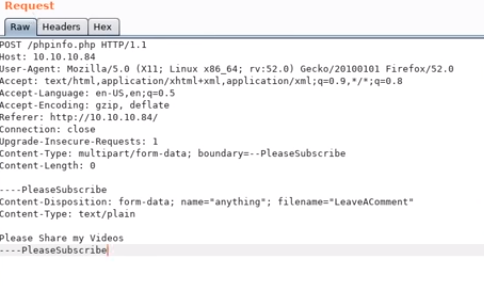
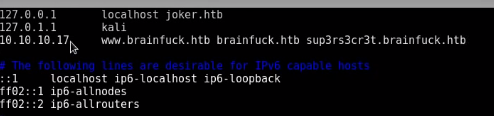
**IMPORTANT POINTS**

* Nmap: **nmap –sC –sV –oA test.txt <ip>**
* To see for sudo mispermissions: **sudo –l**
* Don’t use hydra without knowing the blacklist policy.
* GOBUSTER:  **gobuster –w <location of the worldlist> -u <url> -k –x<file formats ,eg .txt>**
* Wordlist: /usr/share/dirbuster/directory-list-2.3-medium.txt
* **-k =>** ignore ssl while using https websites
* To check for bad character in url command execution type env to get enviroinmental variable and use **+** for space(tjnull:- sensei) (url encode=> ctrl+u)
* X[13]=> {x:13:1} (bash)
* To run a vulnerability scanner in nmap : nmap --script vuln <ip>
* To understand a exploit in a easy way :  **xkcd** => website
* To decode base 64: echo –n <text> |base 64 –d
* To convert to base 64 in the url: file?= php://filter/convert.base64.encode/resource=ini.php
* TO upload: repeater =>**right click =>change request method** ,in request content type=mutipart/form-data. EG
* **PS:** running processes **, netstat –na** : listening ports
* Use the security certificates for more info in https. To add ip to host name: /etc/hosts
* Smbclient: smbclient –l//<ip>
* python -c 'import pty; pty.spawn("/bin/bash")'
* to check all files having suid : find / -perm -u=s -type f 2>/dev/null
* Wordpress scanner: wpscan
* Email client(unknowm smtp server):evolution
* Cipher decoding: rumpkin=>one pad
* Chmod +600 for ssh key
* Dnslookup:- dig akfr @<ip> crons.htb
* Website for reverse shell: pentset monkey reverse shell chaet sheet
* To run powershell script(file based) 
* Sherlock powershell.
* 
* `power shell s: nisangs

**For ftp we can use hydra to enumerate or brute force**

**Shell upgrade:**

**python -c 'import pty; pty.spawn("/bin/bash")'**

**export TERM=xterm**

**stty raw -echo; fg**