Bonus 2 Attacco a un Database MySQL

In questo laboratorio, completa il seguente obiettivo:

● Visualizzare un file PCAP relativo a un attacco precedente contro un database SQL.

Parte 1: Apri Wireshark e carica il file PCAP.
Parte 2: Visualizza l'attacco di SQL Injection.
Parte 3: L'attacco di SQL Injection continua…
Parte 4: L'attacco di SQL Injection fornisce informazioni sul sistema.
Parte 5: L'attacco di SQL Injection e informazioni sulle tabelle.
Parte 6: L'attacco di SQL Injection si conclude.

Parte 1: Apri Wireshark e carica il file PCAP.
L'applicazione Wireshark può essere aperta utilizzando vari metodi su una workstation Linux.

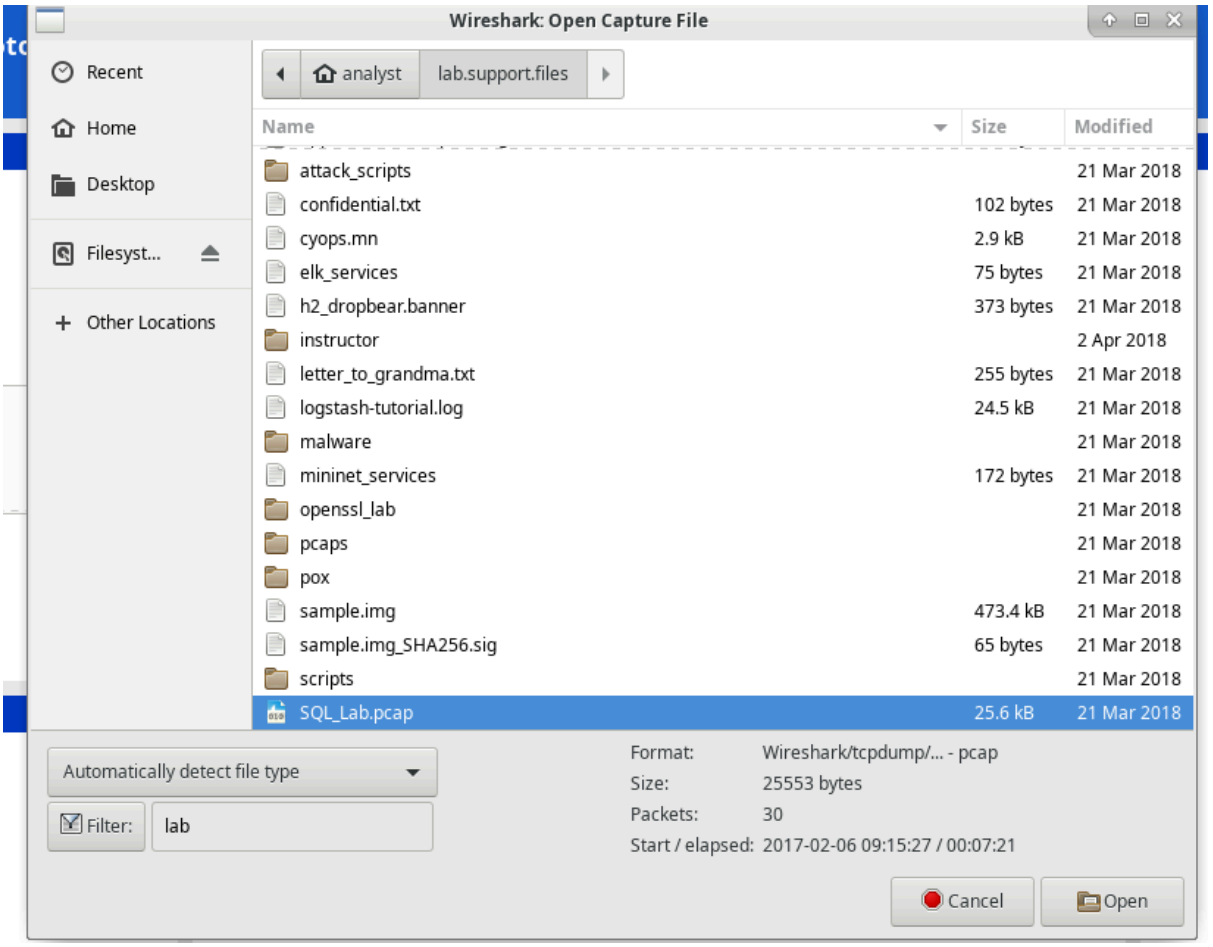
a. Avvia la VM della CyberOps Workstation.

