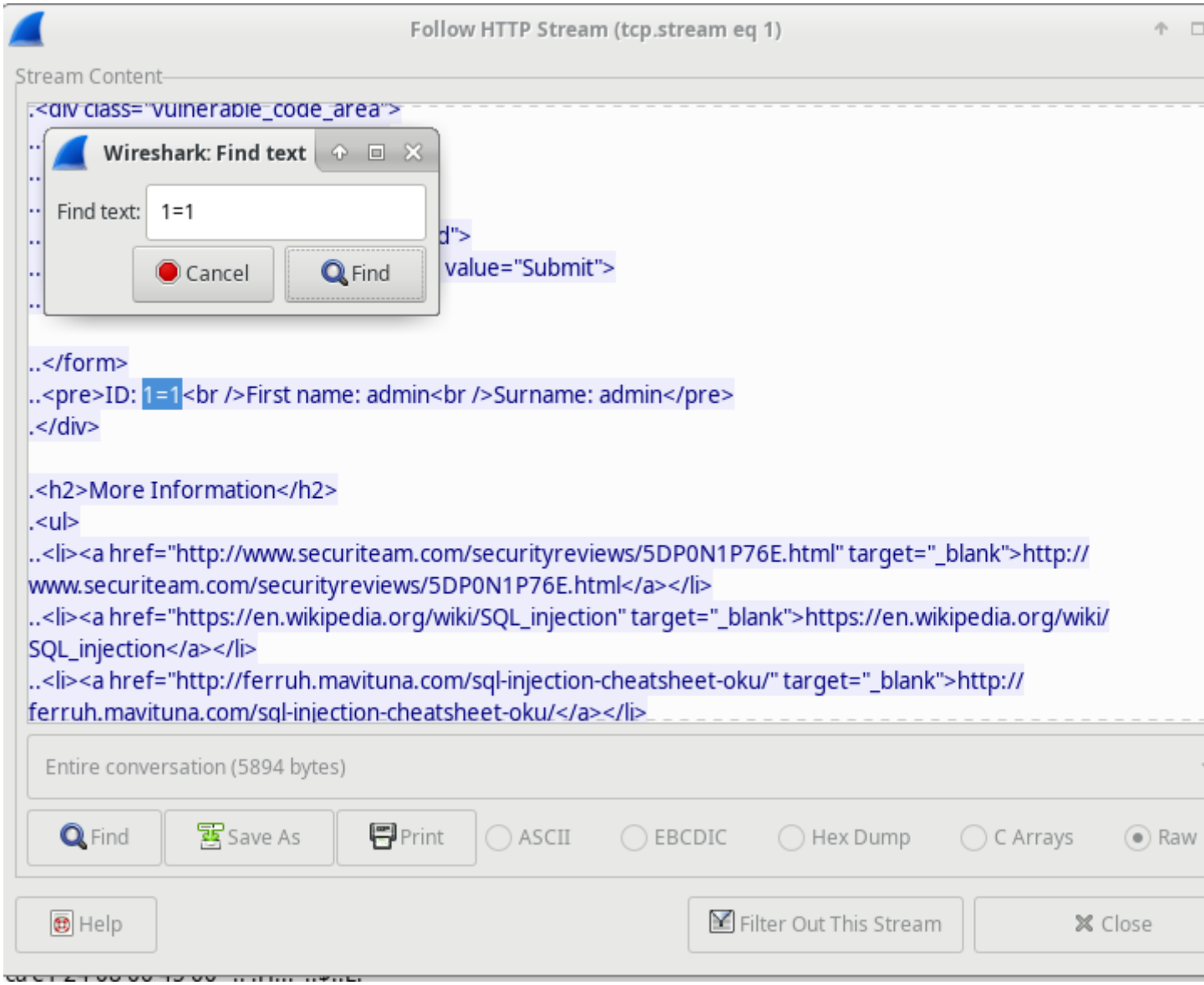
ESERCIZIO S11-L5 PARTE 4

1. Analisi dell'inizio dell'attacco

Andiamo a identificare il primo tentativo di SQL Injection. Su wireshark apriami il file SQL_Lab.pcap, andiamo sulla riga 13 e selezioniamo Follow http stream. Questa riga contiene una richiesta GET HTTP inviata all'host vittima10.0.2.15.

