Instituto Tecnológico de San Juan del Río

Tópicos de Ciberseguridad

Tema 1

R005

Documentación del proceso para parchar un ejecutable

P R E S E N T A:

Equipo Púrpura

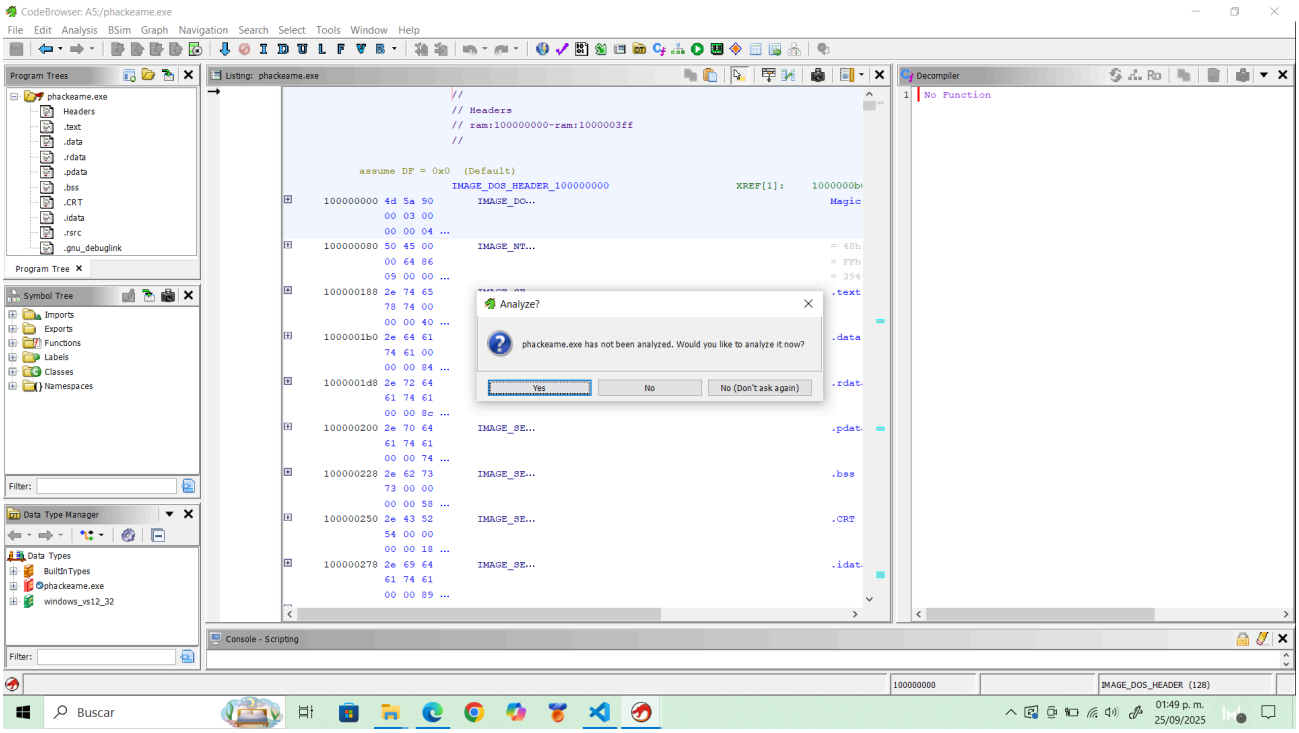
PERIODO
AGOSTO-DICIEMBRE 2025

Proceso para parchar el ejecutable proporcionado por el profesor

1. Abrir el archivo ejecutable con la herramienta Ghidra

Se creó una carpeta de trabajo en la que se importó el ejecutable. Para abrirlo sólo se hace clic sobre este mismo, (aparece una imagen de Ghidra).

