Securitatea Datelor

Laboratorul nr.6 Atacuri SQL Injection

Nivel Mediu (BurpSuite)

## Cuprins

[Ce este SQL Injection? 3](#_Toc5364)

[Aplicații utilizate 3](#_Toc5365)

[Demonstrație atac SQL Injection 3](#_Toc5366)

[Temă 13](#_Toc5367)

# Ce este SQL Injection?

Acest tip de atac constă în inserarea unui script de tip SQL (Structured Query Language) într-o [aplicație w](https://www.link-academy.com/curs-introducere-in-dezvoltarea-aplicatiilor-android)eb 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.

# Aplicații utilizate

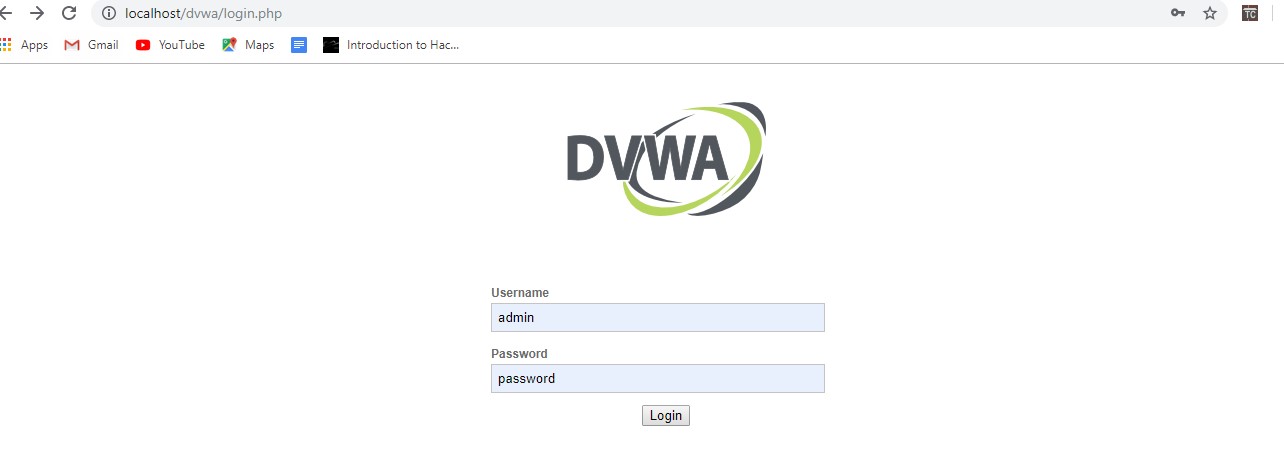
* Damn Vulnerable Web Application – (aplicația asupra căreia se va realiza atacul)
* BurpSuite (Utilitar specific atacurilor de tipul Brute Force – ( utilitar din Pentest Box) • Mozilla Firefox 45.0

# Demonstrație atac SQL Injection

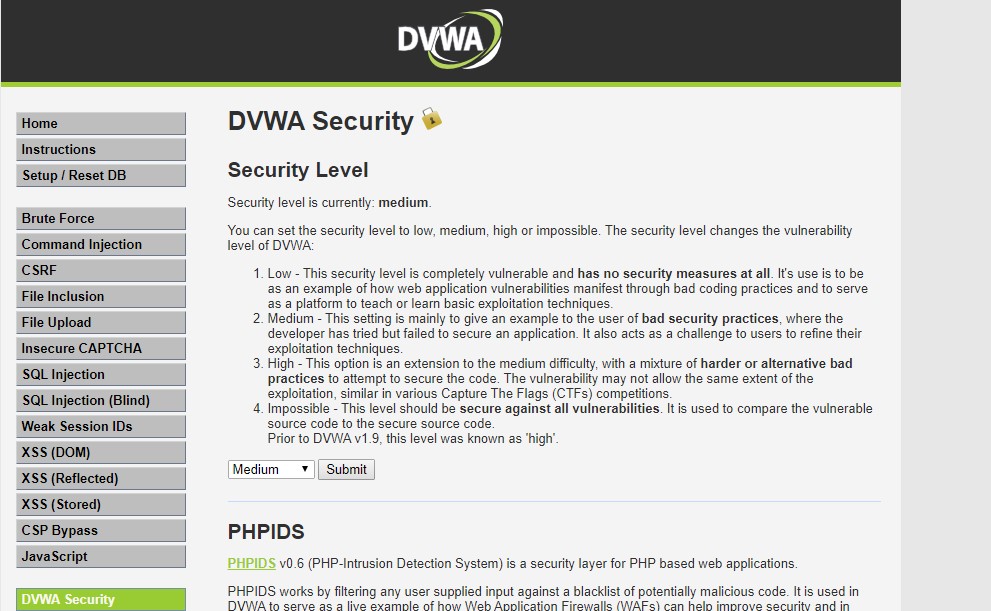
În pașii următori este descris un atac de tipul SQL Injection asupra aplicației DVWA – Security Level Medium

