Securitatea Datelor

Laboratorul nr.1:Configurarea Laboratorului

**Cuprins**

[1. Introducere 2](#_Toc8767)

[2. Scop 2](#_Toc8768)

[3. Principalele tipuri de vulnerabilități web 2](#_Toc8769)

[4. Aplicații necesare pentru configurarea laboratorului 3](#_Toc8770)

[4.1 Descriere XAMPP 3](#_Toc8771)

[4.1.1 Instalare XAMPP 3](#_Toc8772)

[4.2 Descriere DVWA 8](#_Toc8773)

[4.2.1 Instalare DVWA 8](#_Toc8774)

[4.3 Descriere PentestBox 13](#_Toc8775)

[4.3.1 Instalare PentestBox 13](#_Toc8776)

[5. Studiu individual 15](#_Toc8777)

# Introducere

Dezvoltarea internetului a creat premisa apariției vulnerabilităților specifice oricărui produs tehnologic. Numărul acestora este în continuă creștere deși cele mai populare atacuri se bazează pe vulnerabilități identificate pentru prima dată acum câțiva ani buni.

# Scop

Dezvoltarea cunoștințelor despre securitatea aplicațiilor web, identificarea și exploatarea celor mai întâlnite vulnerabilități.

# Principalele tipuri de vulnerabilități web

Pe parcursul orelor de laborator vom încerca să identificăm și să exploatăm vulnerabilități web de tipul:

* Brute Force
* Command Injection
* CSRF
* File Inclusion
* File Upload
* SQL Injection
* SQL Injection Blind
* XSS Dom
* XSS Reflected
* XSS Stored

# Aplicații necesare pentru configurarea laboratorului

Pentru a putea realiza scanări si atacuri asupra aplicațiilor web avem nevoie de următoarele aplicații:

* XAMPP
* DVWA
* PentestBox



## Descriere XAMPP

XAMPP este o distribuţie Apache uşor de instalat ce conţine MySQL, PHP şi Perl. Pachetul este open source XAMPP și are scopul de a găzdui local aplicația web vulnerabilă. Este disponibilă pentru următoarele sisteme de operare: Windows, Linux, OS X.

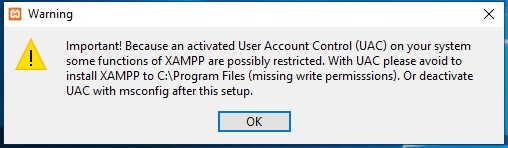


### Instalare XAMPP

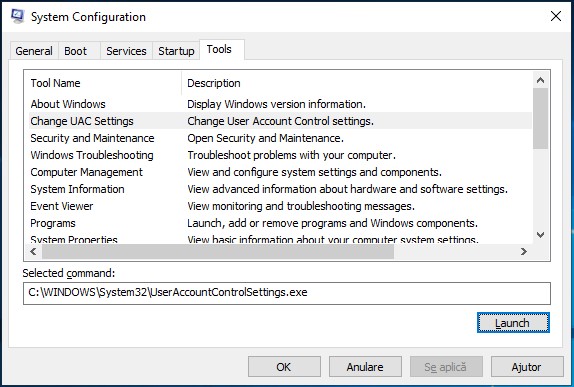
Pasul 1) Aplicația XAMPP se poate descărca de pe site-ul oficial de pe următorul link: <https://www.apachefriends.org/ro/download.html>

Pasul 2) După finalizarea procesului de descărcare, rulăm fișierul pentru a porni instalarea propriu-zisă.

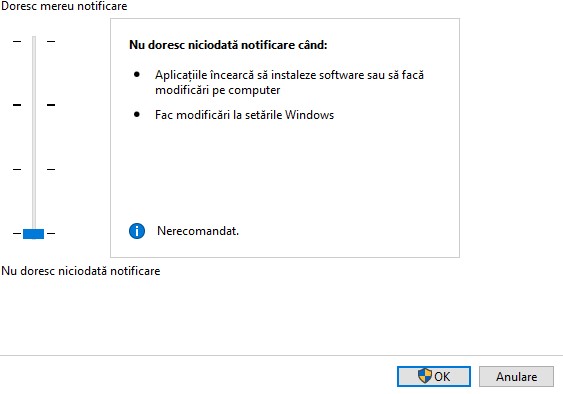
Pasul 3) În anumite cazuri putem primi următorul mesaj :