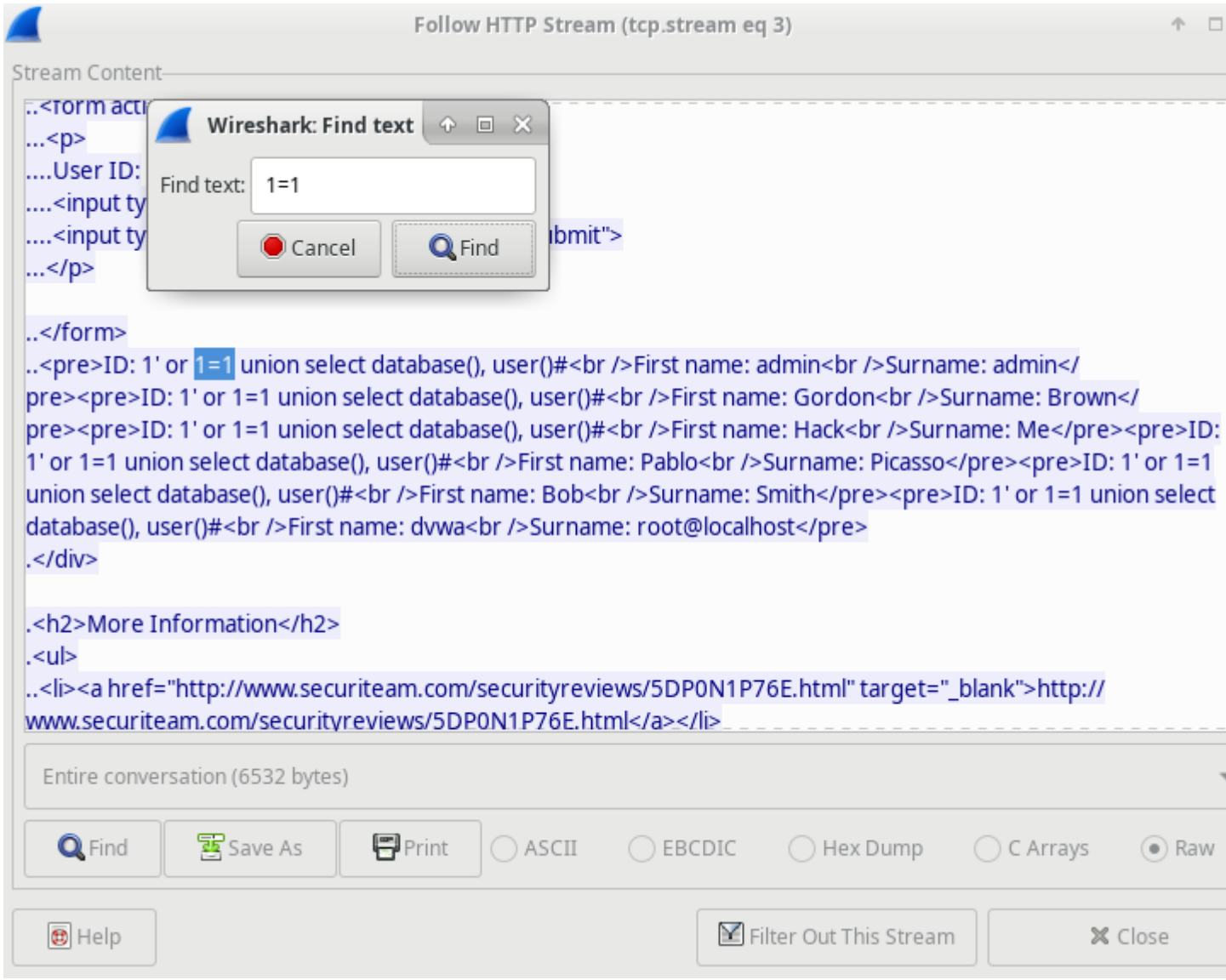
L'attaccante ha inviato un comando SQL 1=1 per verificare se l'applicazione è vulnerabile. Invece di restituire un messaggio di errore, il server risponde con un record del database, confermando che il sistema è esposto a SQL Injection.



