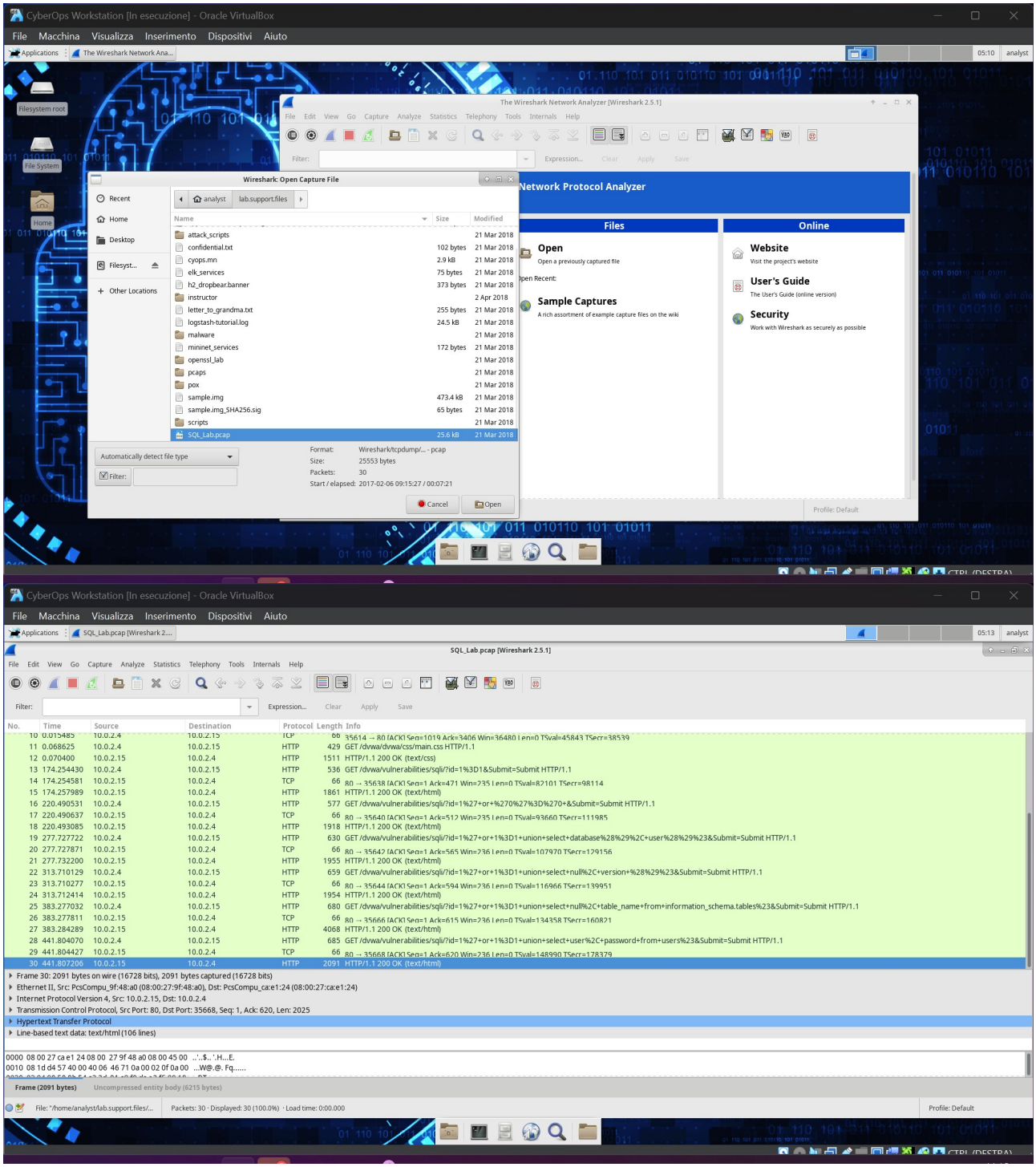
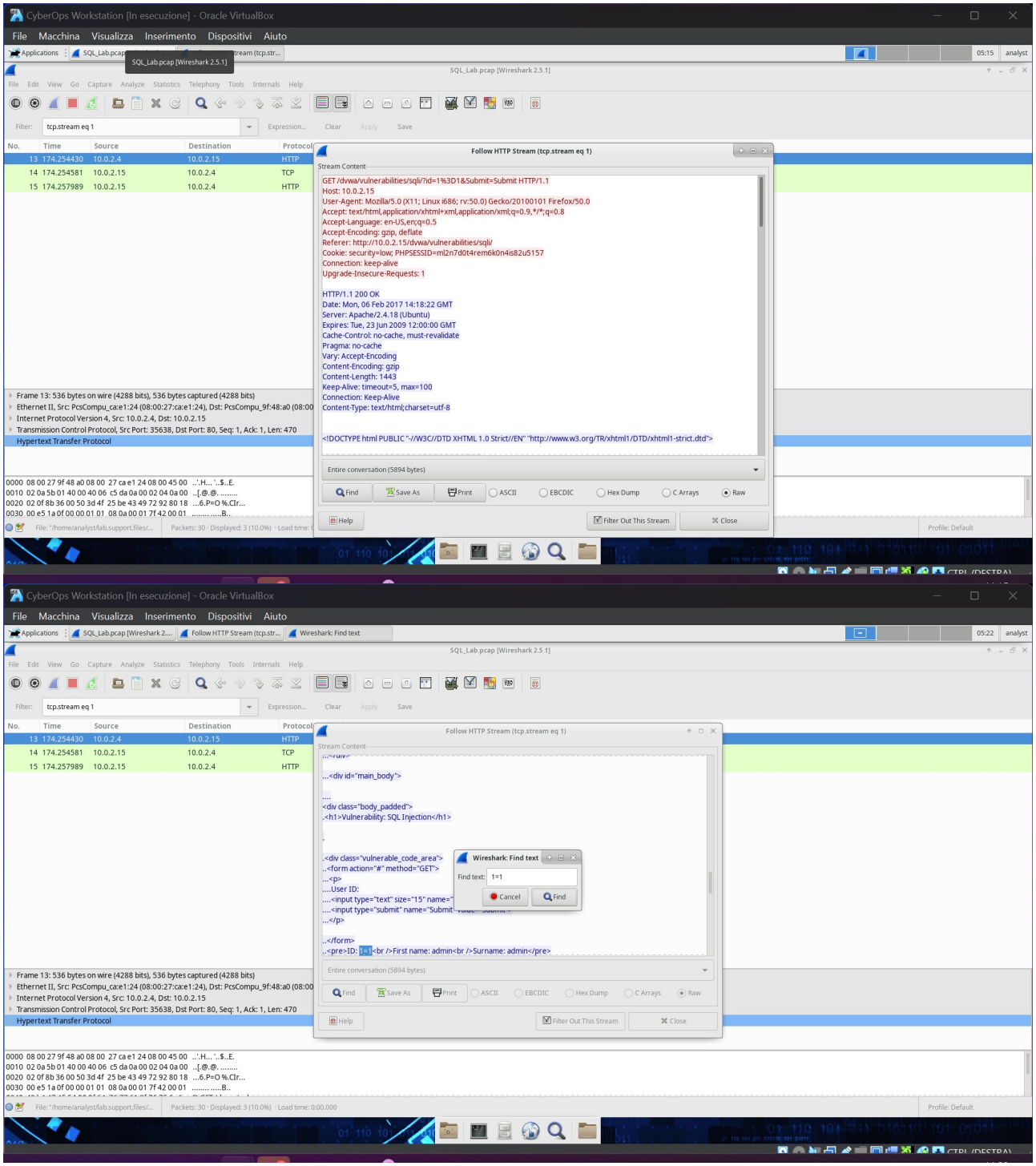
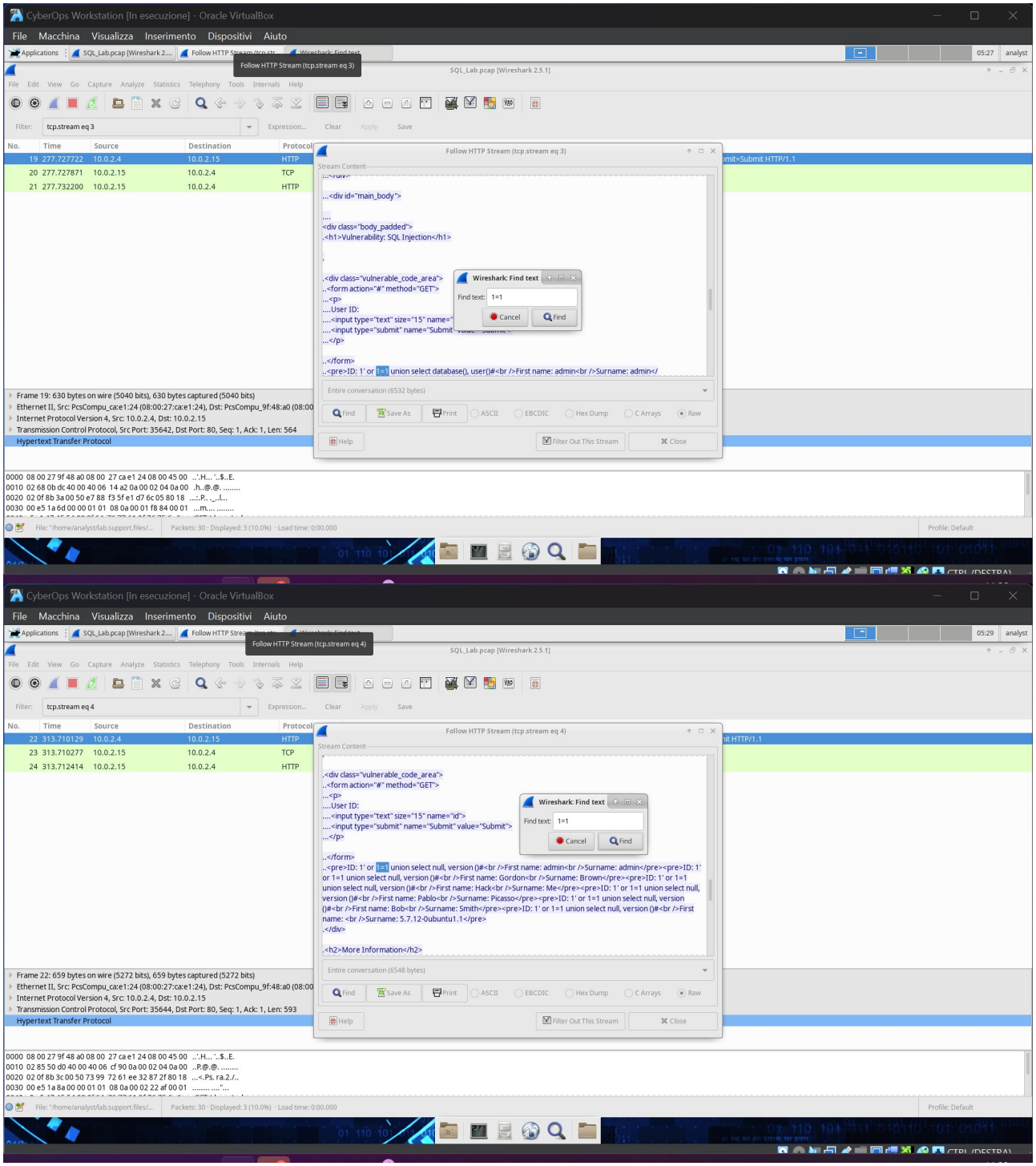
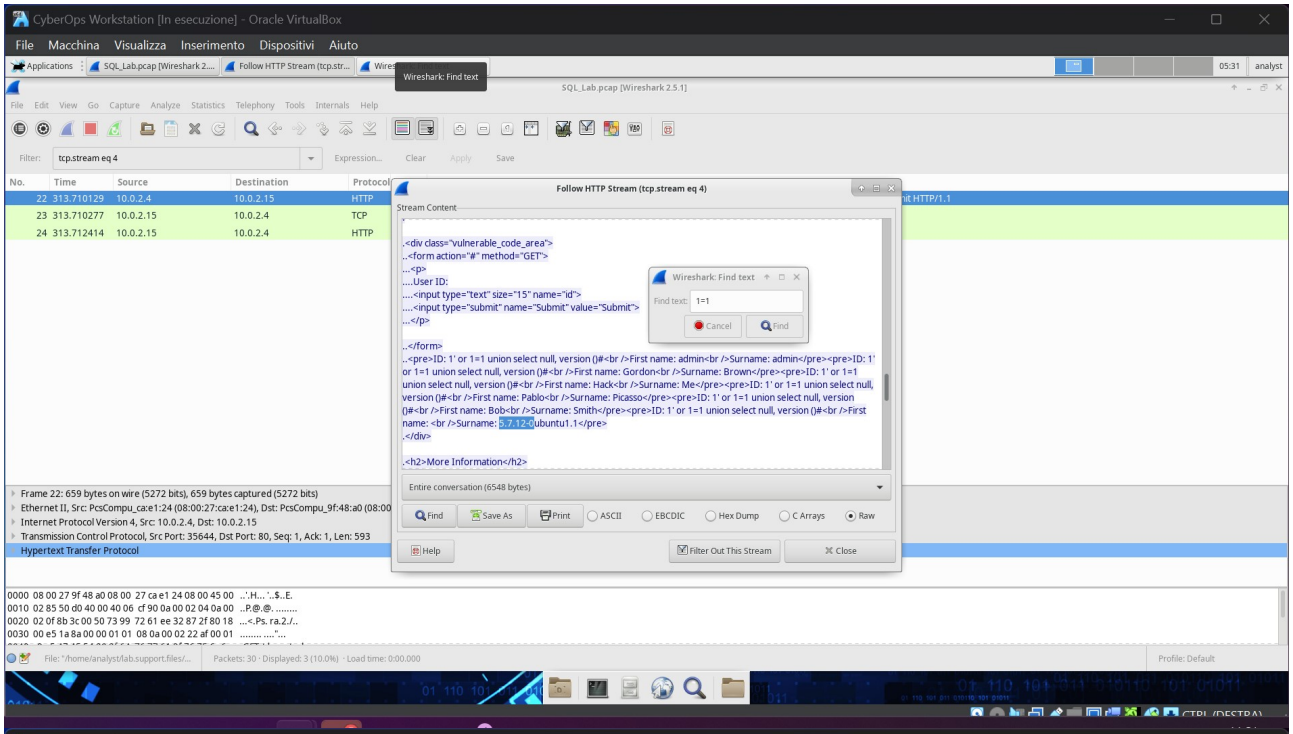
Attacco a un Database MySQL

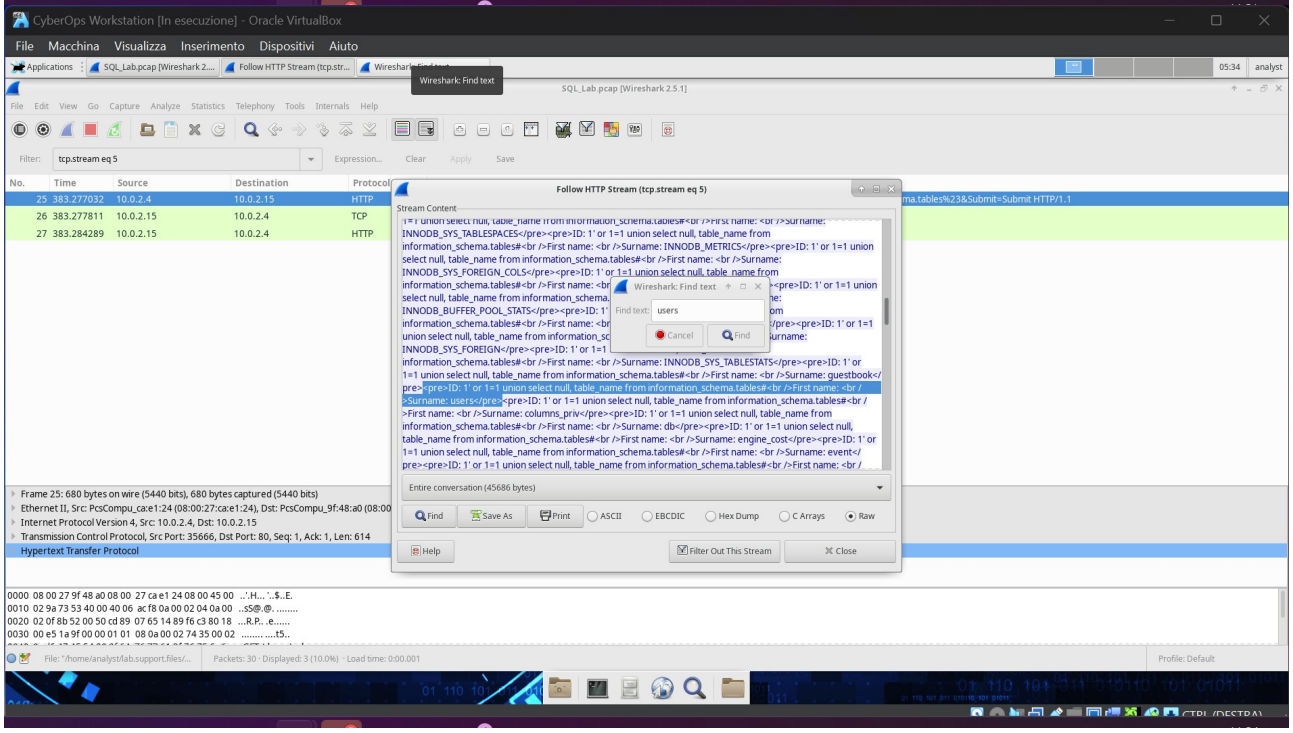


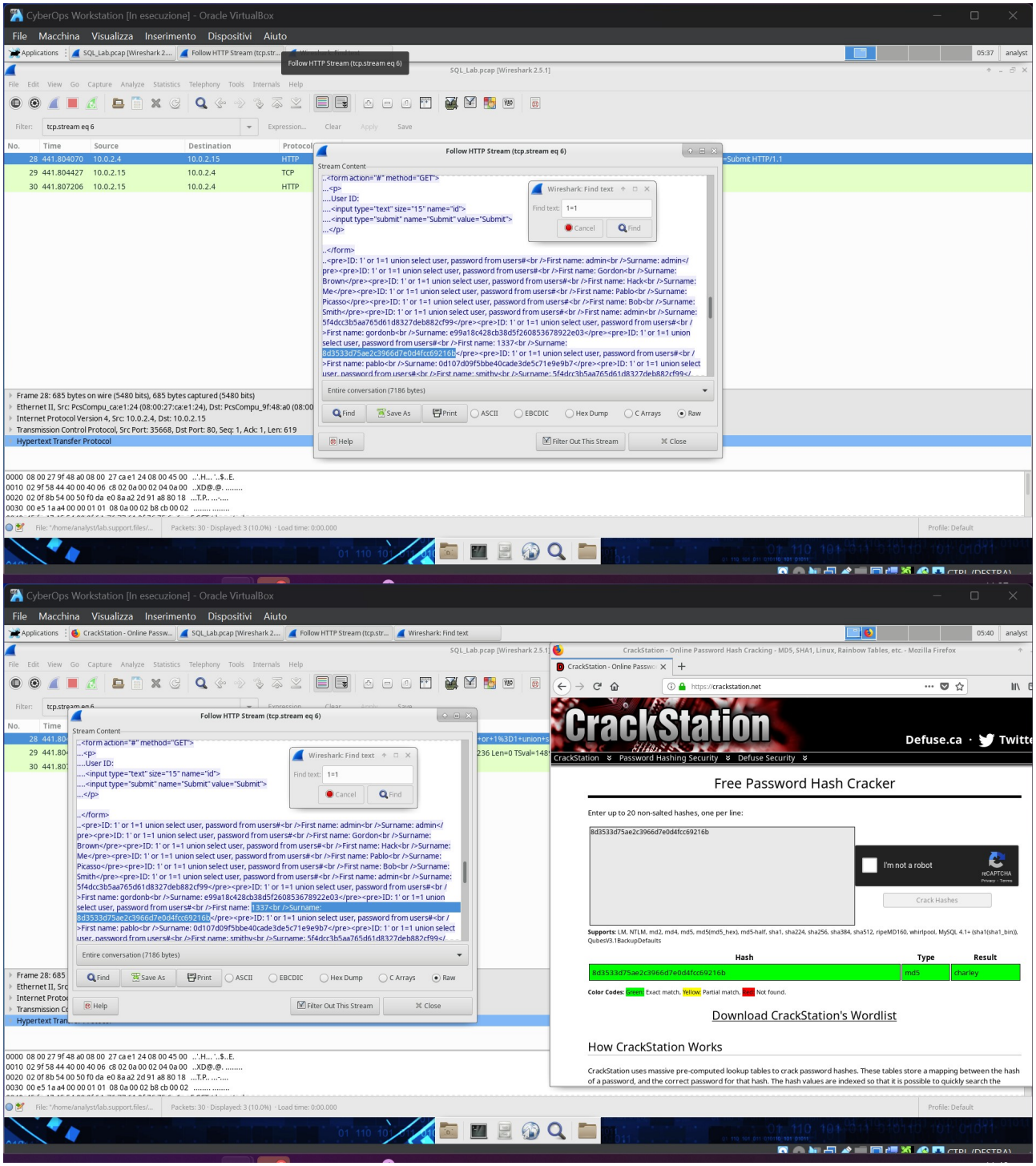

CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 1)
Stream Content
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0