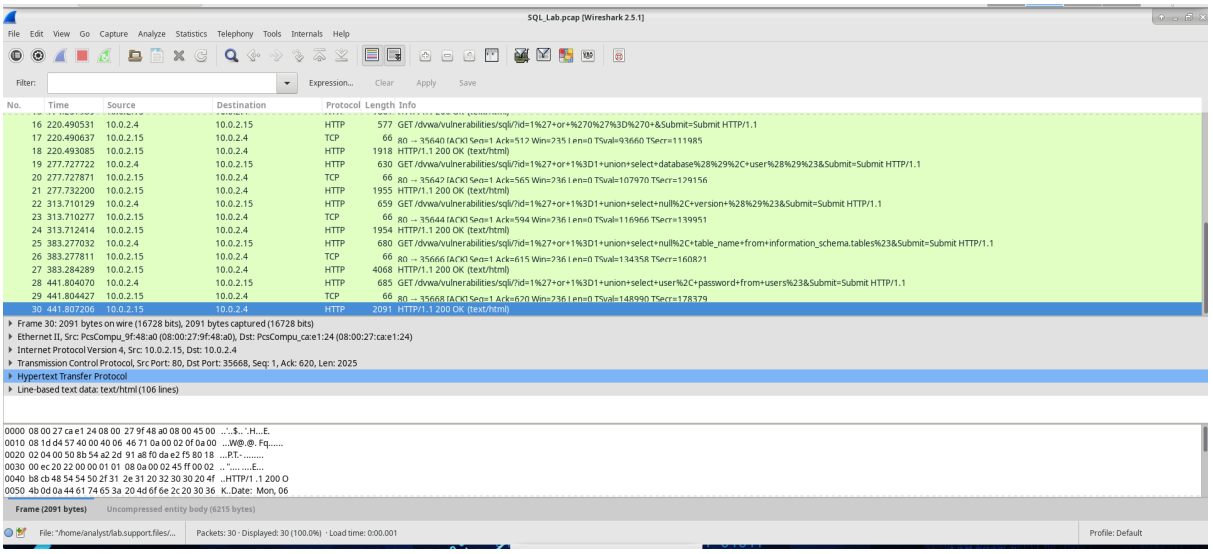
b. Clicca su **Applicazioni > CyberOPS > Wireshark** sul desktop e cerca l'applicazione Wireshark.

c. Nell'applicazione Wireshark, clicca su **Apri** nel centro dell'applicazione sotto **File**.

d. Naviga nella directory **/home/analyst/** e cerca la cartella **lab.support.files**. Nella directory **lab.support.files**, apri il file **SQL_Lab.pcap**.

e. Il file PCAP si apre in Wireshark e mostra il traffico di rete catturato. Questo file di cattura copre un periodo di 8 minuti (441 secondi), corrispondente alla durata di questo attacco di SQL injection.



