# Securitatea Datelor

**Laboratorul nr.9: Vulnerabilitate: File Upload Level: Low**

1CUPRINS:

1. Definiție ........................................................................................................................................... 3
2. Recomandare .................................................................................................................................. 3
3. Demonstrație atac File Uploud ....................................................................................................... 3

## 1.DEFINIȚIE

Acest tip de vulnerabilitate, practic, nu e o vulnerabilitate, de cele mai multe ori. Dacă aveți un serviciu de upload pe server, aveți grijă ca utilizatorii să nu poată uploada fisiere PHP. Nu faceti acest lucru verificând ca extensia să nu fie ".php". recomandarea mea e sa cititi fisierul ( in caz ca nu se pot uploada fisiere mari ) si sa verificati daca contine cod PHP.

**2.** RECOMANDARE

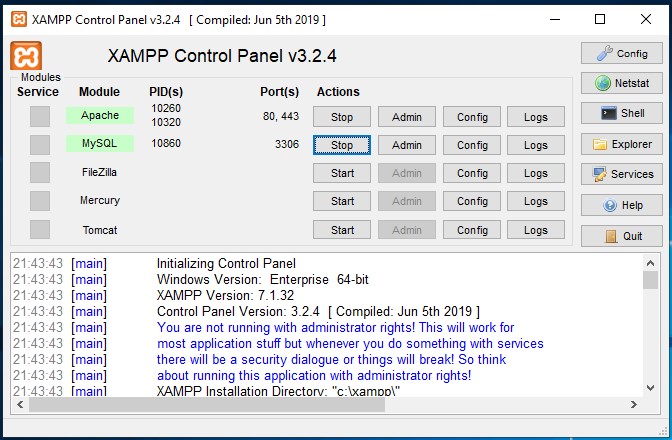
Citiți fisierul ( în caz că nu se pot uploada fișiere mari ) și să verificați dacă conține cod PHP.

$fisier=file\_get\_contents($\_FILES['fisier']['tmp\_name']));

if(explode("<?php",$fisier) 1 && explode("?>",$fisier)) print "Cod PHP detectat";

## 3.DEMONSTRAȚIE ATAC FILE UPLOUD

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



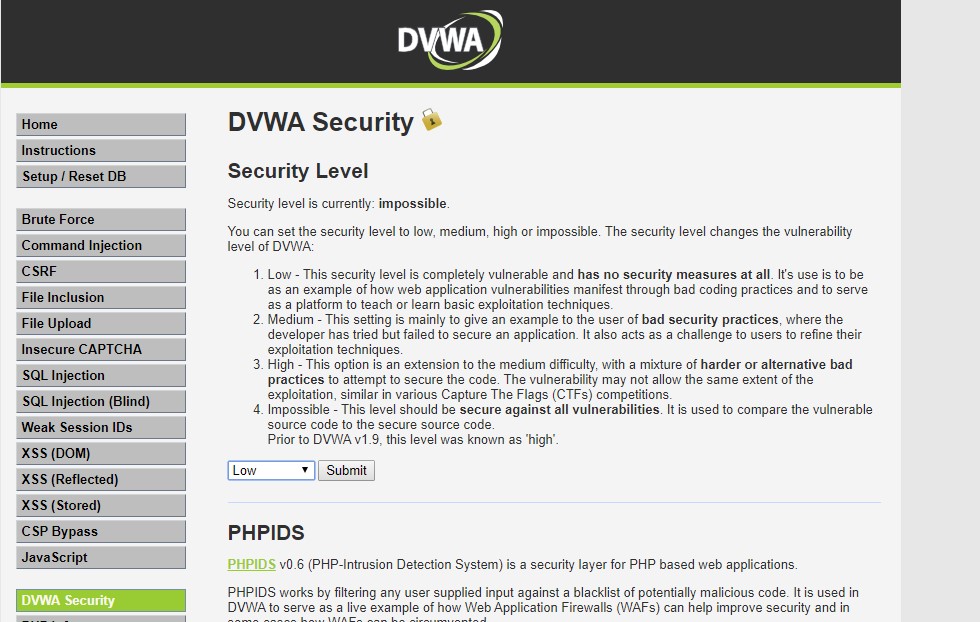
* Pasul 2. Accesăm aplicația dvwa <http://localhost/dvwa/login.php>



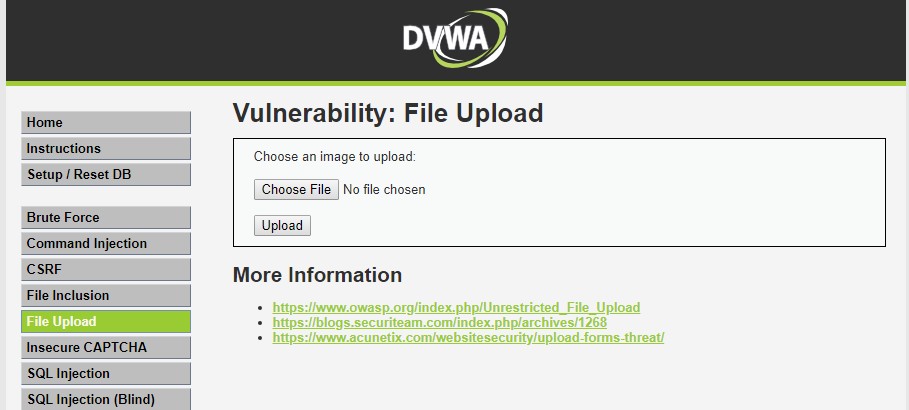
Ne autentificăm cu următoarele credențiale:

Username: admin Passsword: password

* Pasul 3. Din tab-ul din partea stângă accesăm categoria DVWA Security – setăm nivelul de securitate Low și apăsăm butonul Submit

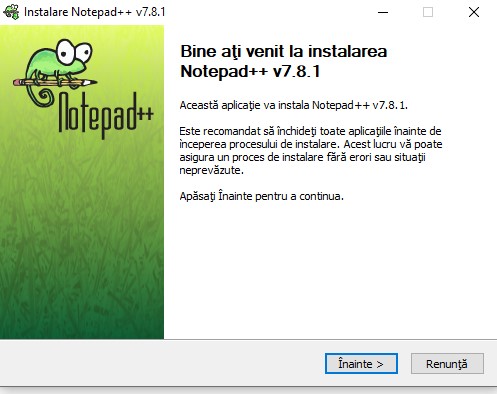


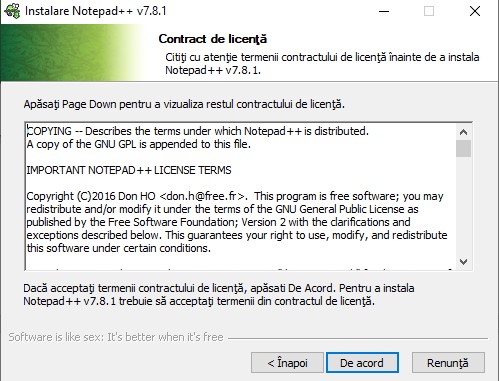
* Pasul 4. Selectăm din tab-ul din partea stăngă categoria File Uploud

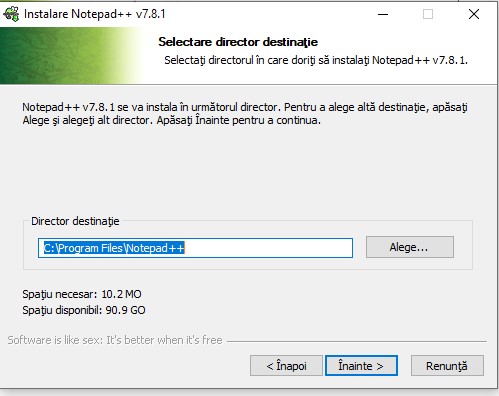


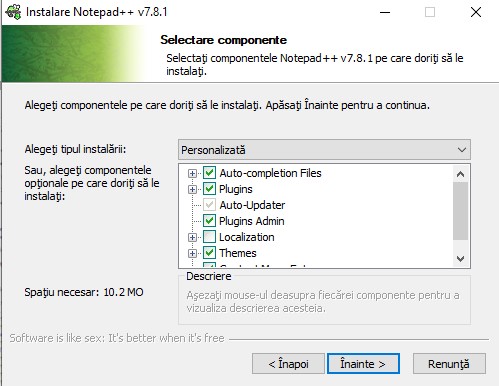
* Pasul 5. Descărcăm aplicația Notepad++ și o instalăm

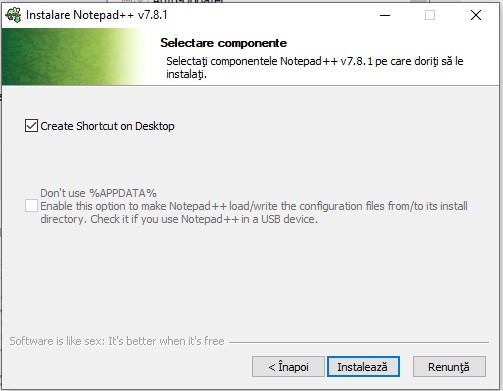
Link: <https://notepad-plus-plus.org/downloads/v7.8.1/>