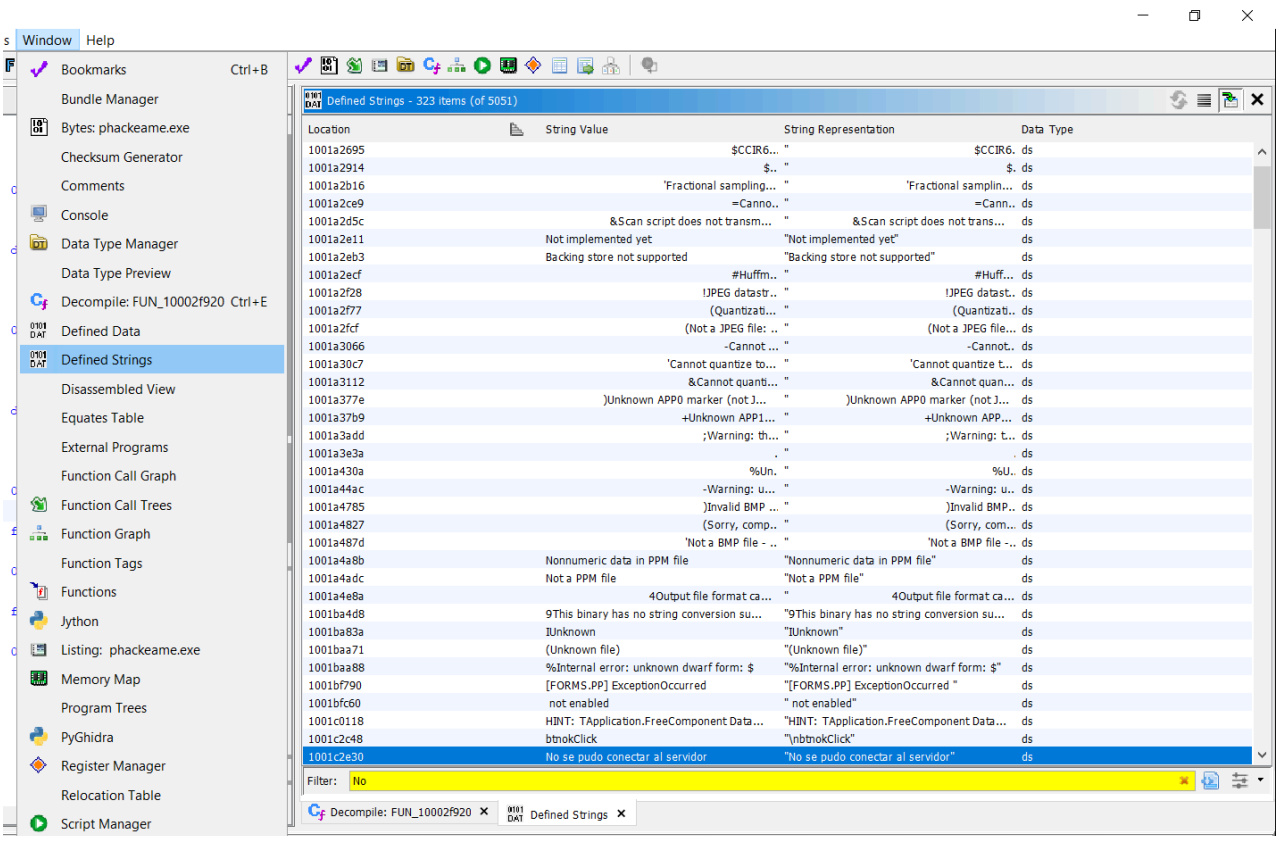
Se acepta para que se confirmen algunos criterios del análisis. Y se podrá acceder a la parte del desensamblador en donde podemos observar el código máquina (en ensamblador) del ejecutable.