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 Medium și apăsăm butonul Submit

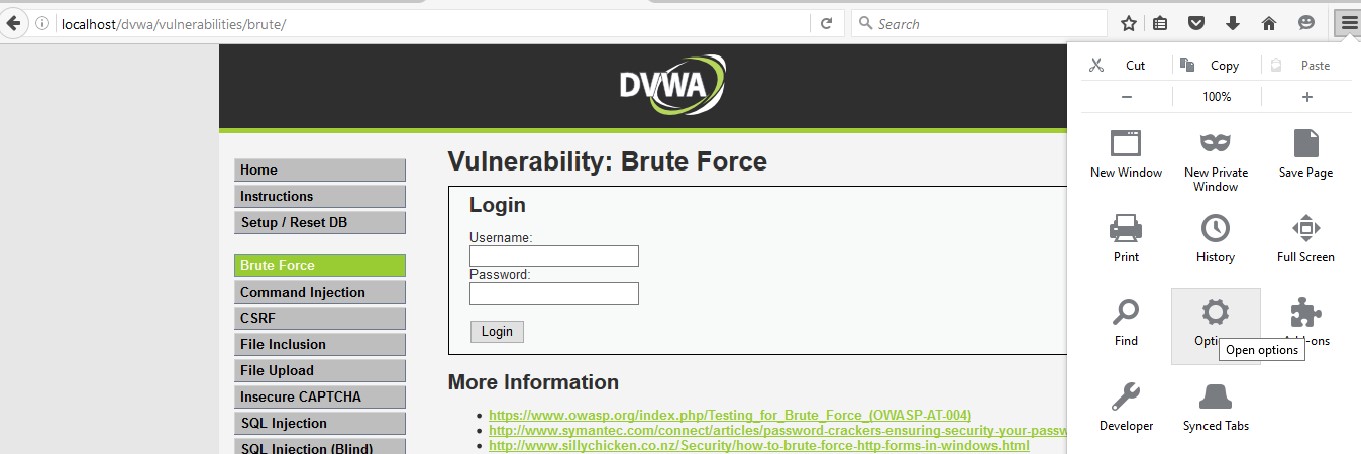


Pasul 3) Selectăm Sql Injection pentru a realiza atacurile de acest tip

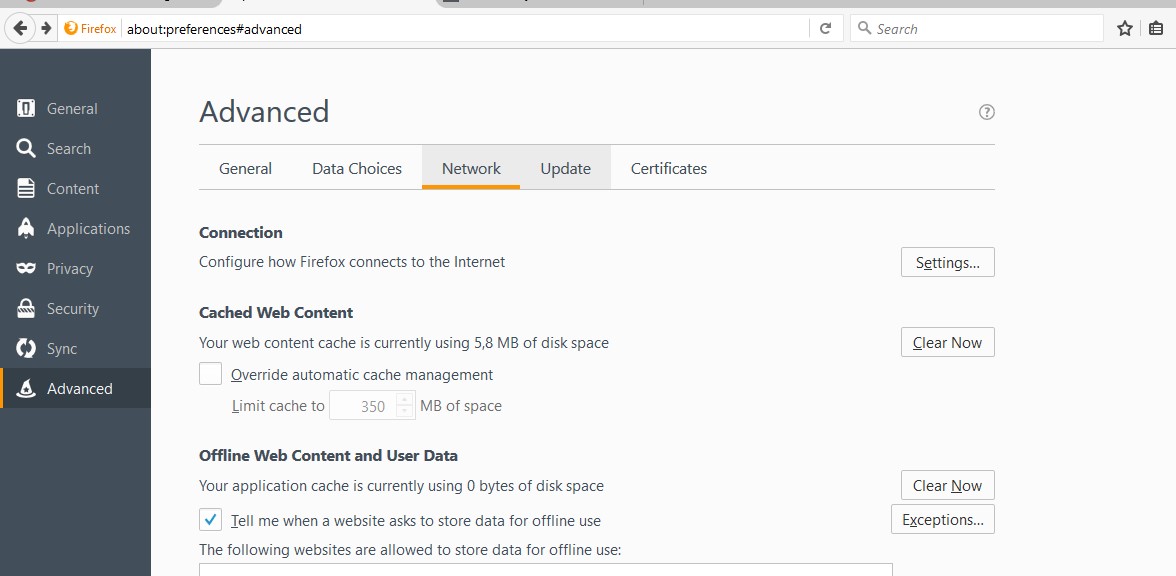


Pasul 4) Realizăm următoarele setări în browser Mozilla Firefox

* + Selectăm din Meniu categoria Options



* + Din tab-ul din partea stângă selectăm Advanced → Network



