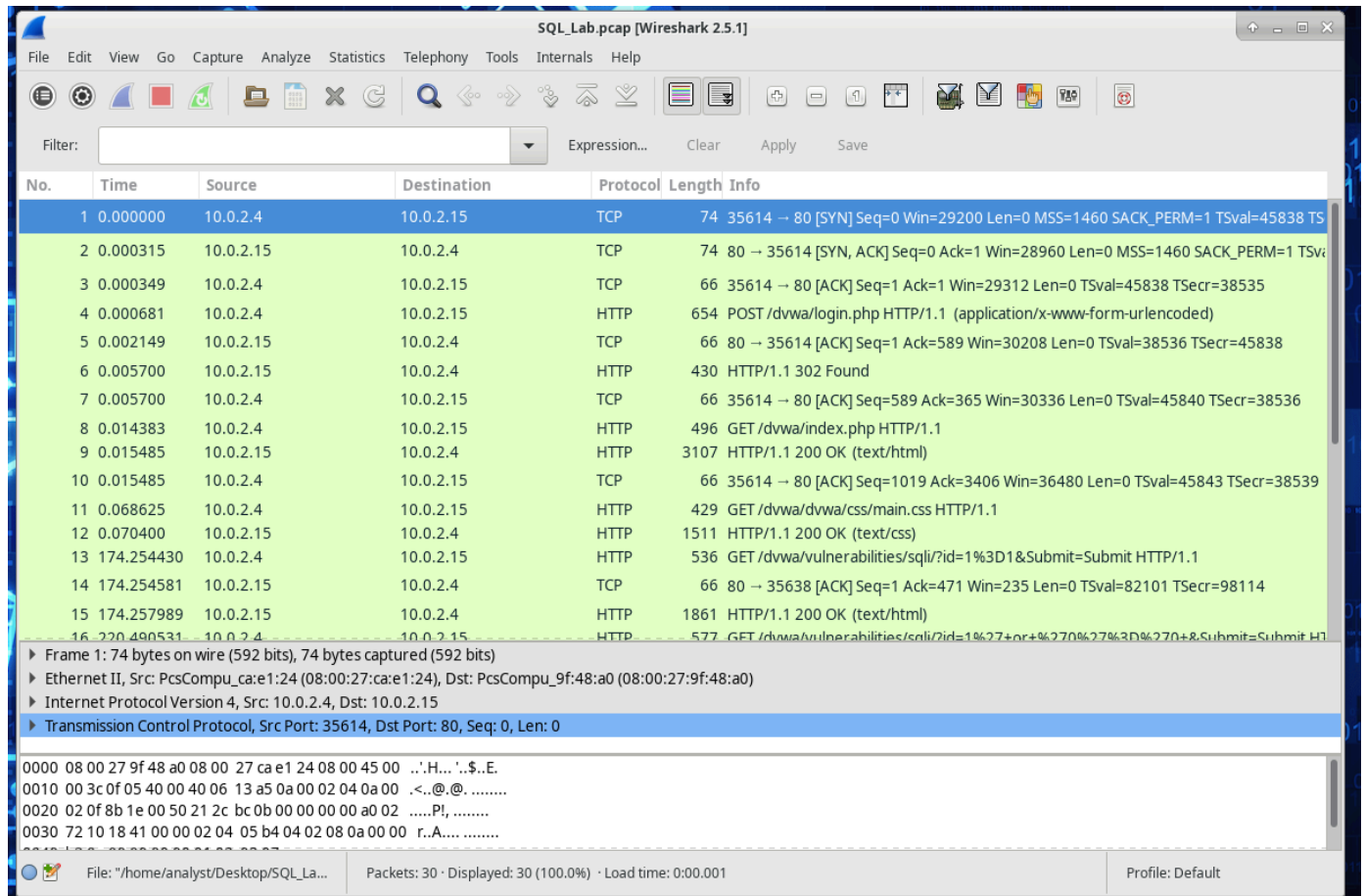


BONUS SQL

Ho aperto il file.



