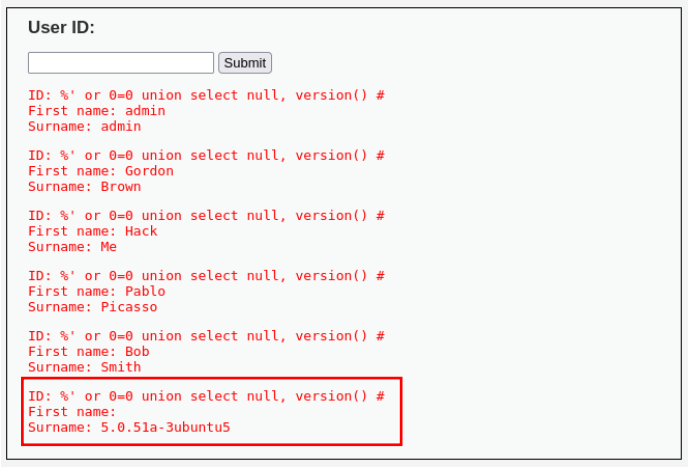
[CONSEGNA SETTIMANA 6 LEZIONE 4]

Attacco SQL Injection

L'attacco ai database viene chiamato **SQL Injection**, dove tramite delle **query** particolari è possibile andare a compromettere il database e recuperare importanti informazioni.

Nel nostro caso andremo a compromettere il database della macchina *metasploitable*, per la precisione ***DVWA***.

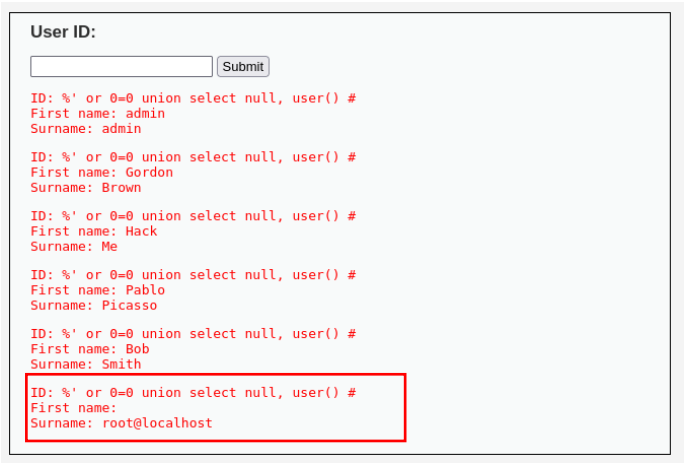
Andremo quindi a recuperare: versione del **database, utenti e password.**



Tramite la query

```
%' or 0=0 union select null, version() #
```

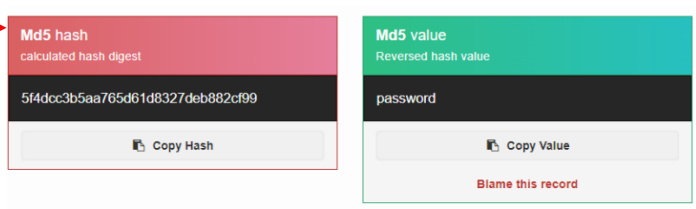
possiamo recuperare la versione della macchina su cui è hostato il database, nel nostro caso metasploitable si basa sulla versione di ubuntu 5.0.51a.



In maniera analoga, tramite la query

```
%' or 0=0 union select null, user() #
```

possiamo recuperare tutti gli utenti presenti all interno del database.



Infine, tramite la query

```
%' and 1=0 union select null,
concat(first_name,0x0a,last_name,0x0a,use
r,0x0a,password) from users #
```

possiamo recuperare le password associate ad ogni utente presente nel database. Da notare che le password sono criptate in codice hash md5, un semplice modo di poter recuperare il valore hash inverso può essere trovato tramite software dedicati come *john*.