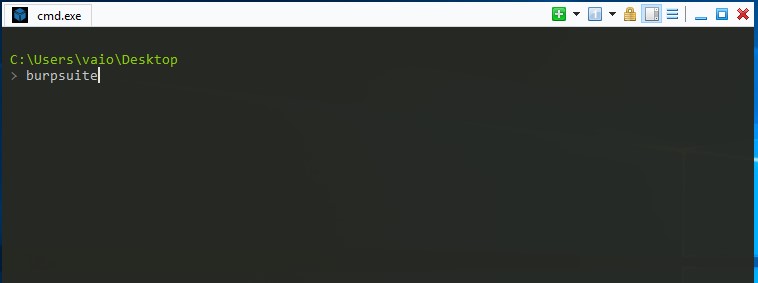
* + Dăm click pe Settings și la Connection Settings facem următoarele setări:

o Bifăm Manual proxy configuration o HTTP Proxy: 127.0.0.1 o Port: 8080 o Bifăm Use this proxy server for all protocols o Click butonul OK

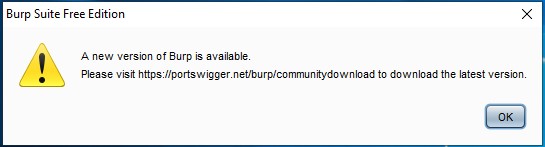


Pasul 5) Pornim aplicația BurpSuite din Pentest Box

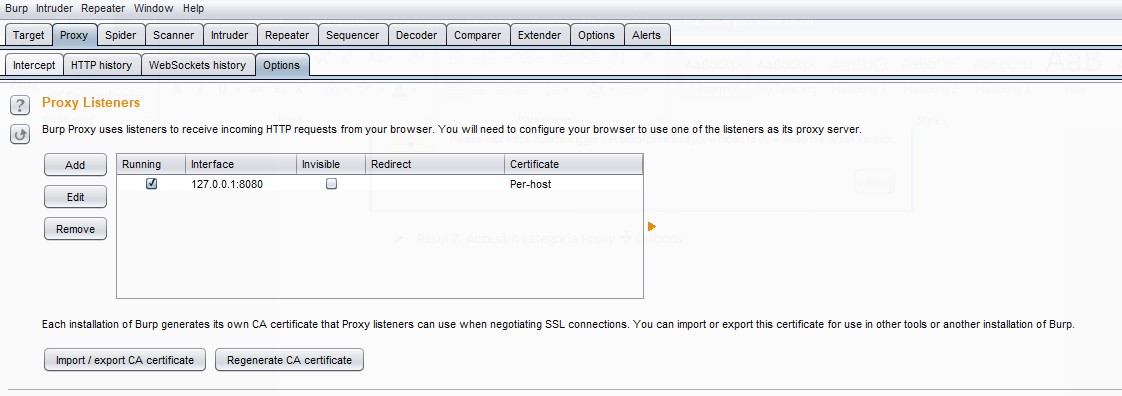
* scriem următoarea comandă în terminal:



Pasul 6) La primirea mesajului din următoarea imagine apăsăm butonul OK



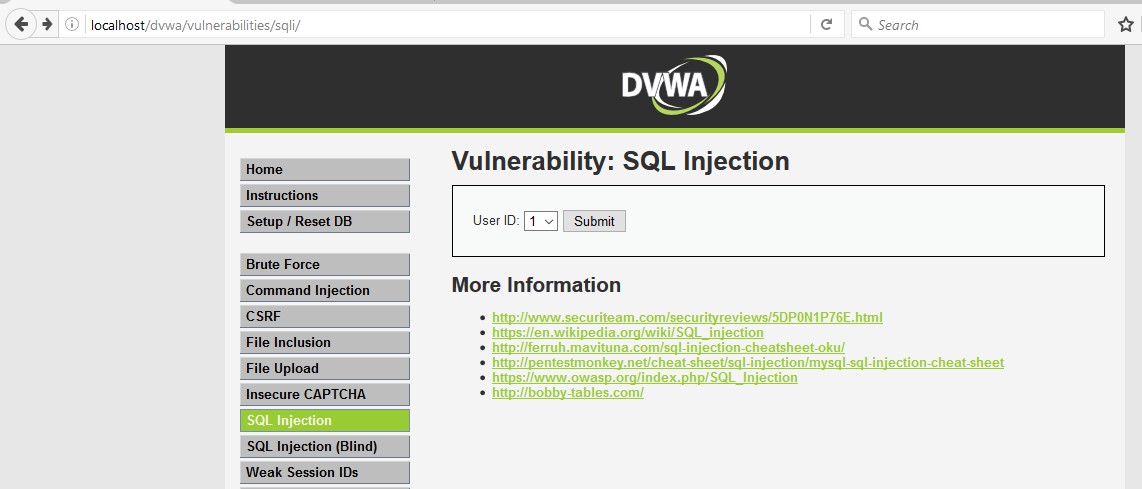
Pasul 7) Accesăm categoria Proxy → Options



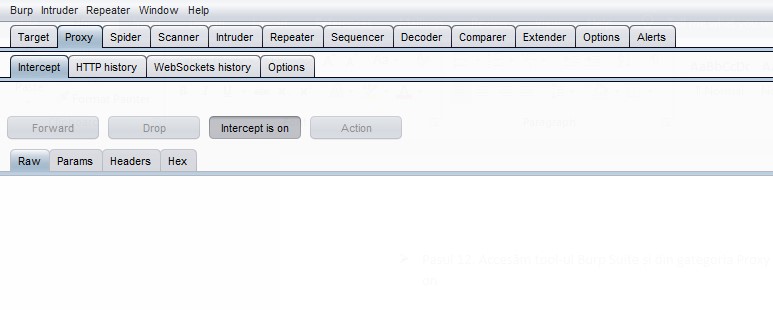
Pasul 8) Verificăm dacă sunt următoarele setări

* Running – bifat
* Interface: 127.0.0.1:8080

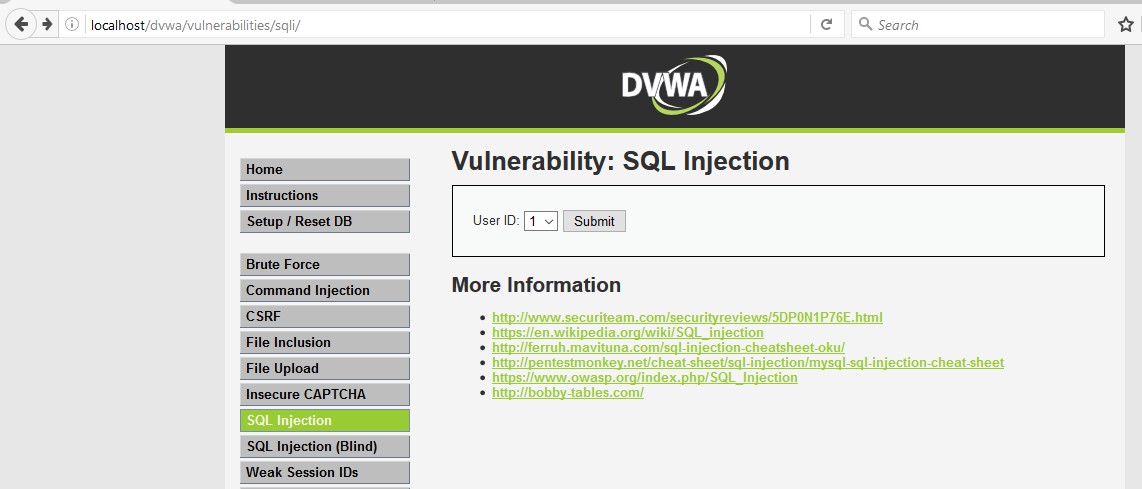
Pasul 9) Accesăm aplicația DVWA și selectăm tab-ul SQL Injection