SQL_Lab.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TS
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSv
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D0%270+&Submit=Submit H

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

▶ Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00:27:9f:48:a0)

▶ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15

▶ Transmission Control Protocol, Src Port: 35614, Dst Port: 80, Seq: 0, Len: 0

0000 08 00 27 9f 48 a0 08 00 27 ca e1 24 08 00 45 00 ...H...'.\$.E.

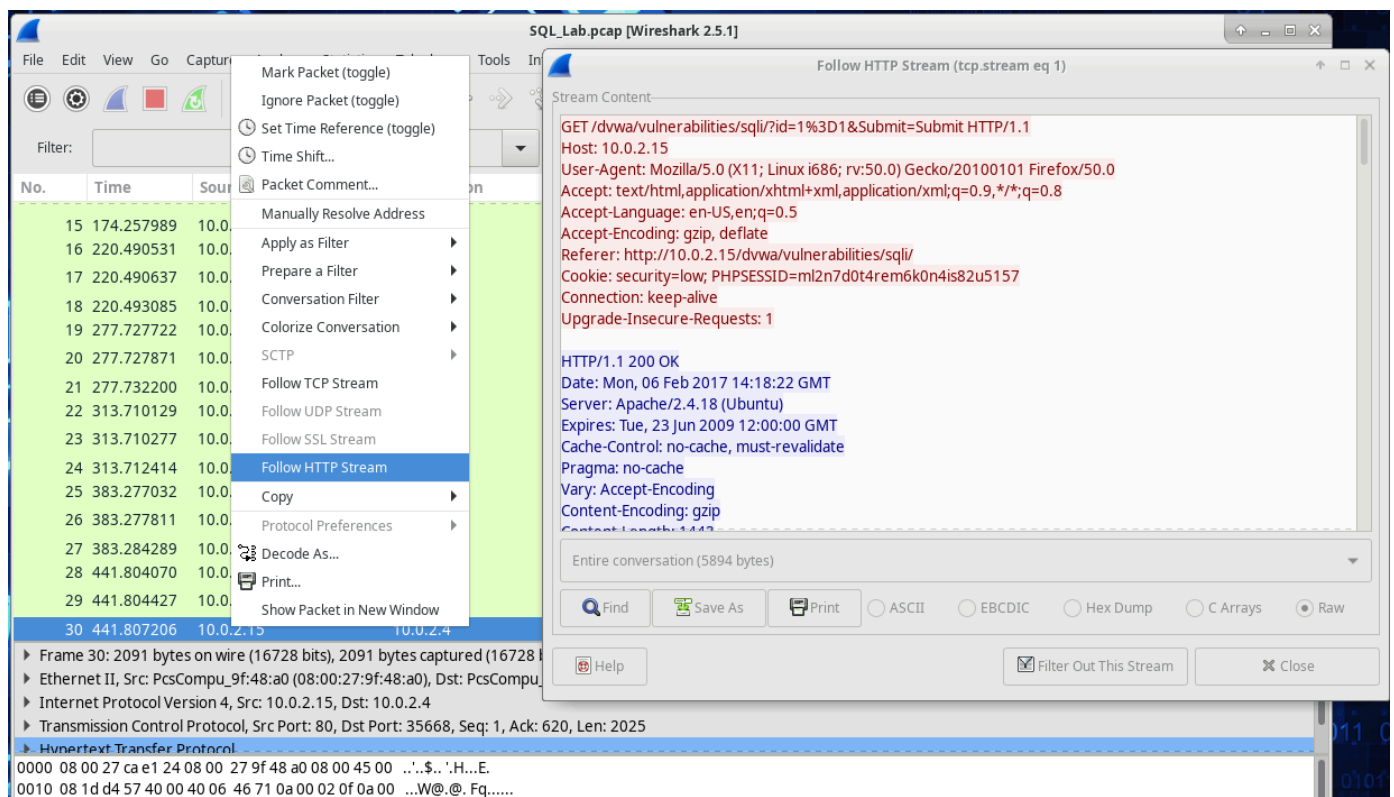
0010 00 3c 0f 05 40 00 40 06 13 a5 0a 00 02 04 0a 00 ...<.@.