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://10.0.2.15/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:18:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
Entire conversation (5894 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close
Wireshark: Find text
Find text:
1=1
Cancel
Find
...

.<h1>Vulnerability: SQL Injection</h1>
.
..<form action="#" method="GET">
...
....User ID:
....<input type="text" size="15" name="
....<input type="submit" name="Submit
...
..</form>
..<pre>ID: 1=1
First name: admin
Surname: admin</pre>


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Follow HTTP Stream (tcp.stream eq 3)
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 3)
Wireshark: Find text
Find text: 1=1
Cancel
Find
Frame 19: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35642, Dst Port: 80, Seq: 1, Ack: 1, Len: 564
Hypertext Transfer Protocol
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Follow HTTP Stream (tcp.stream eq 4)
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 4)
Wireshark: Find text
Find text: 1=1
Cancel
Find
Frame 22: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35644, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
Hypertext Transfer Protocol


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Wireshark: Find text
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 4)
Stream Content
Find text: 1=1
Entire conversation (6548 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Wireshark: Find text
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 5)
Stream Content
Find text: users
Entire conversation (45686 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Follow HTTP Stream (tcp.stream eq 6)
SQL_Lab.pcap [Wireshark 2.5.1]
Stream Content
Wireshark: Find text
Find text: 1=1
Cancel
Find
Entire conversation (7186 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close
Frame 28: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35668, Dst Port: 80, Seq: 1, Ack: 1, Len: 619
Hypertext Transfer Protocol

CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
https://crackstation.net
CrackStation
Defuse.ca
Password Hashing Security
Defuse Security
Free Password Hash Cracker
Enter up to 20 non-salted hashes, one per line:
8d3533d75ae2c3966d7e0d4fcc69216b
I'm not a robot
reCAPTCHA
Crack Hashes
Hash
Type
Result
8d3533d75ae2c3966d7e0d4fcc69216b
md5
charley
Download CrackStation's Wordlist
How CrackStation Works