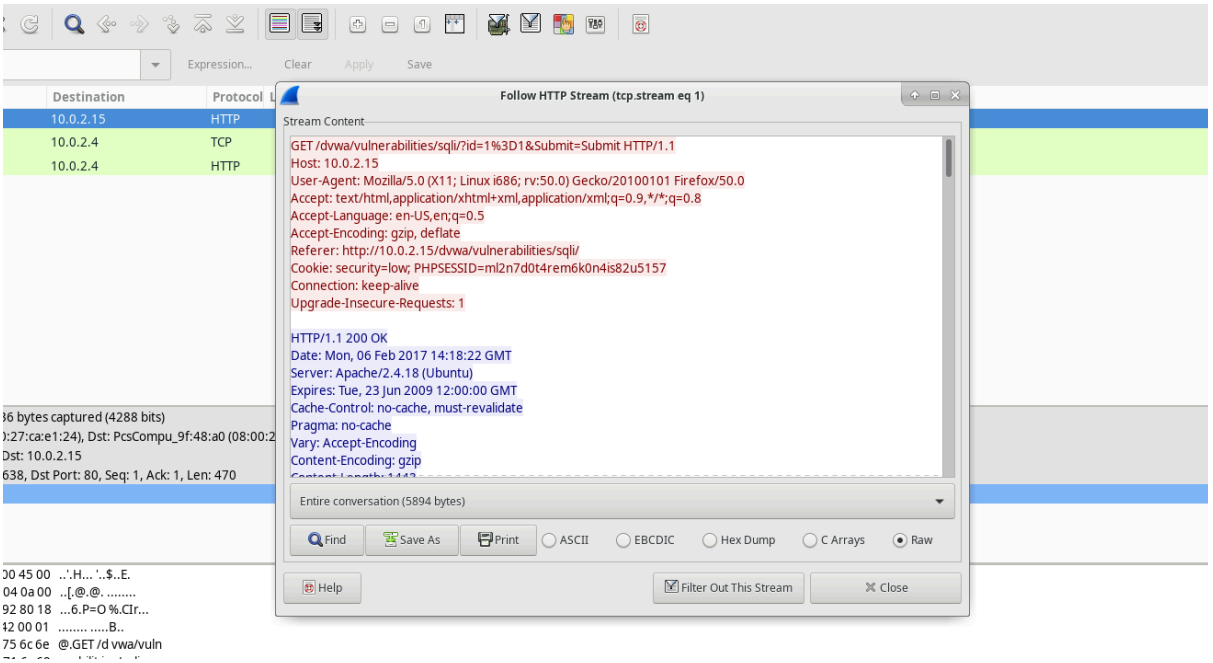


Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?

10.0.2.4 e 10.0.2.15

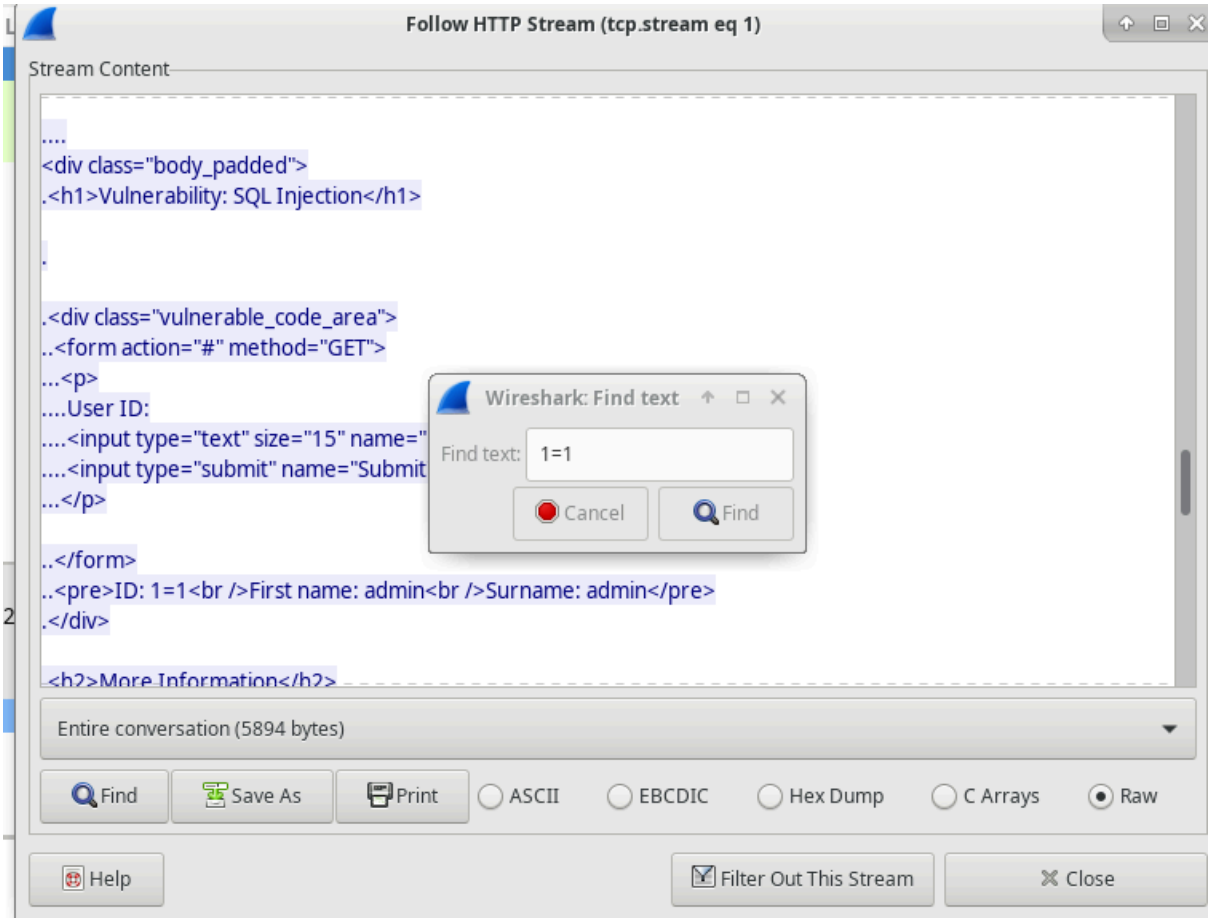
Parte 2: Visualizza l'attacco di SQL Injection.
In questo passaggio, visualizzerai l'inizio di un attacco.