0020 02 0f 8b 1e 00 50 21 2c bc 0b 00 00 00 00 a0 02P!r,

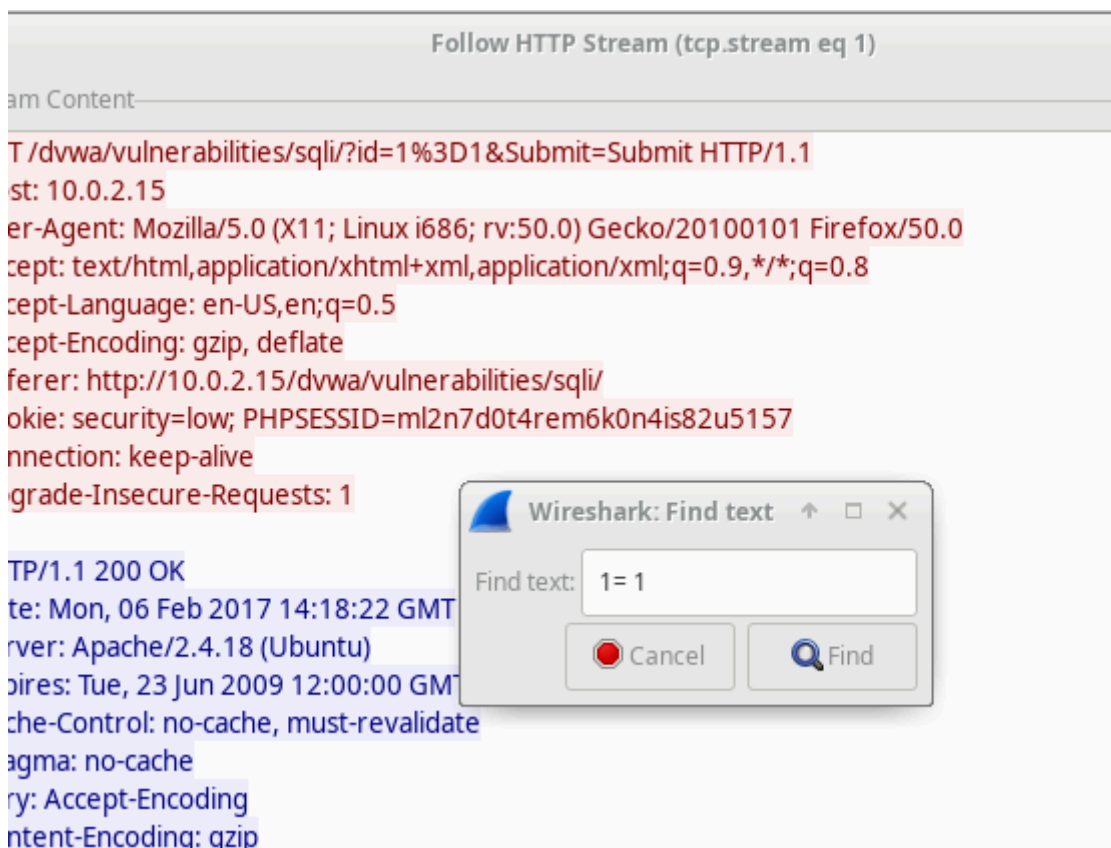
0030 72 10 18 41 00 00 02 04 05 b4 04 02 08 0a 00 00 r..A....