2. Continuazione dell'attacco

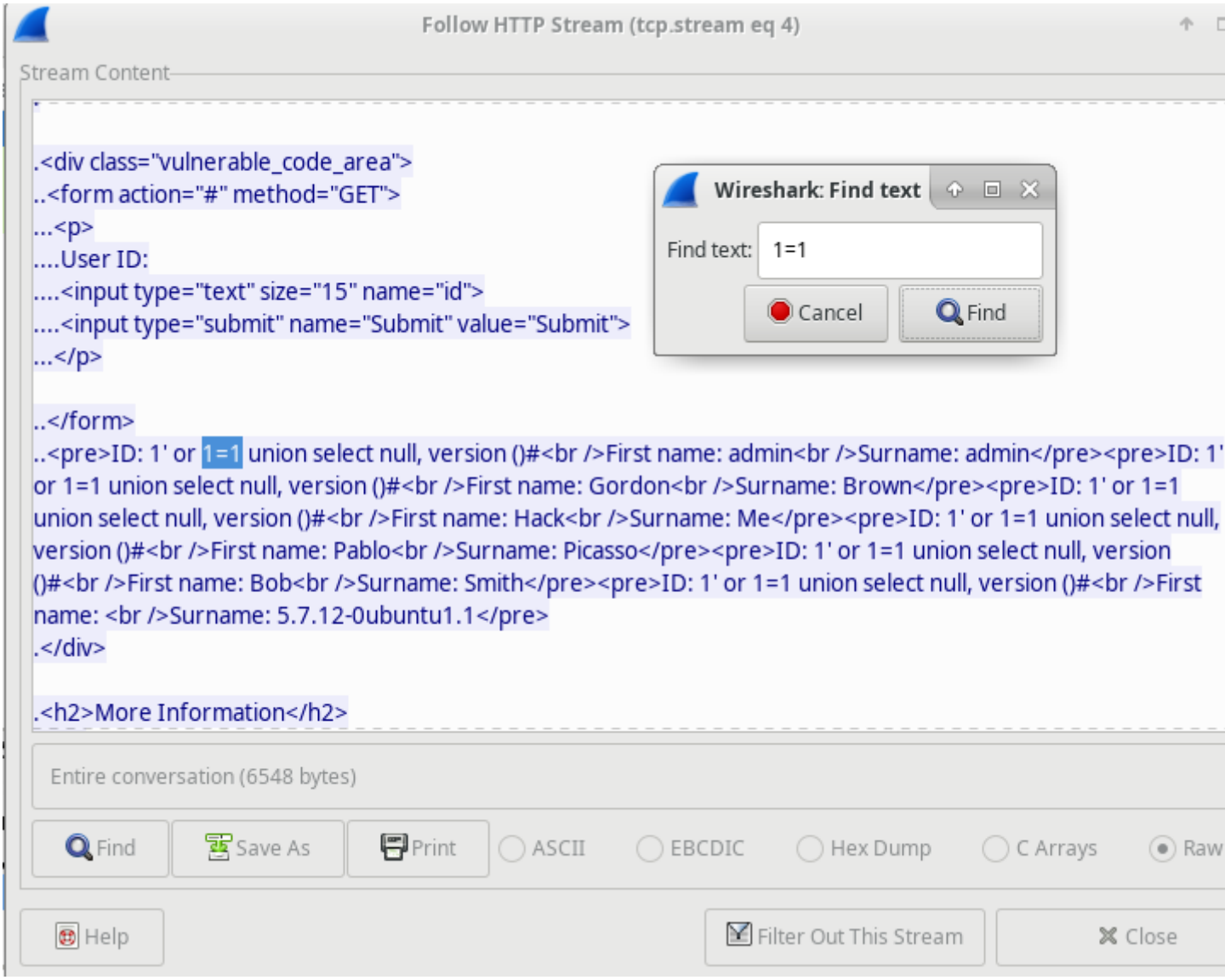
L'attaccante prosegue l'attacco per ottenere ulteriori informazioni dal database.

Il server risponde rivelando il nome del database ("dvwa") e l'utente del database ("root@localhost").