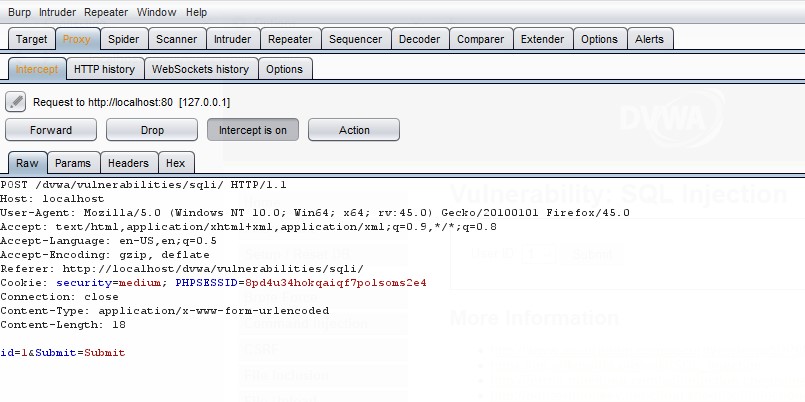
Pasul 10) Accesăm tool-ul Burp Suite și din gategoria Proxy → Intercept setăm Intercept is on



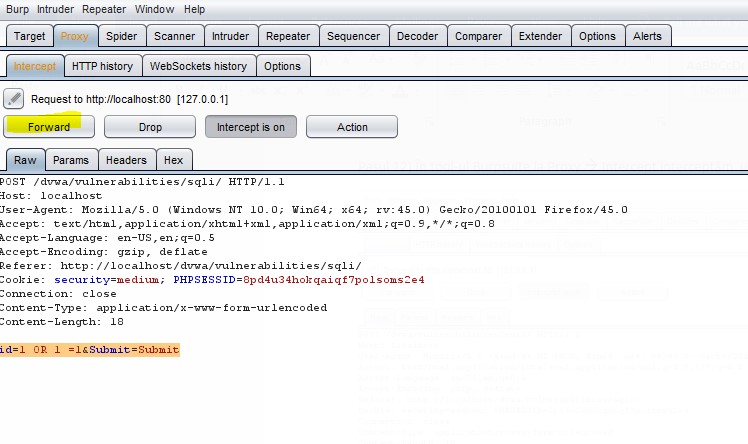
Pasul 11) Redeschidem Mozilla Firefox la pagina <http://localhost/dvwa/vulnerabilities/sqli/>și apăsăm butonul Submit



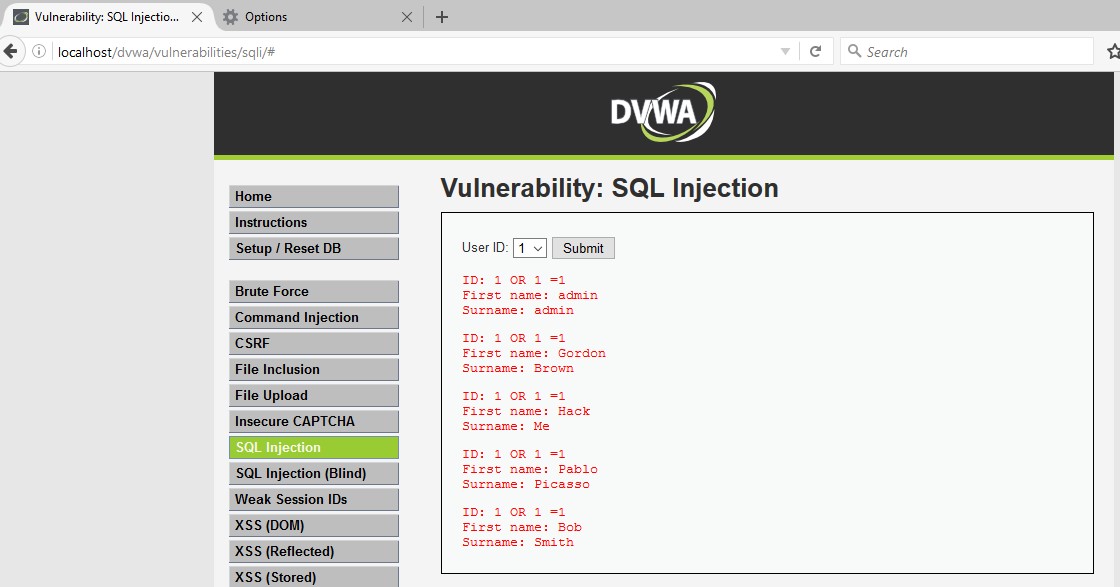
Pasul 12) În tool-ul Burpsuite la Proxy → Intercept interceptăm următorul text