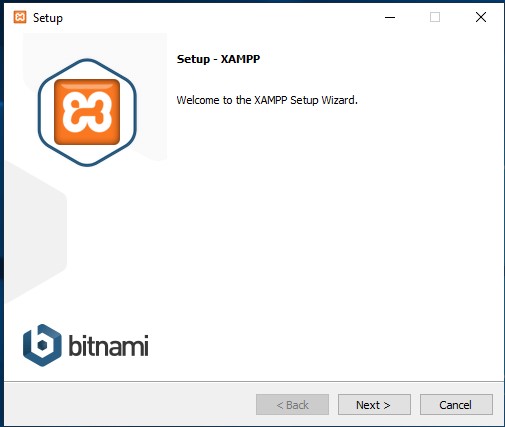
În acest caz, tastăm în Start comanda msconfig



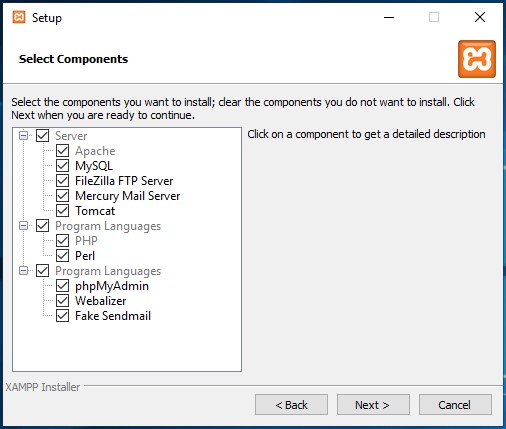
După deschiderea Ferestrei System Configuration, din tabul Tools, lansăm Change UAC Settings și selectăm nivelul minim ca în următoarea imagine:



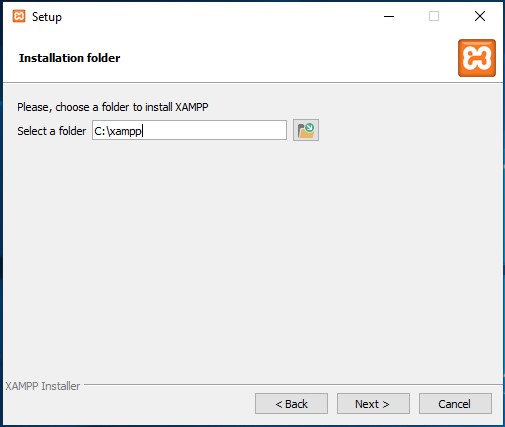
Pasul 4) Setup  Next



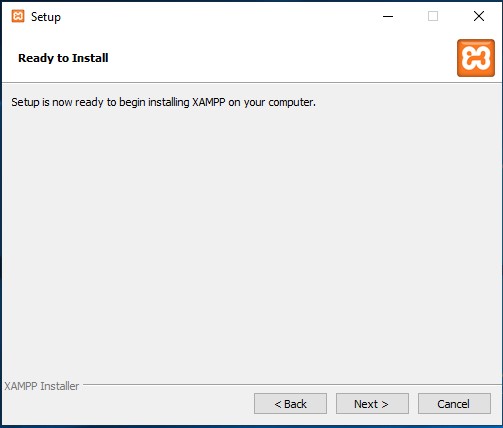
Pasul 5) Selectăm toate componentele



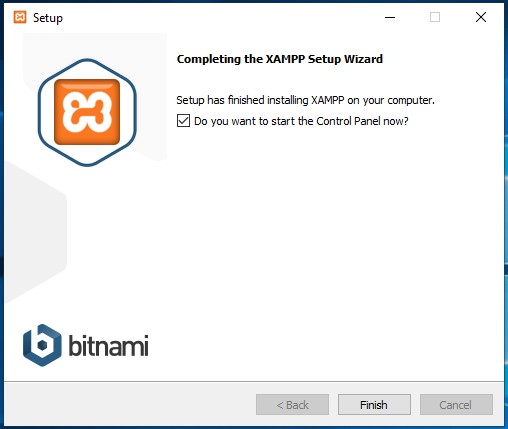
Pasul 6) Selectăm locația unde dorim să instalăm aplicația