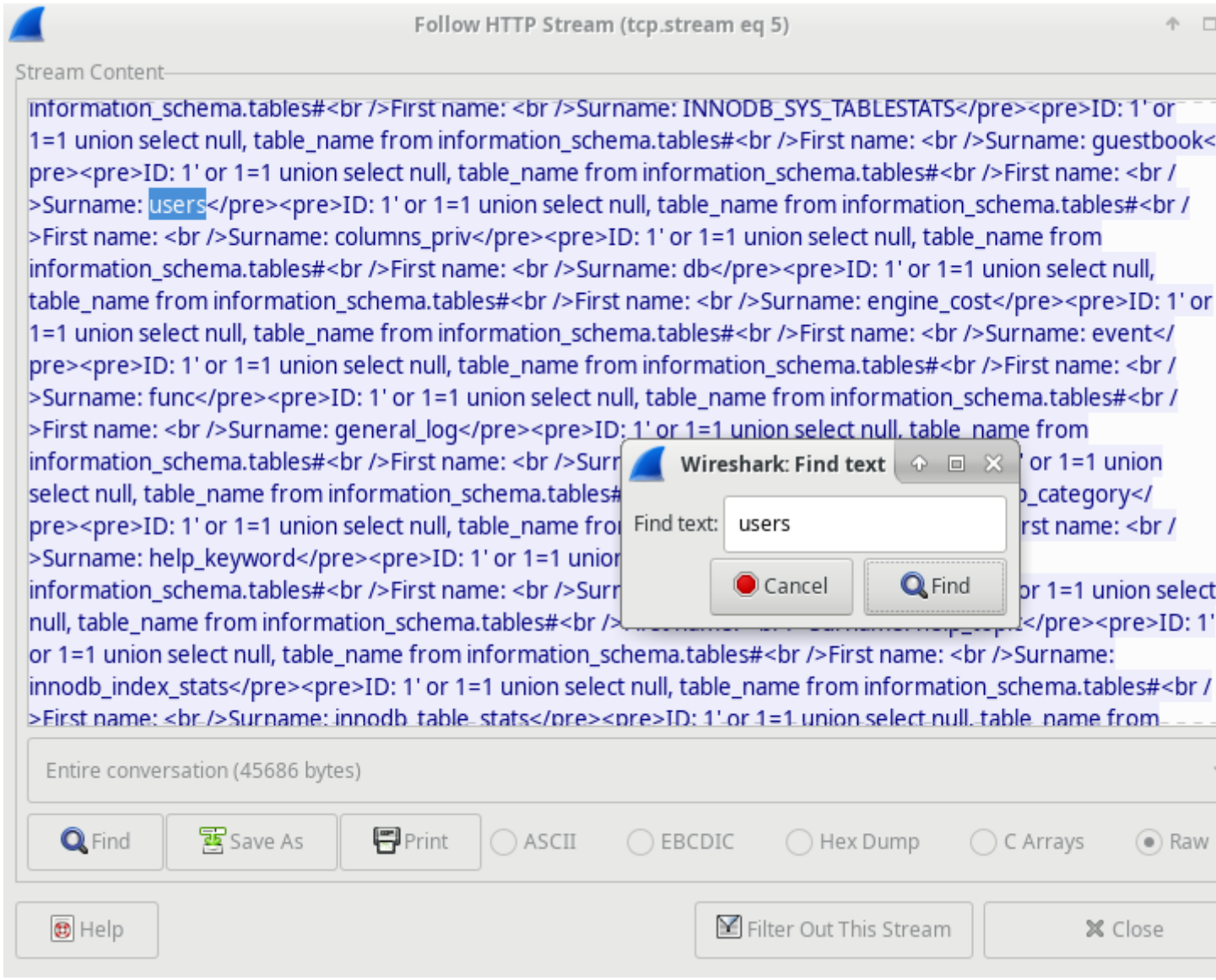
3. Identificazione della versione del database

Il server risponde con la versione del database, mostrata poco prima del tag </pre>. nel codice HTML.



