Analyze the binary (200):

1) We clicked on runme.exe and nothing executed, so we ran *file runme.exe* in the terminal and found that it was a tcpdump capture file.
2) Opened the file in Wireshark and filtered using "tcp contains key".
3) Found 2 packets: one which contained the instructions found by following the TCP stream and one that was the video file that we exported. The first packet instructions said:
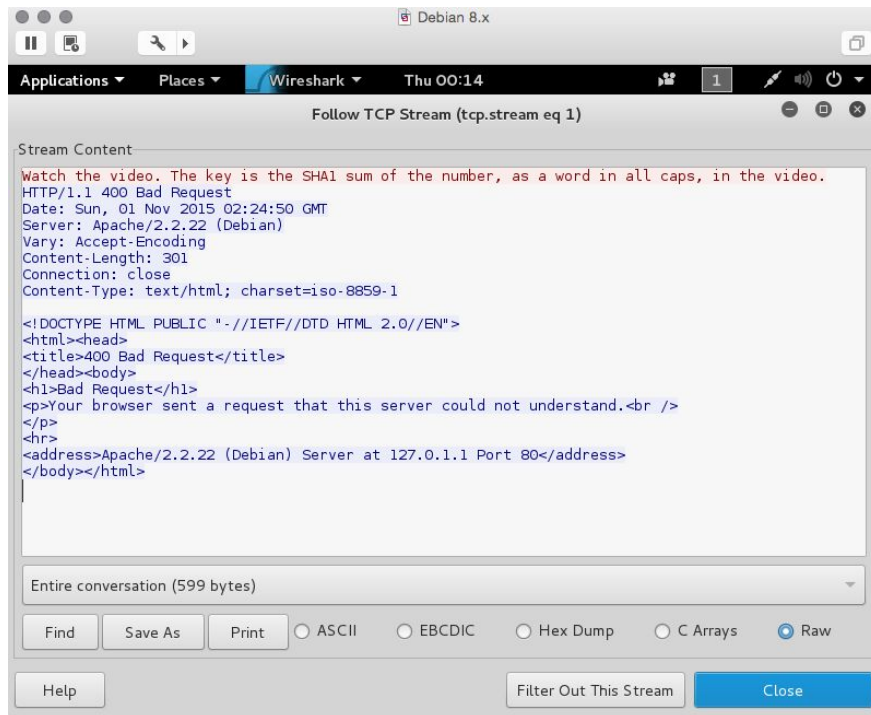
4) We extracted the mp4 file from the stream.
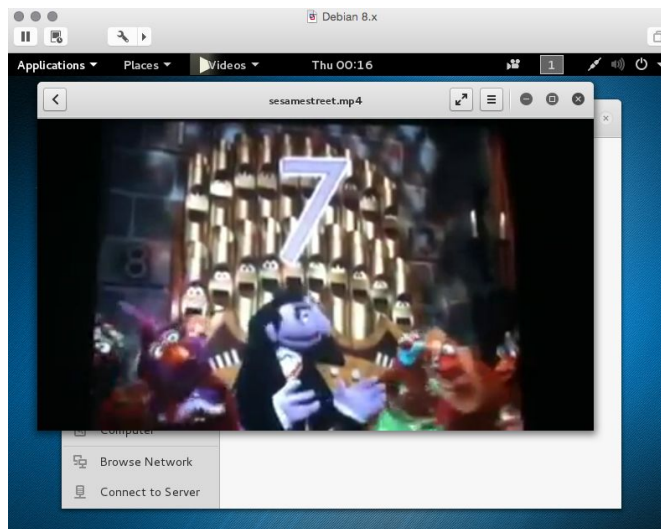
5) Put the string "SEVEN" into a SHA1 hash generator and found the flag was the generated hash. (www.timestampgenerator.com/tools/sha1-generator/)

Convert text to SHA1

Text to convert

```
SEVEN
```

Generate SHA1

SHA1 Hash

```
cabd534c35ee6a39365f4ed3bce4eafdcc3d4b8d
```

Unnecessary Service (100):