a. All'interno della cattura di Wireshark, fai clic con il tasto destro sulla riga 13 e seleziona Segui > Stream HTTP. La riga 13 è stata scelta perché si tratta di una richiesta HTTP GET. Questo sarà molto utile per seguire il flusso dei dati come li vede il livello applicativo e porterà fino al test della query per la SQL injection.



Il traffico di origine è mostrato in rosso. La sorgente ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo **Trova**, inserisci **1=1**. Clicca su **Trova successivo**.



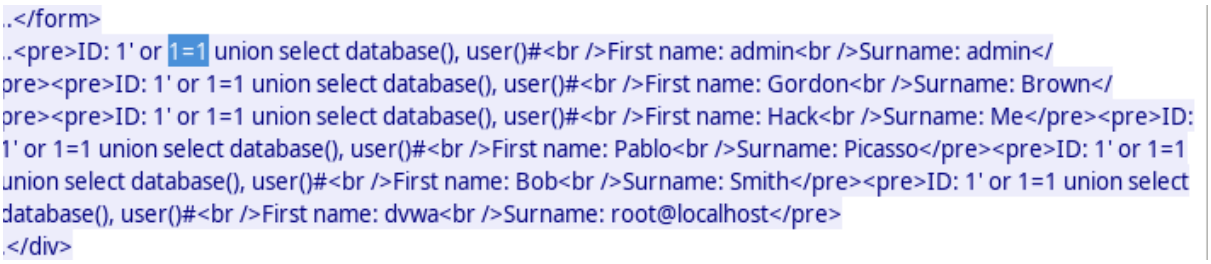
L'attaccante ha inserito una query (1=1) in un campo di ricerca UserID sul target 10.0.2.15 per verificare se l'applicazione è vulnerabile a un attacco di SQL injection. Invece di ricevere un messaggio di errore relativo al login, l'applicazione ha risposto con un record dal database. L'attaccante ha verificato che può inserire un comando SQL e il database risponderà. La stringa di ricerca 1=1 genera una dichiarazione SQL che sarà sempre vera. Nell'esempio, non importa cosa venga inserito nel campo, sarà sempre vero.

Parte 3: L'attacco di SQL Injection continua...
In questo passaggio, visualizzerai la continuazione di un attacco.

a. All'interno della cattura di Wireshark, fai clic con il tasto destro sulla riga 19 e seleziona **Segui > Stream HTTP**.

b. Nel campo **Trova**, inserisci **1=1**. Clicca su **Trova successivo**.

c. L'attaccante ha inserito una query (**1' or 1=1 union select database(), user()#**) in un campo di ricerca UserID sul target 10.0.2.15. Invece di ricevere un messaggio di errore relativo al login, l'applicazione ha risposto con le seguenti informazioni:



Il nome del database è **dvwa** e l'utente del database è **root@localhost**. Vengono inoltre visualizzati più account utente.

d. Chiudi la finestra **Segui Stream HTTP**.