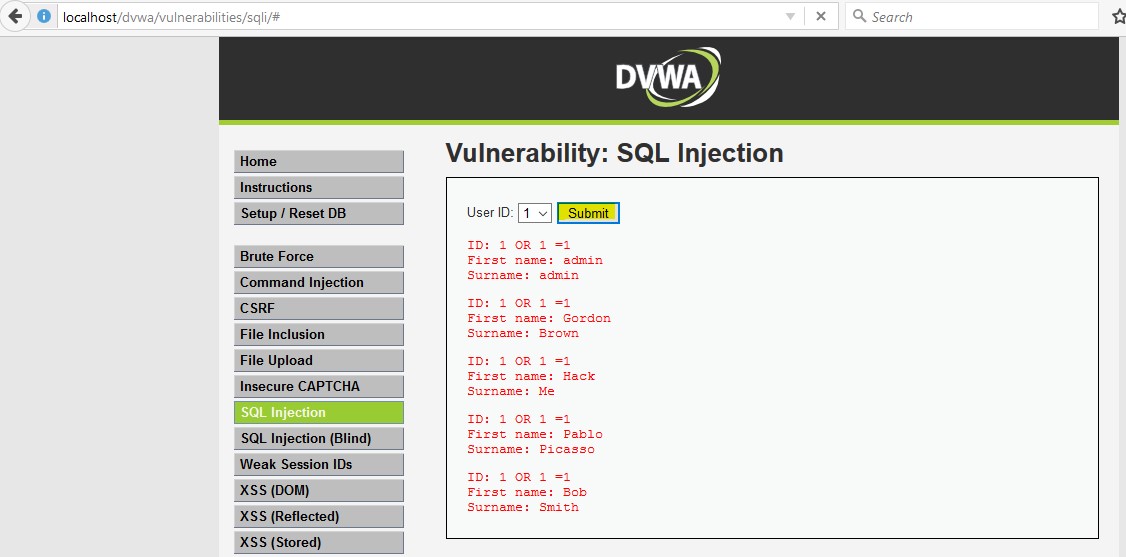
Pasul 13) Ultimul rând id=1&Submit=Submit îl înlocuim cu id=1 OR 1 =1&Submit=Submit și apăsăm butonul Forward



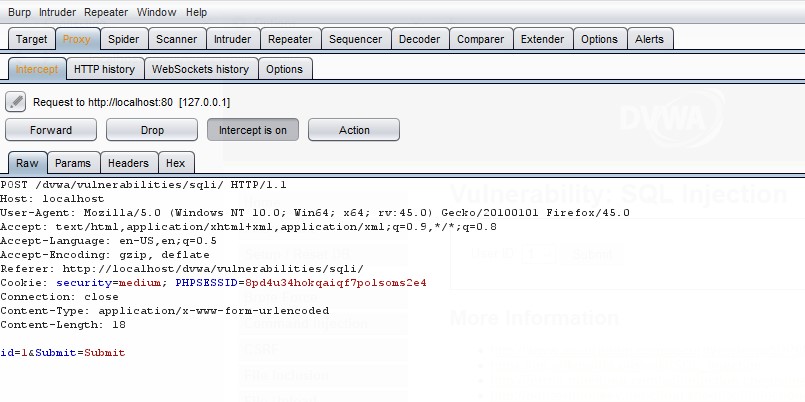
Pasul 14) În browser se afișează userii din baza de date