Pasul 7) Aplicația este gata pentru instalare



Pasul 8) Finalizarea procesului de instalare



## Descriere DVWA

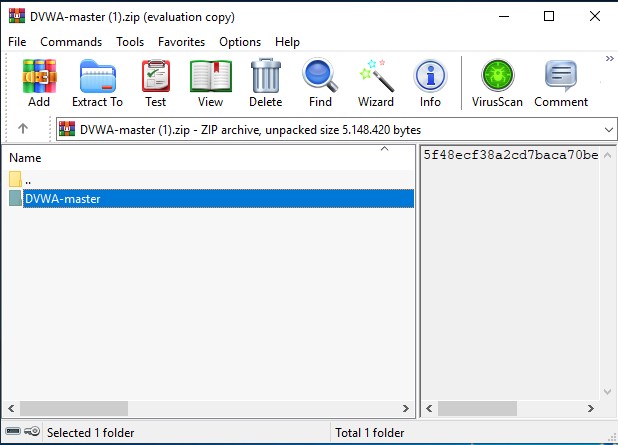
DVWA = Damn Vulnerable Web Application - este o aplicatie web scrisa in PHP/MySQL ce contine vulnerabilitati si este folosita pentru testare in scop didactic.



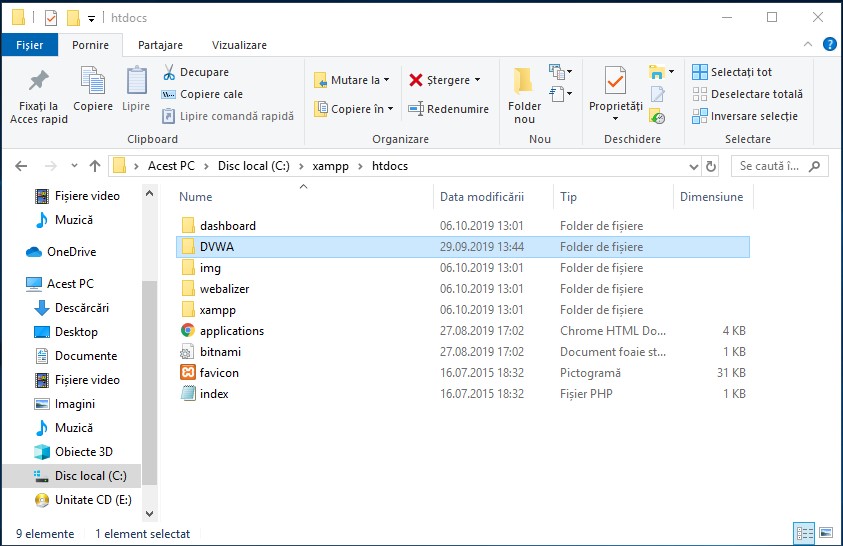
### Instalare DVWA

Pasul 1) Descărcam aplicația de pe site-ul: [www.dvwa.co.uk](http://www.dvwa.co.uk/)

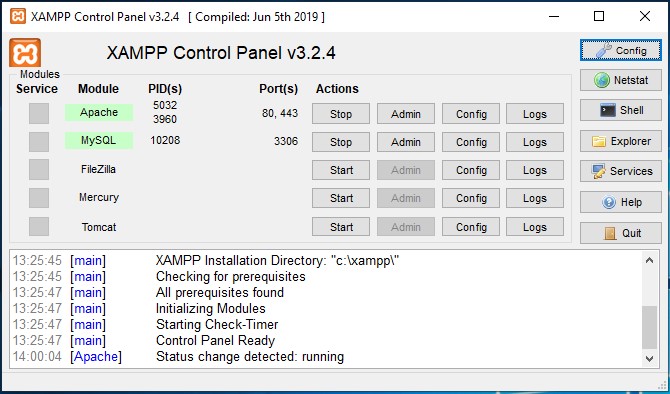
Pasul 2) Dezarhivăm fișierul descărcat



Pasul 3) Redenumim fișierul dezarhivat din DVWA-master în DVWA și îl copiem in următoarea locație din aplicația XAMPP: C:\xampp\htdocs



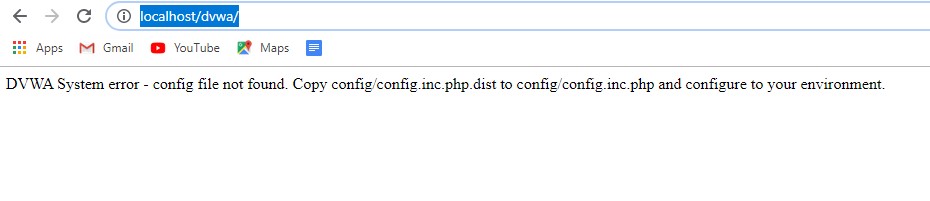
Pasul 4) Accesăm aplicația XAMPP și pornim modulul Apache și modulul MySQL