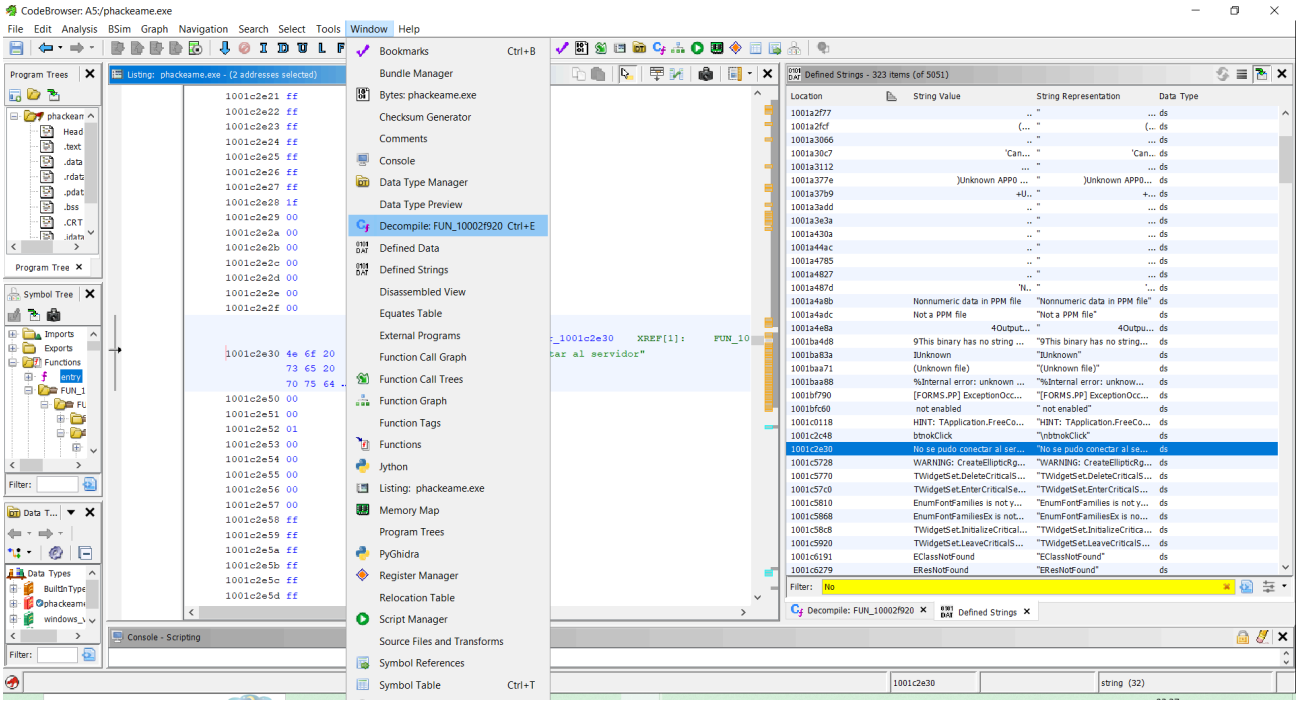
2. Análisis

Se localizó la línea que contiene la validación que se debe saltar. Se sabe que la aplicación muestra un mensaje luego de que se intenta colocar un usuario o contraseña incorrectos, y lo que se requiere es que el ejecutable funcione y dé el acceso sin importar el usuario o contraseña que se coloquen .

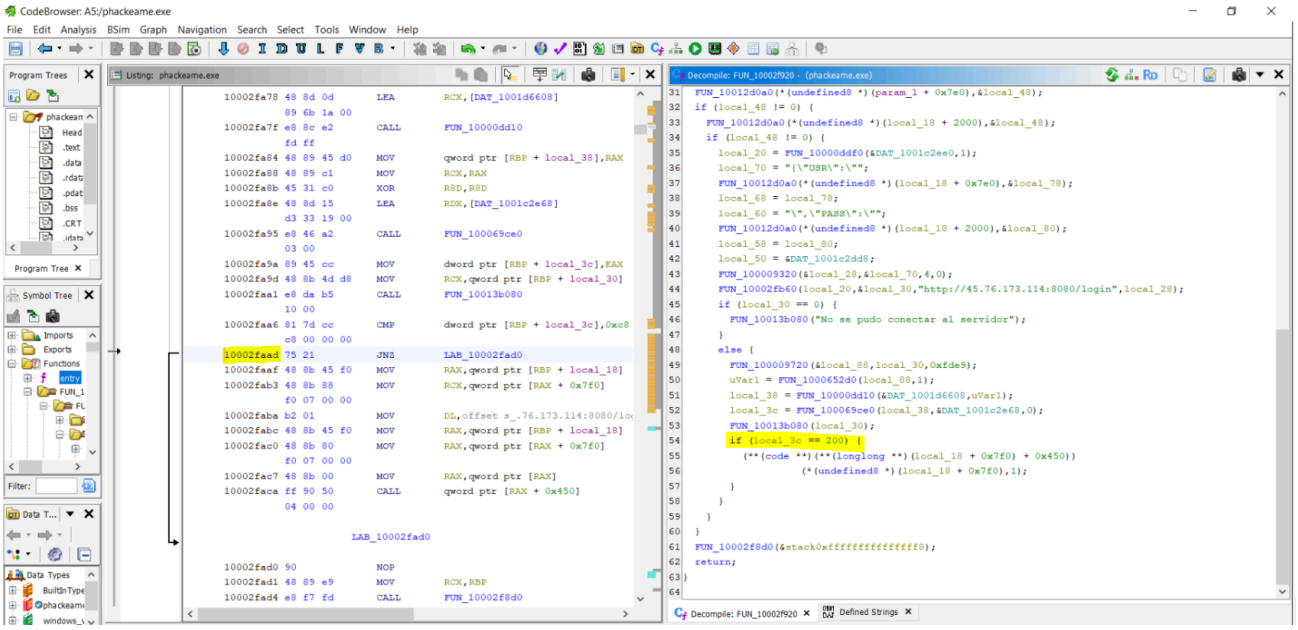
Se identificó la parte del código que contiene la salida: “No se pudo conectar al servidor”. Lo que permite Ghidra es hacer un filtrado para localizar de manera más sencilla esta location en el código, para ello seleccionamos en la barra superior: window > Defined Strings.