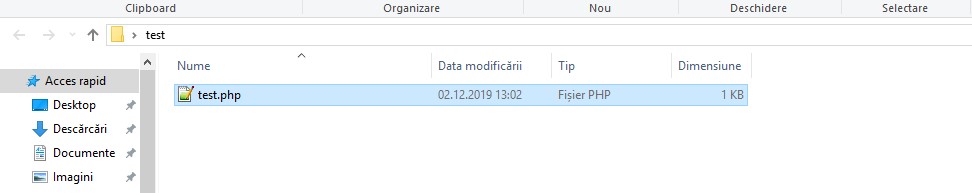




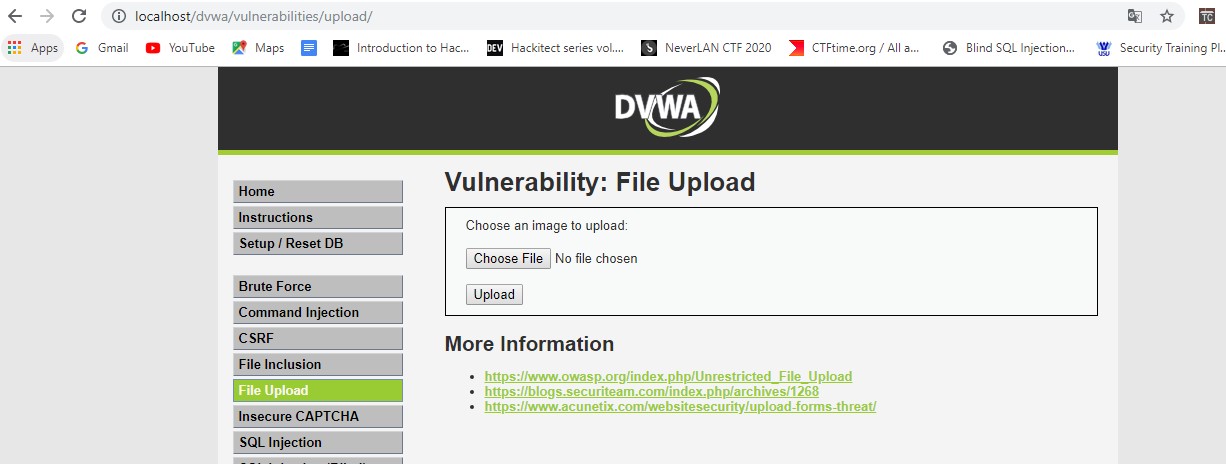
* Pasul 6. Deschidem notepad++ și tastăm următorul cod:



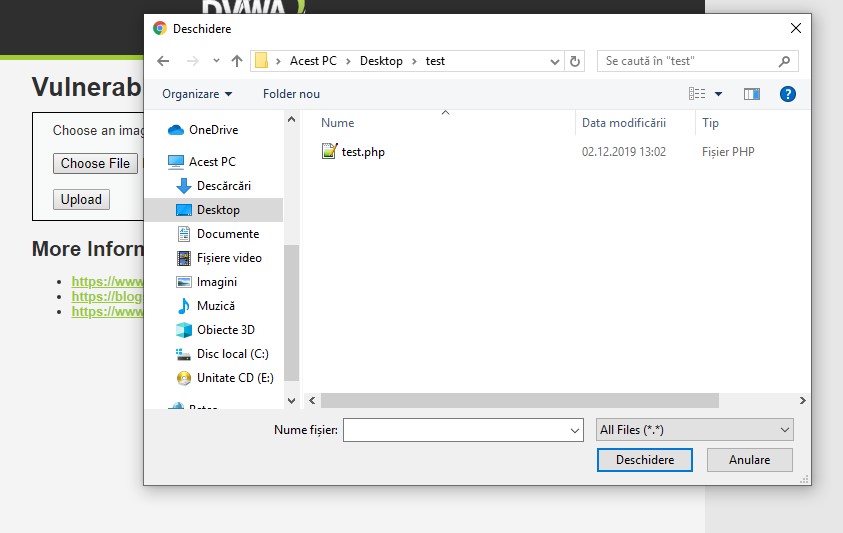
* Pasul 7. Salvăm cu extensia .php



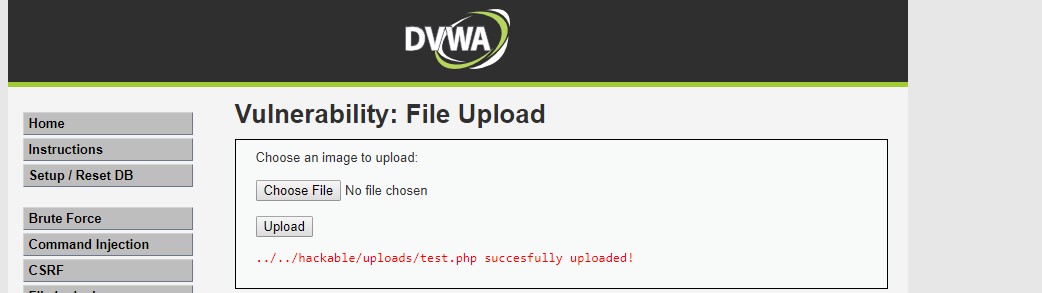
* Pasul 8. În aplicația DVWA în tabul File Upload



* Pasul 9. Facem click pe butonul Choose File și selecăm fișierul creat la pasul 7 (test.php)



* Pasul 10. Facem click pe butonul Uploud



- Am identificat calea vulnerabilă file uploud și anume:

/hacktable/uploads/test.php