Pasul 5) Pentru configurarea aplicației DVWA, din browser accesăm următorul link:

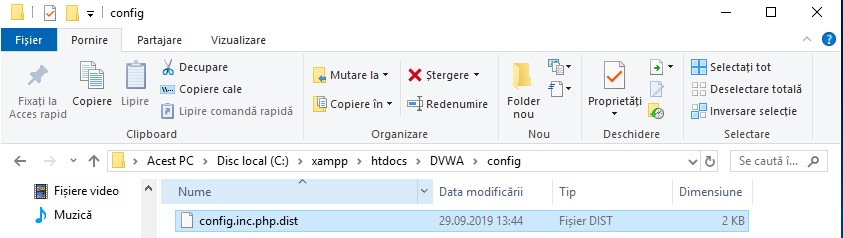
<http://localhost/dvwa/>

Pasul 6) Putem întălni următoarea eroare

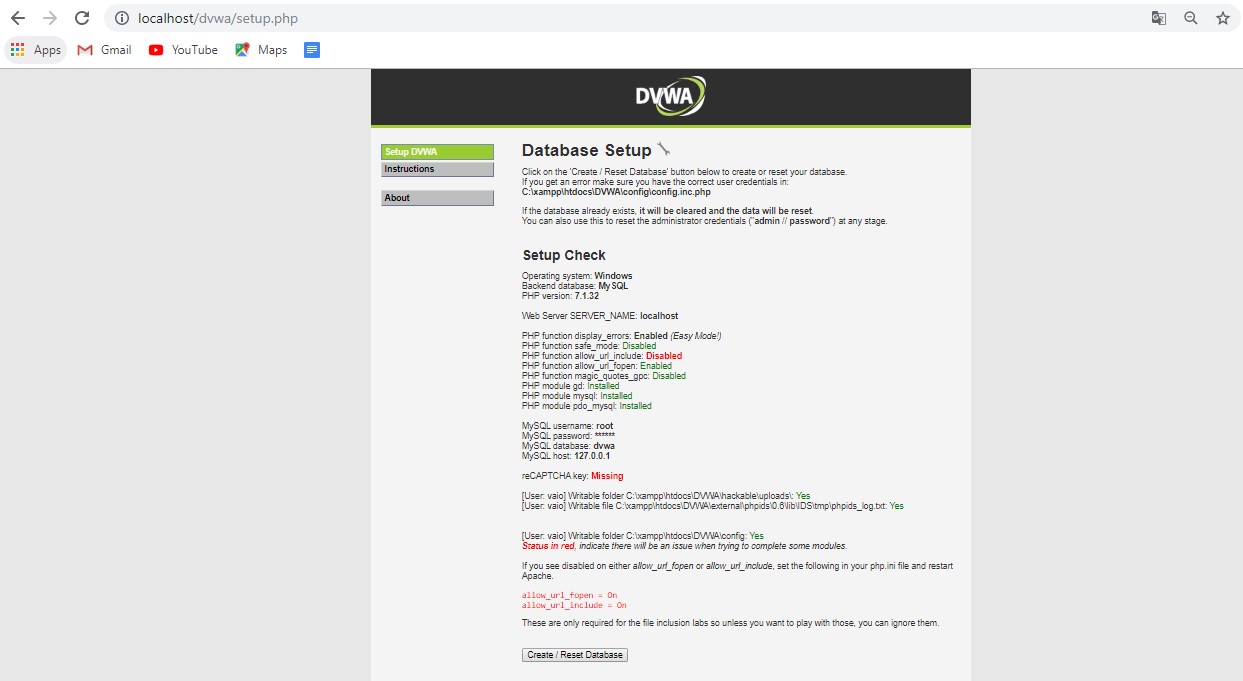


Pentru remedierea acestei erori facem urătoarele setări: - accesăm locația: C:\xampp\htdocs\DVWA\config