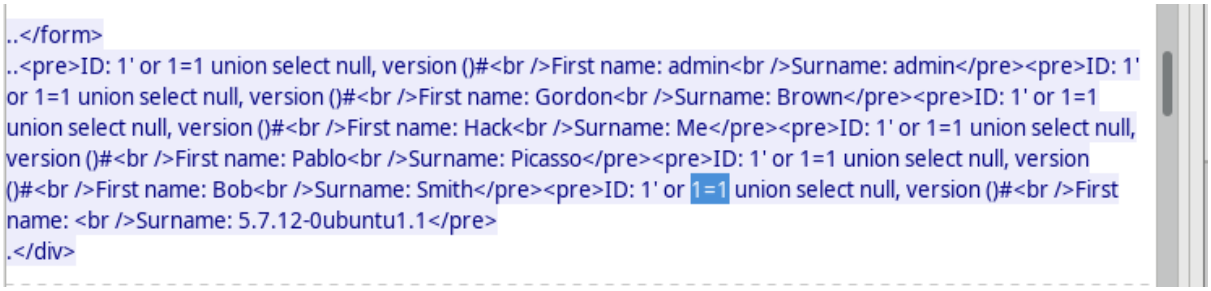
e. Clicca su **Pulisci filtro di visualizzazione** per mostrare l'intera conversazione di Wireshark.

Parte 4: L'attacco di SQL Injection fornisce informazioni sul sistema.
L'attaccante continua e inizia a mirare a informazioni più specifiche.

a. All'interno della cattura di Wireshark, fai clic con il tasto destro sulla riga 22 e seleziona **Segui > Stream HTTP**. In rosso, il traffico di origine è mostrato e sta inviando la richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo **Trova**, inserisci **1=1**. Clicca su **Trova successivo**.

c. L'attaccante ha inserito una query (**1' or 1=1 union select null, version()#**) in un campo di ricerca UserID sul target 10.0.2.15 per localizzare l'identificativo della versione. Nota come l'identificativo della versione si trovi alla fine dell'output, proprio prima del codice HTML di chiusura **</pre>. **.



Qual è la versione del database?

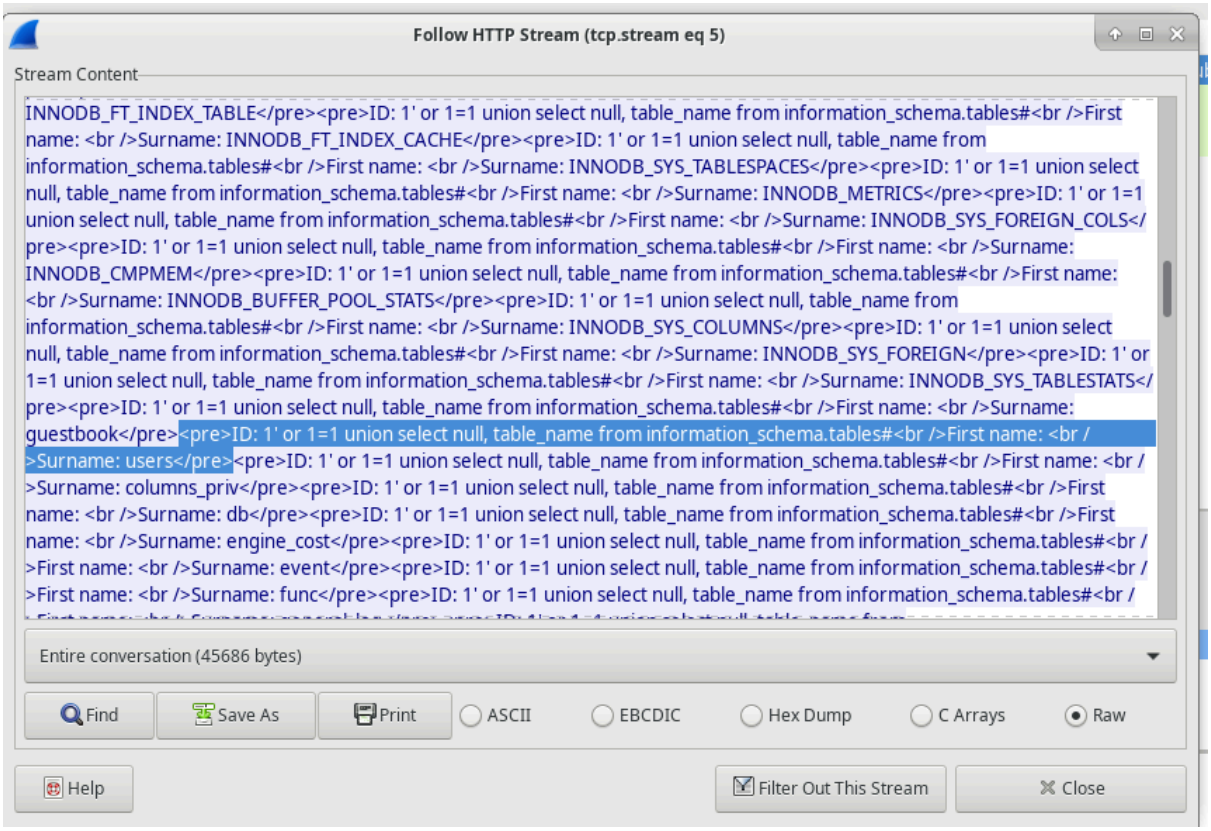
La versione è **MySQL 5.7.12-0**.