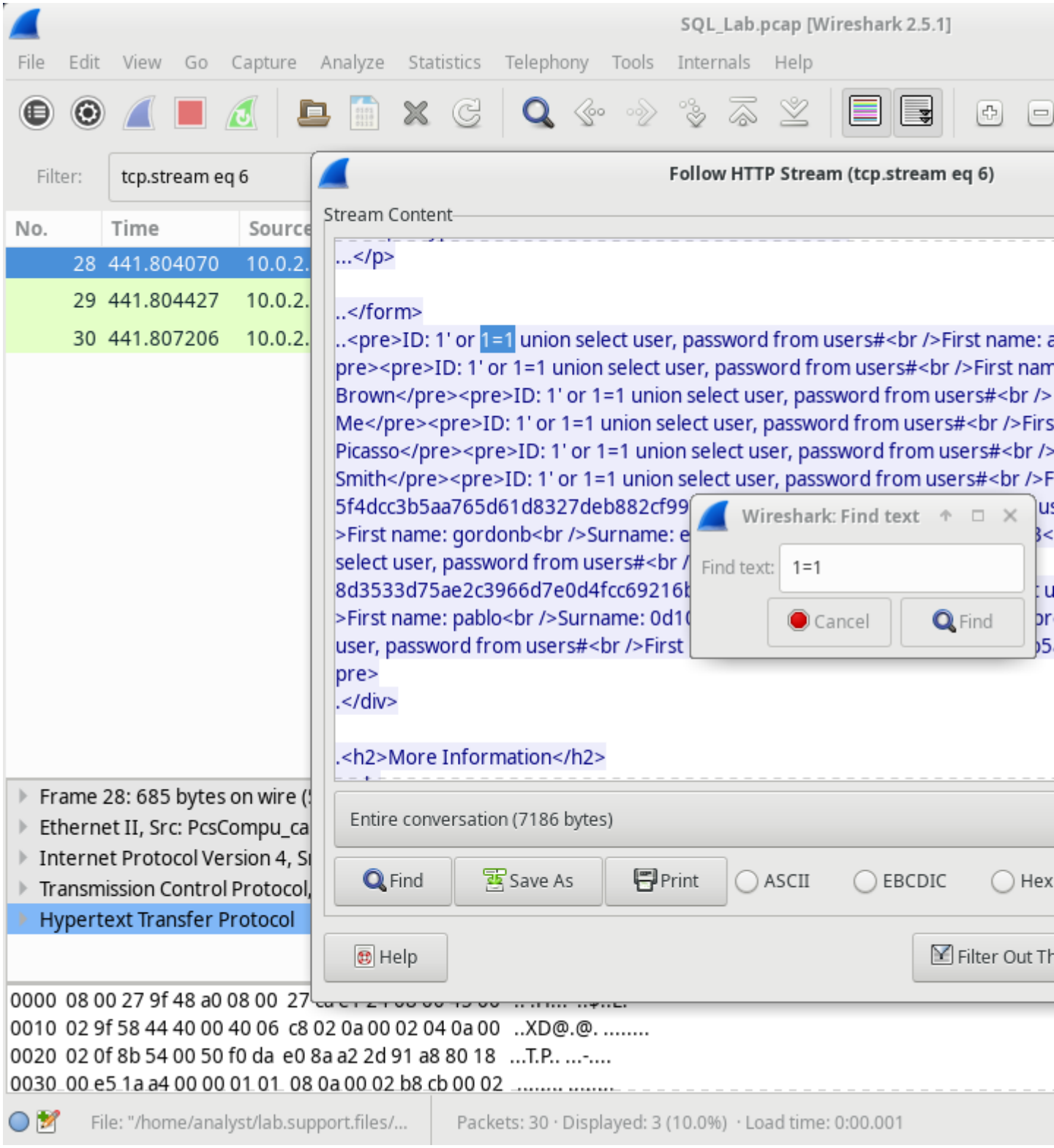
4. Scoperta delle tabelle del database

Il server risponde con un elenco completo delle tabelle disponibili nel database.



5. Recupero delle credenziali

Il server restituisce un elenco di nomi utente e password hashate.


SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 6
No. Time Source
28 441.804070 10.0.2.
29 441.804427 10.0.2.
30 441.807206 10.0.2.
Follow HTTP Stream (tcp.stream eq 6)
Stream Content
...</p>
..</form>
..<pre>ID: 1' or 1=1 union select user, password from users#
First name: a
pre><pre>ID: 1' or 1=1 union select user, password from users#
First nam
Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#
Me</pre><pre>ID: 1' or 1=1 union select user, password from users#
Firs
Picasso</pre><pre>ID: 1' or 1=1 union select user, password from users#
Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#
F
5f4dcc3b5aa765d61d8327deb882cf99
>First name: gordonb
Surname: e
select user, password from users#
8d3533d75ae2c3966d7e0d4fcc69216b
>First name: pablo
Surname: 0d1
user, password from users#
First
pre>
.
.<h2>More Information</h2>
Wireshark: Find text
Find text: 1=1
Cancel
Find
Entire conversation (7186 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex
Help
Filter Out Th
Frame 28: 685 bytes on wire (
Ethernet II, Src: PcsCompu_ca
Internet Protocol Version 4, S
Transmission Control Protocol,
Hypertext Transfer Protocol
0000 08 00 27 9f 48 a0 08 00 27
0010 02 9f 58 44 40 00 40 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 ....
File: "/home/analyst/lab.support.files/...
Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.001