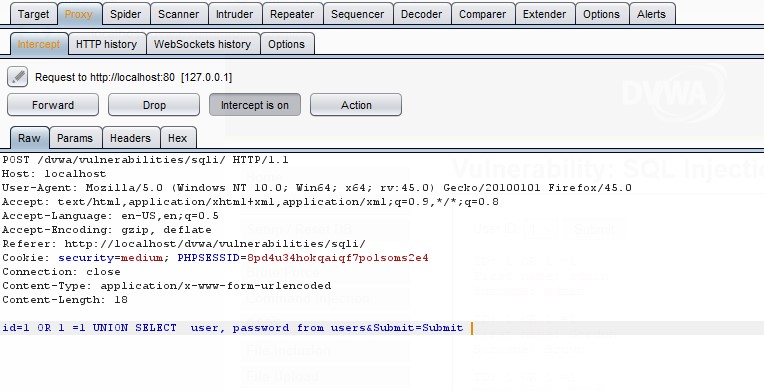
Pasul 15) Apăsăm butonul Submit



Pasul 16) În tool-ul Burpsuite la Proxy → Intercept interceptăm următorul text

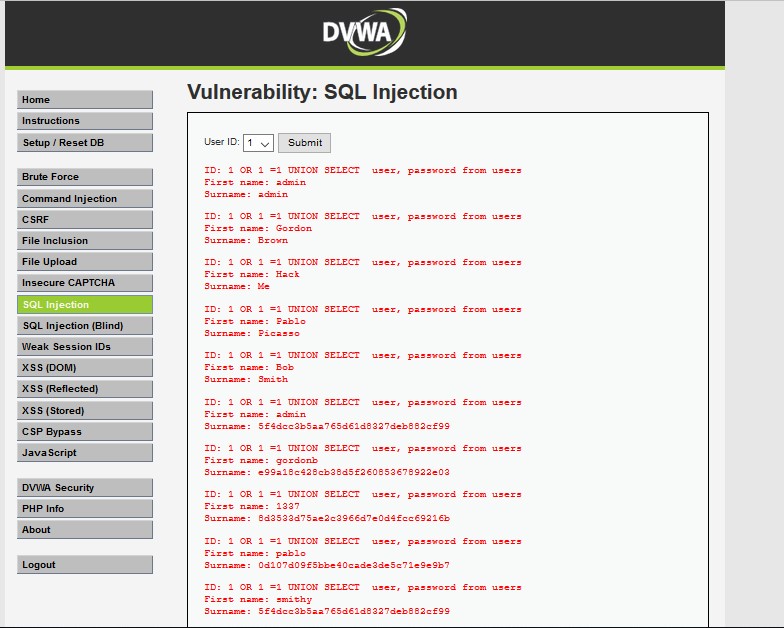


Pasul 17) Ultimul rând id=1&Submit=Submit îl înlocuim cu id=1 OR 1 =1 UNION SELECT user, password from users&Submit=Submit și apăsăm butonul Forward

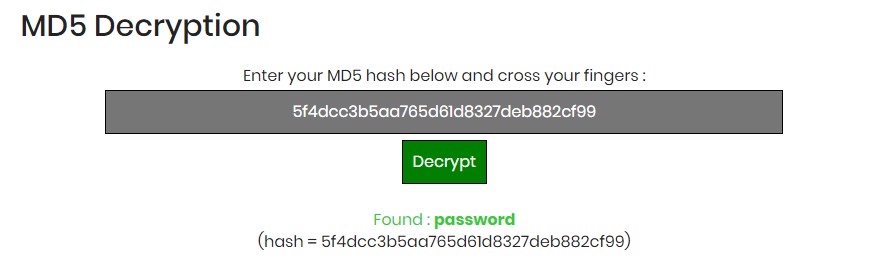


Pasul 18) În browserul Mozilla Firefox au fost identificate următoarele credențiale (parola este criptată md5)

Pasul 20) Accesăm următorul link <https://www.md5online.org/md5-decrypt.html>prentru a decripta parola pentru user-ul:



• admin(hash md5: 5f4dcc3b5aa765d61d8327deb882cf99) = password



# Temă

1) Aflați parola și pentru umrătorii useri:

* gordonb
* 1337
* pablo
* smithy