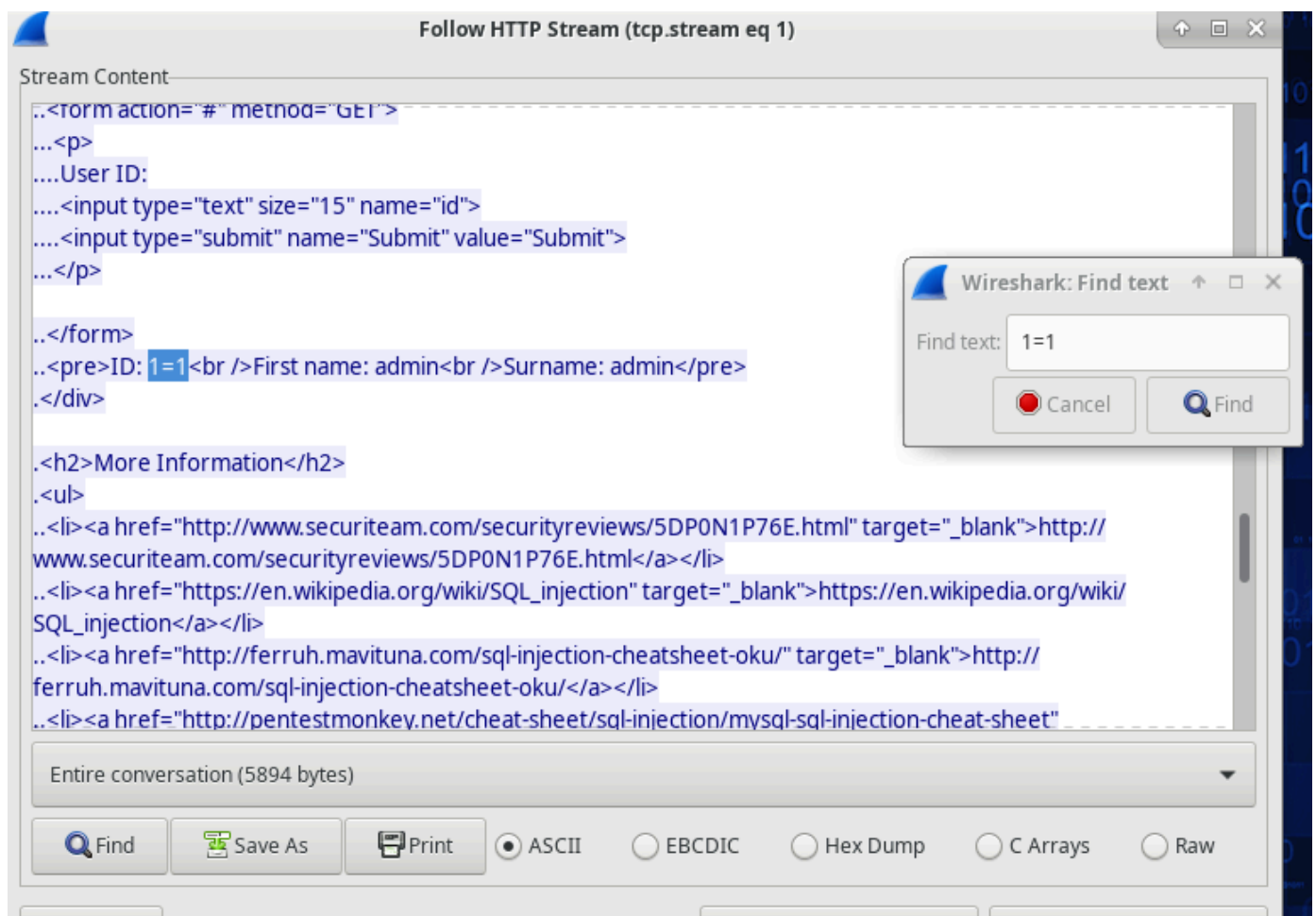
File: "/home/analyst/Desktop/SQL_La... Packets: 30 · Displayed: 30 (100.0%) · Load time: 0:00.001 Profile: Default

Ho analizzato lo stream http.



Ho digitato il comando `1=1` La stringa di ricerca `1=1` crea un'istruzione SQL che sarà sempre vera.





Qua otterremo molte informazioni metto come esempio una che risulta parecchio è che questa attacco è stato svolto su una DVWA.