Parte 5: L'attacco di SQL Injection e le informazioni sulle tabelle.
L'attaccante sa che esiste un gran numero di tabelle SQL piene di informazioni. L'attaccante cerca di trovarle.

a. All'interno della cattura di Wireshark, fai clic con il tasto destro sulla riga 25 e seleziona **Segui > Stream HTTP**. La sorgente è mostrata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo **Trova**, inserisci **users**. Clicca su **Trova successivo**.

c. L'attaccante ha inserito una query (**1'or 1=1 union select null, table_name from information_schema.tables#**) in un campo di ricerca UserID sul target 10.0.2.15 per visualizzare tutte le tabelle nel database. Questo genera un grande output con molte tabelle, poiché l'attaccante ha specificato **null** senza ulteriori specifiche.



Cosa farebbe per l'attaccante il comando modificato (1′ OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users')?

Il database risponderebbe con un output molto più corto filtrato dalla presenza della parola "users".

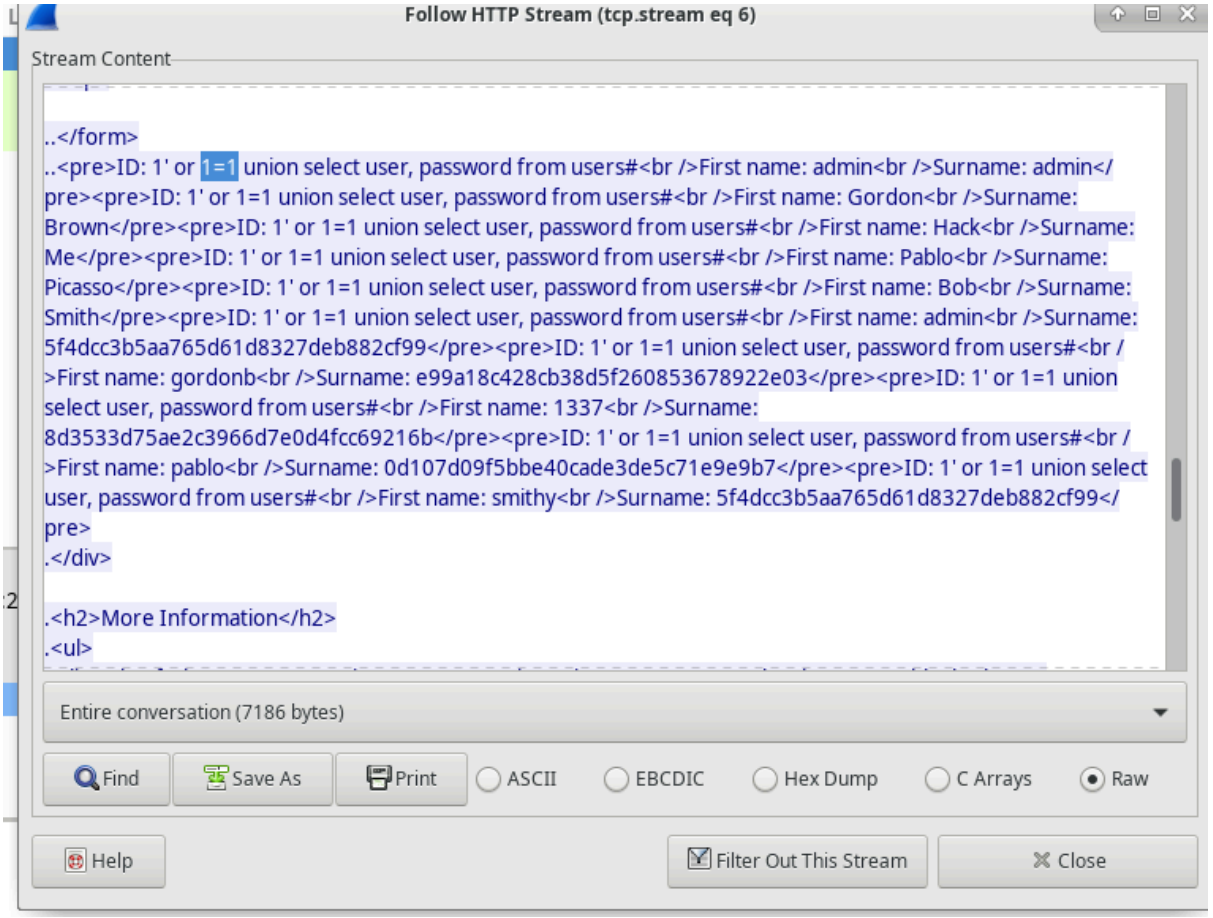
Parte 6: L'attacco SQL Injection si conclude.