- moficăm extensia fișierului config.inc.php.dist în config.inc.php

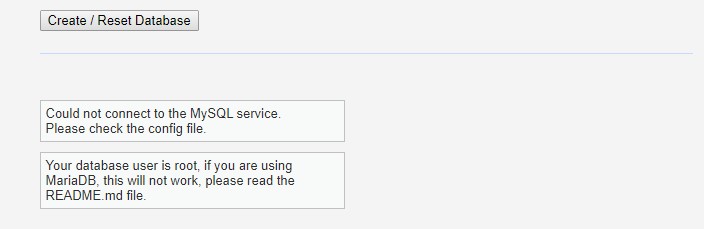


Pasul 7) Accesăm din nou <http://localhost/dvwa/>și va apărea următoarea fereastră



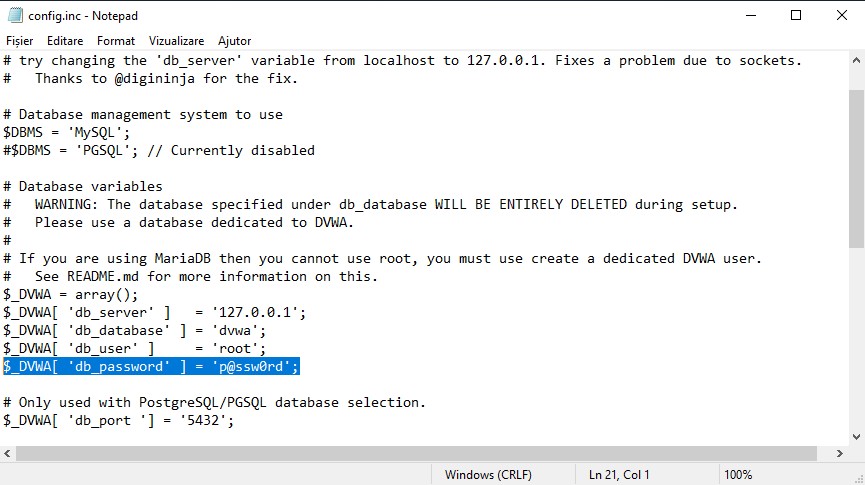
Pasul 8) În partea de jos a paginii avem butonul Create/ Reset Database

La crearea/ resetarea bazei de date putem întălni următoarea eroarea



O putem remedia făcând următoarele setări:

- deschidem cu notepad fișierul config.inc din locația C:\xampp\htdocs\DVWA\config



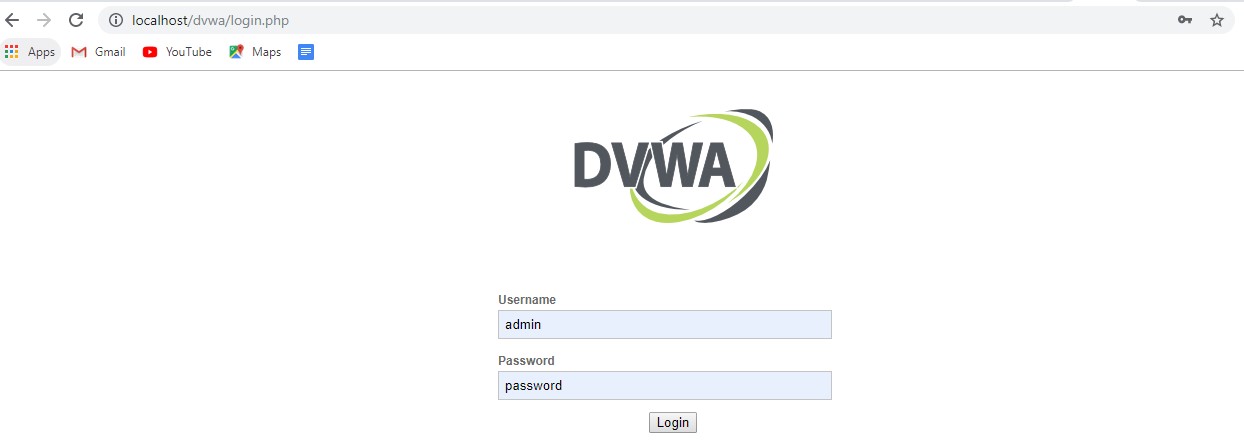
-înlocuim $\_DVWA[ 'db\_password' ] = 'p@ssw0rd'; cu $\_DVWA[ 'db\_password' ] = '';

-acum ar trebui să putem reseta baza de date și să accesăm pagina de autentificare