1) Ran *nmap -sS 67.23.79.113* to see what ports were open.
2) Looked for unnecessary services on open ports, found FTP on port 21.
3) FTPed to the server ip.
4) Got the key as a response.

```
                              root@kali: ~                          ─ □ ✕
File  Edit  View  Search  Terminal  Help
crackedpasswords  Downloads      Pictures   Templates
Desktop           hydra.restore  Public     Untitled Folder
root@kali:~# nmap -sS 67.23.79.113

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-09 19:40 EST
Nmap scan report for www.pupcast.com (67.23.79.113)
Host is up (0.063s latency).
Not shown: 993 closed ports
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
2222/tcp  open      EtherNetIP-1
3306/tcp  open      mysql

Nmap done: 1 IP address (1 host up) scanned in 54.72 seconds
root@kali:~# ft 67.23.79.113
bash: ft: command not found
root@kali:~# ftp 67.23.79.113
Connected to 67.23.79.113.
220 key{3ade9451b891078b05616e2a3a9754ce33ff3a6e}
Name (67.23.79.113:root): █
```
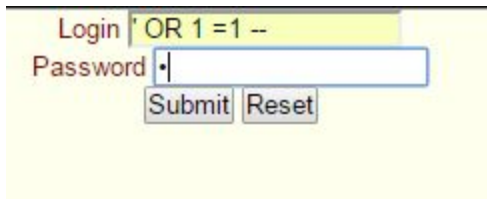
Login SQL Injection (200 points)

1) Went to 67.23.79.113/ctf/board.php with JS disabled
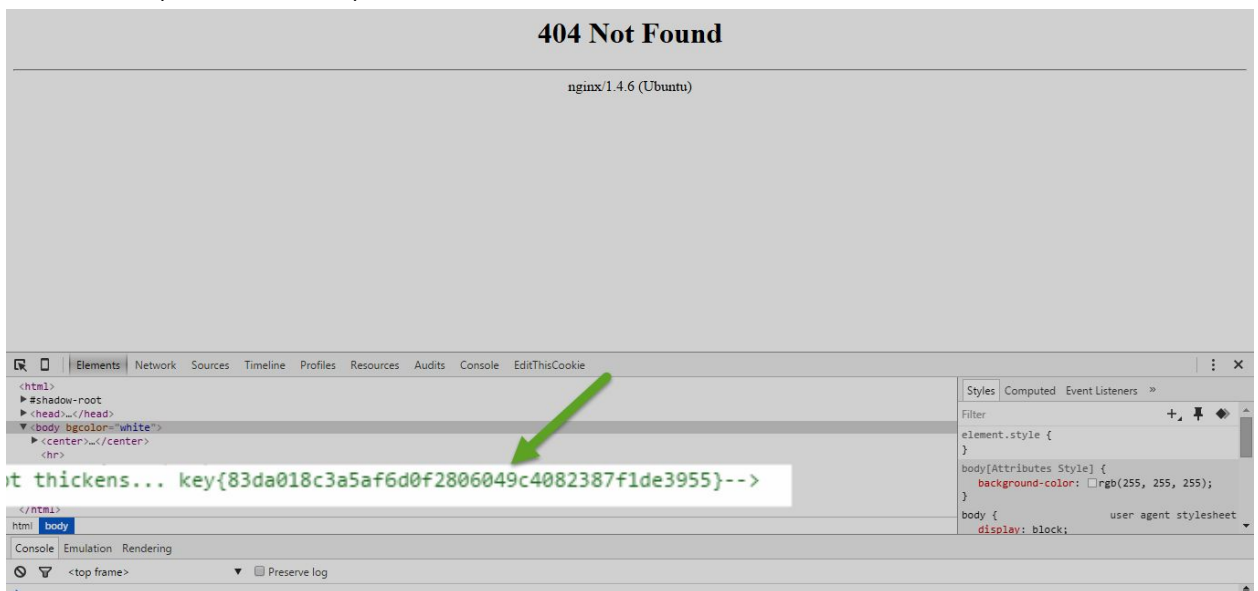2) Navigated to bottom of page and clicked "Administration" link
3) Arrived at http://67.23.79.113/ctf/admin.php (as seen below)

4) Injected SQL to bypass login with any password (as seen below)

5) Successful login took us to http://67.23.79.113/ctf/main.php with flag in HTML source as a comment (as seen below)

Logout.php (100):

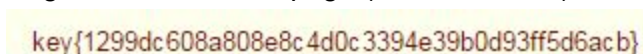1. Navigated to http://67.23.79.113/ctf/logout.php after successfully logging into main.php to cover your tracks. Logout success message was displayed on page (as seen below)

2. Flag was at bottom of page (as seen below)

key{1299dc608a808e8c4d0c3394e39b0d93ff5d6acb}