Con ello obtenemos la location del string, al darle clic nos manda a ella dentro del código que se está visualizando del ejecutable. Ahora volvemos a seleccionar: “window”, y esta vez en la opción de “Decompile”. Esto para transformar el código en ensamblador en un código en pseudo-C (más legible para nosotros).



Una vez en con el código en C, localizamos la siguiente función y se debe seleccionar sobre ella para que nos devuelva su equivalente en la parte del lado del ensamblador.

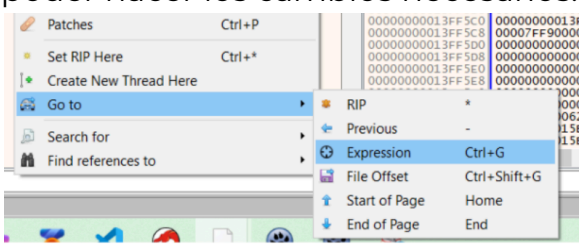


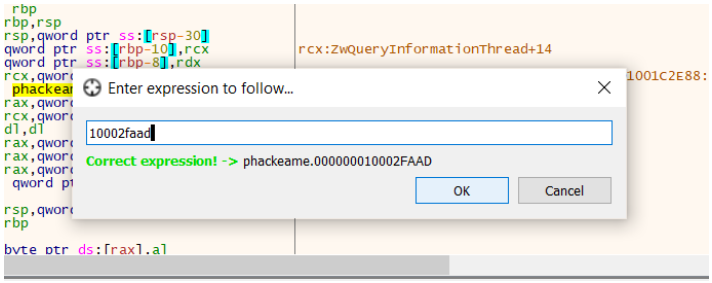
Antes se debe comprender que es lo que hace ese condicional que se marcó en la imagen. Este if se encarga de verificar si la respuesta del servidor indica un acceso válido en donde el servidor devuelve “HTTP 200”, y se llama a una función que está definida para confirmar que el login remoto fue exitoso y ejecuta la acción correspondiente.

En otras palabras, ese condicional es la puerta que valida si el login fue exitoso. Por lo que logrando que se salte esa parte, siempre se ejecutará el callback, y es así como en la ventana del programa permitirá el acceso aunque la contraseña o usuario sean incorrectos.