L'attacco termina con il miglior premio di tutti: gli hash delle password.

a. All'interno della cattura di Wireshark, fai clic con il tasto destro sulla riga 28 e seleziona **Follow > HTTP Stream**. La fonte è mostrata in rosso. Ha inviato una richiesta **GET** all'host **10.0.2.15**. In blu, il dispositivo di destinazione sta rispondendo alla fonte.

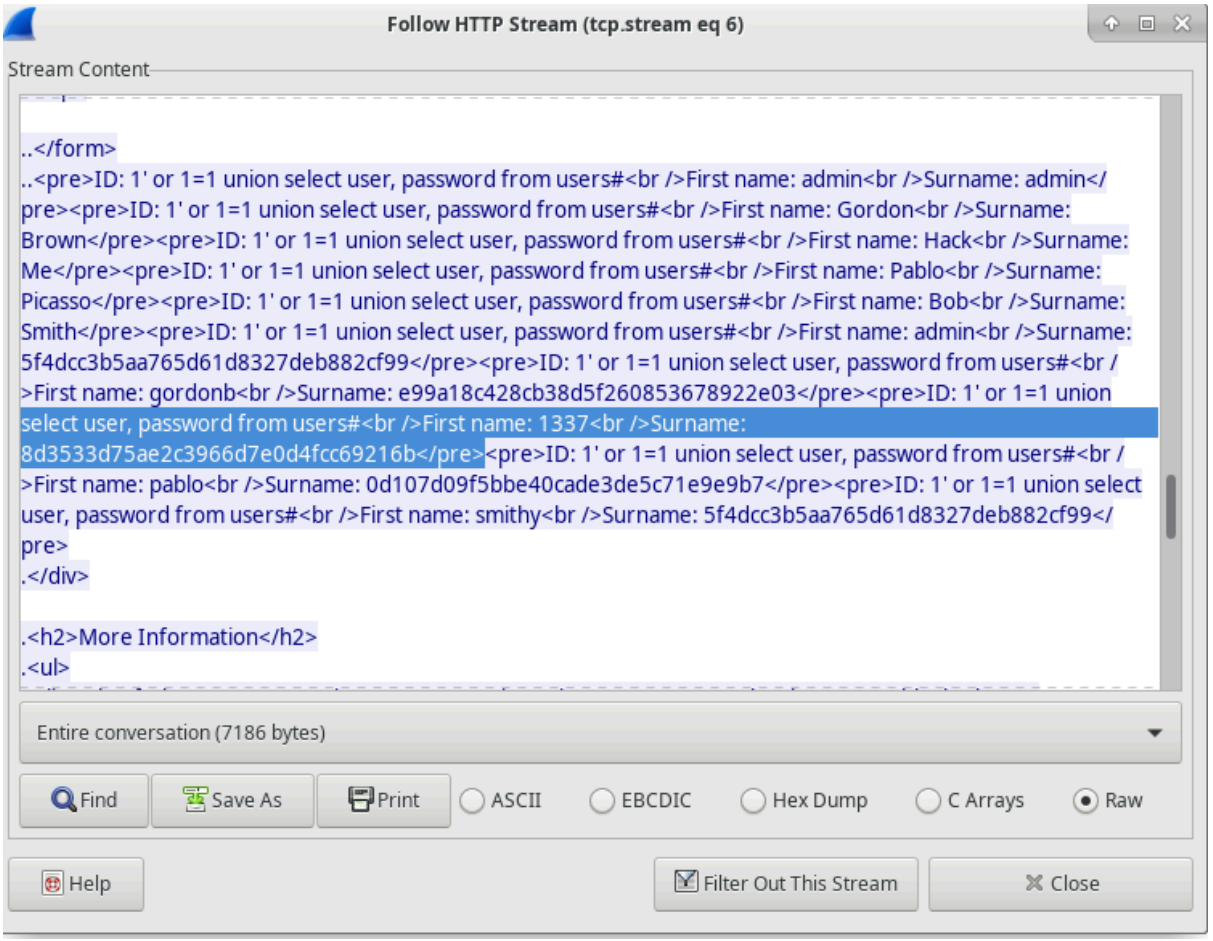
b. Fai clic su **Find** e digita **1=1**. Cerca questa voce. Quando il testo viene trovato, fai clic su **Cancel** nella casella di ricerca del testo.