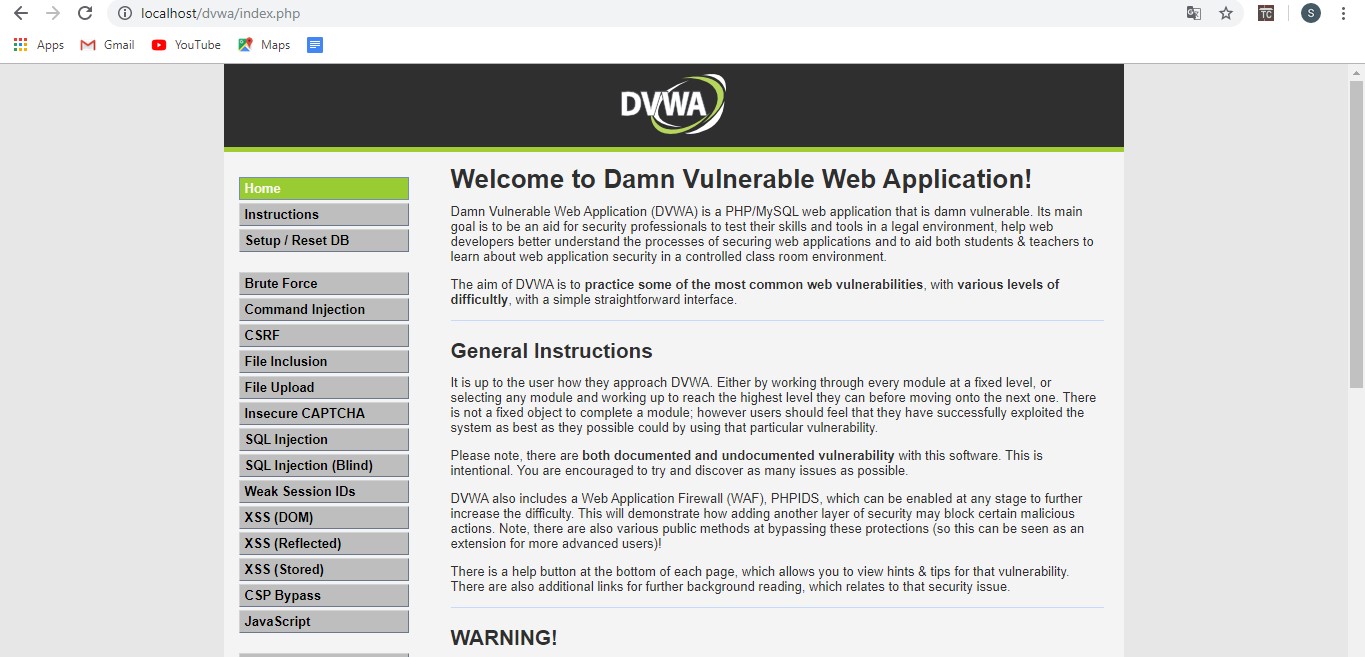
Pasul 9) Autenteficare pe pagina <http://localhost/dvwa/login.php>

Username: admin

Password: password



Pasul 10) În meniul din partea stângă găsim principalele vulnerabilități pe care le vom studia la laborator



## Descriere PentestBox



PentestBox este un mediu portabil de testare din punct de vedere al securității, preconfigurat pentru sistemul de operare Windows. În esență, oferă toate instrumentele de securitate ca pachet software și vă permite să le rulați nativ pe Windows. Acest lucru elimină efectiv cerința de mașini virtuale sau medii dualboot pe Windows.

Principalele tool-uri pentru testarea securității aplicațiilor web sunt următoarele:

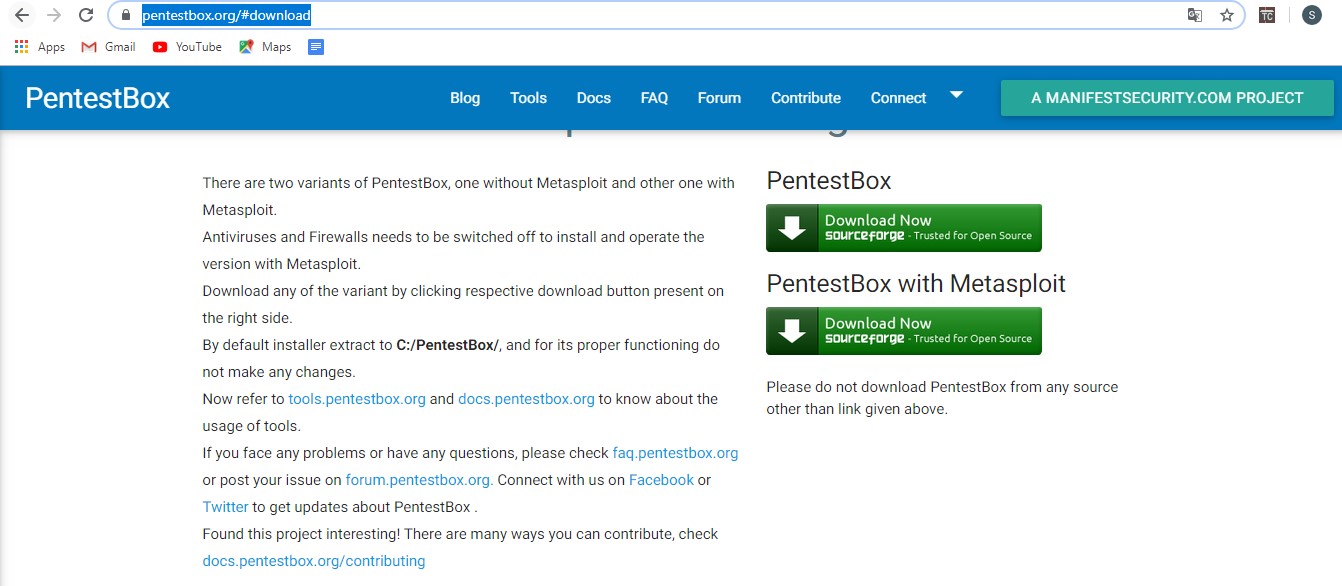
* Burp Suite  Commix
* [Golismero](https://github.com/golismero/golismero)
* [Nikto](https://github.com/sullo/nikto)
* [SqlMap](http://sqlmap.org/)
* [Vega](https://subgraph.com/vega/)
* [Wpscan](https://github.com/wpscanteam/wpscan/)

Lista completă cu utilitarele de testare poate fi accesată la următoarea adresă web: [https://tools.pentestbox.org](https://tools.pentestbox.org/)

### Instalare PentestBox

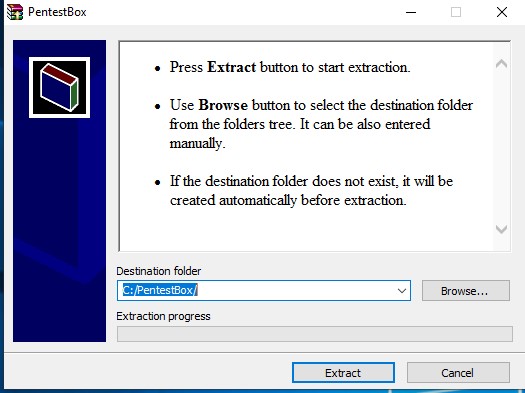
Pasul 1) Este PentestBox este open source și se poate downloada de pe linkul

<https://pentestbox.org/#download>



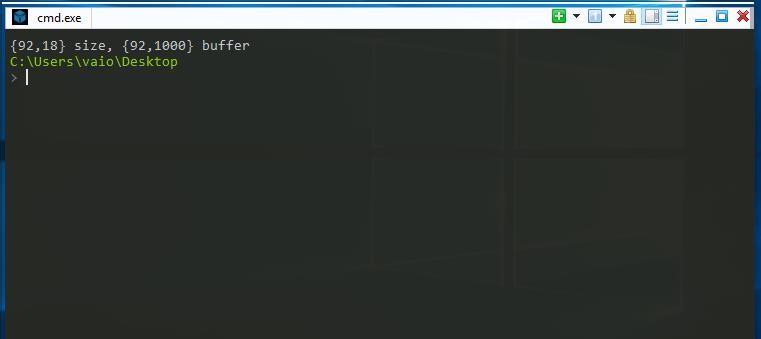
Recomndare download: Versiunea PentestBox ce conține utilitarul Metasploit

Pasul 2) Deschidem fișierul descărcat și extragem datele în urmatoarea locație C:/PentestBox/



Pasul 3) După finalizarea instalării accesăm executabilul aplicației din următoarea locație

C:\PentestBox\PentestBo



# Studiu individual

<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project><https://www.kali.org/><https://www.cybrary.it/><https://www.theprohack.com/2009/09/learn-web-hacking-using-dvwa.html>