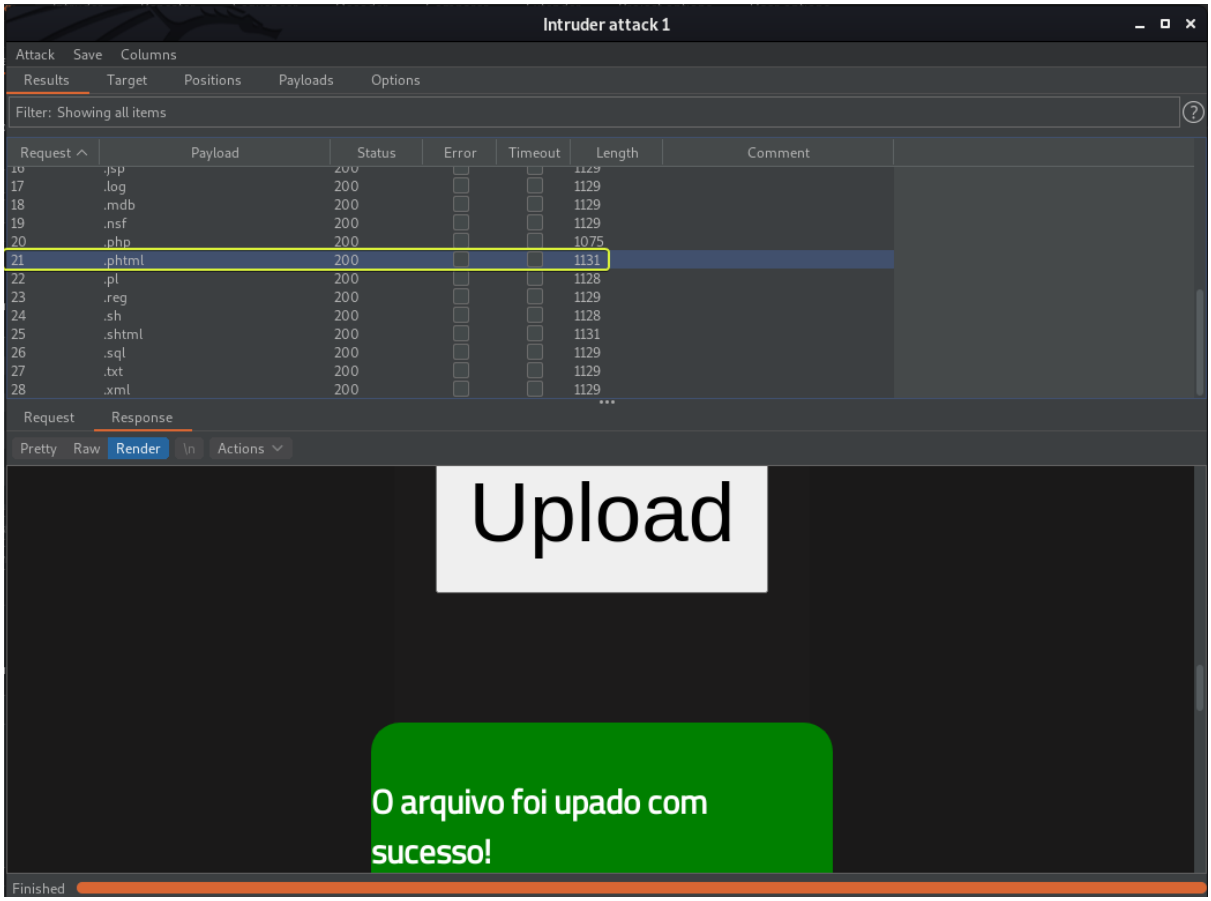




Under the payloads tab. Select a wordlist to use for fuzzing. Here I am making use of the wfuzz common extensions wordlist which is located at /usr/share/wordlists/wfuzz/general/extensions_common.txt on Kali Linux.

Note: Ensure to deselect the URL-encode these characters option else the fuzzing is not going to work properly.

.phtml works in this case



https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

This php reverse shell can be used with the file extension .phtml and with modified parameters. When this file is successfully uploaded we get a reverse connection back to our kali machine.

- ***Step 4:*** Flag searching

We have to now find a *user.txt* file on the system and to do so we will be using the f*ind / -type f -name user.txt 2>/dev/null* command to get us the results */var/www file located.*

- ***Step 5:*** Privilege Escalation

Privilege Escalation here is going to be done by abusing the SUID permission. To get all the files having their SUID permissions to execute we type the command

find / -type f -user root -perm -4000 2>/dev/null

We get */usr/bin/python* to have SUID permissions to execute and we will use it to leverage our permissions. Go to https://gtfobins.github.io/ and search for python and SUID to get the command for privesc. The command will differ based on the version of python installed which can be checked by typing *python –version*. As the binary works we get our root permissions. There is a flag *root.txt* in the root directory.