L'attaccante ha inserito una query (**1' OR 1=1 UNION SELECT user, password FROM users#**) in un campo di ricerca **UserID** sul target **10.0.2.15** per estrarre nomi utente e hash delle password!

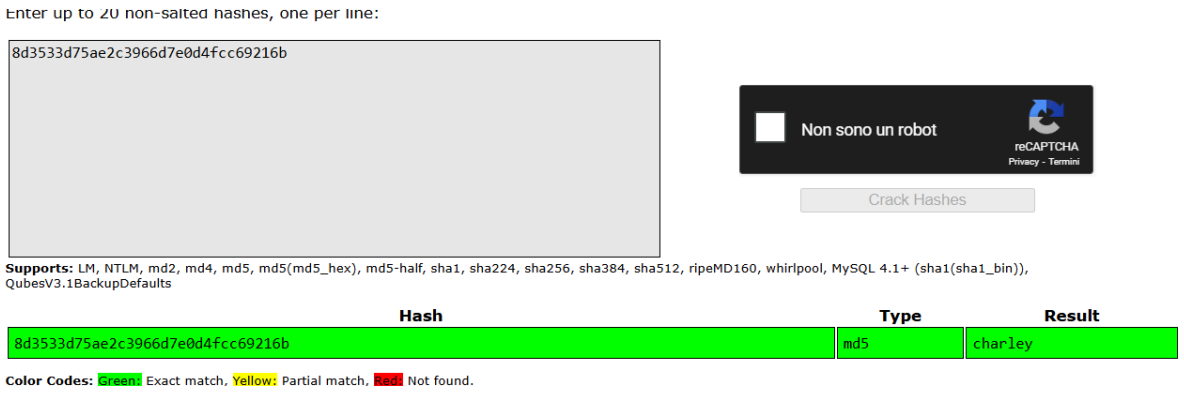


Quale utente ha l'hash della password **8d3533d75ae2c3966d7e0d4fcc69216b**?

L'utente che ha come hash della password **8d3533d75ae2c3966d7e0d4fcc69216b** è l'utente '**1337'**



Utilizzando un sito web come https://crackstation.net/, copia l'hash della password nel tool di cracking delle password e avvia il processo.



Qual è la password in chiaro?

charley