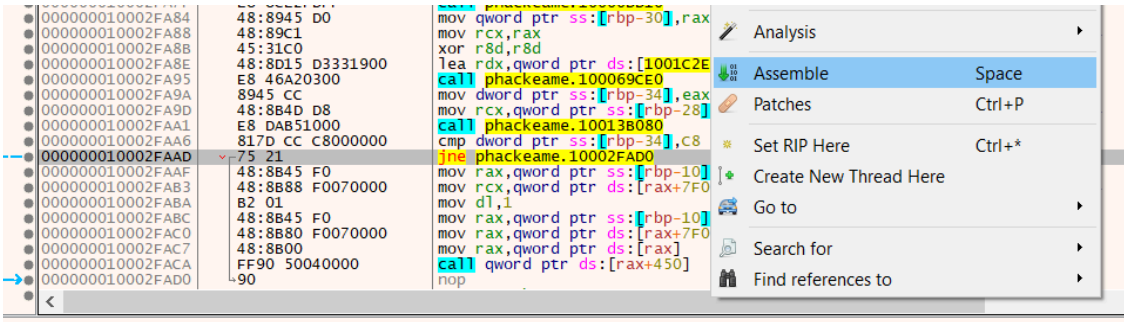
3. Pasos para el parchado

Para lograr estos cambios en el código, es decir, para parchar el ejecutable ahora se debe utilizar la herramienta x64dbg. Una vez abierto el ejecutable se debe dar clic derecho y seleccionar: Go to > Expression y esto permite colocar la location que obtuvimos en Ghidra para que nos lleve a esa parte del código y esta vez poder hacer los cambios necesarios.

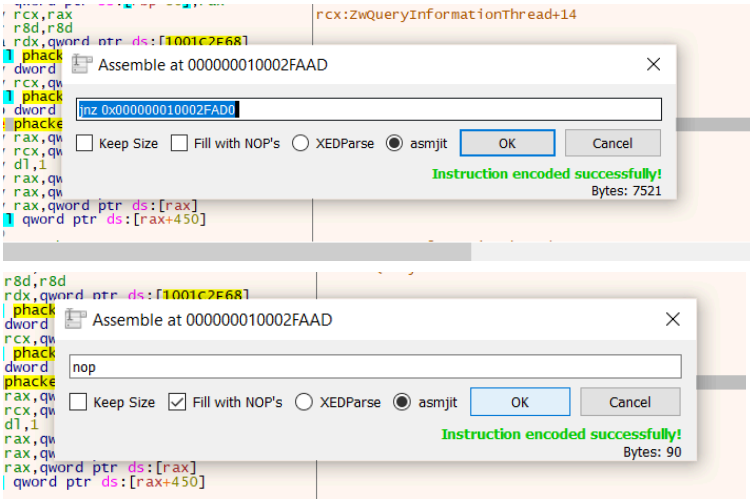




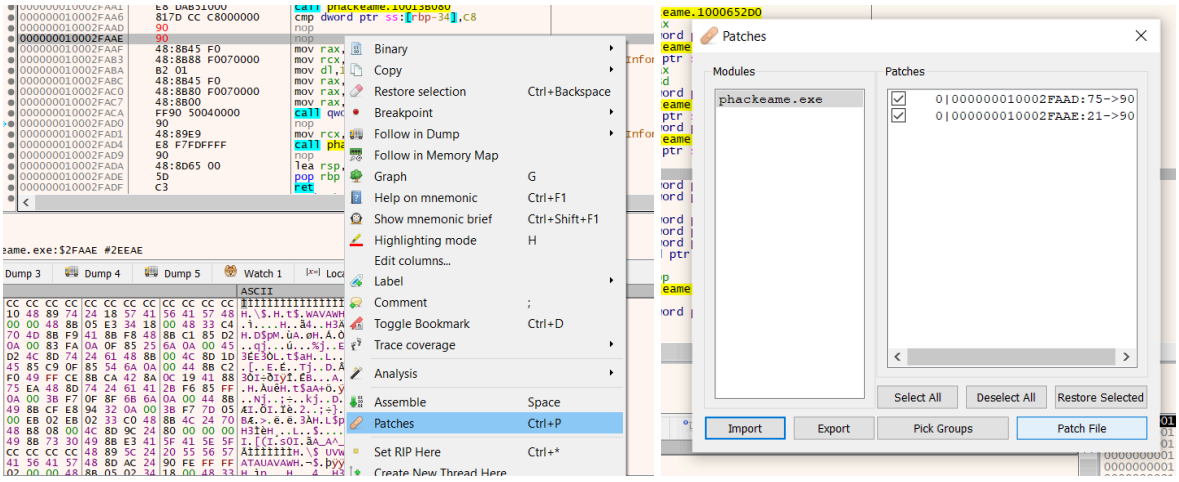
Colocando la location nos muestra justo el lugar donde se realizará el cambio. Y para ello sobre la línea hay que dar clic derecho y seleccionar “Assemble”.



Dado que se requiere que se salté esa parte, se debe cambiar lo que tenga y poner “nop” para saltarse la condicional sin alterar el resto del código.. Además de también seleccionar la casilla correspondiente, tal y como se muestra en las siguientes imágenes.

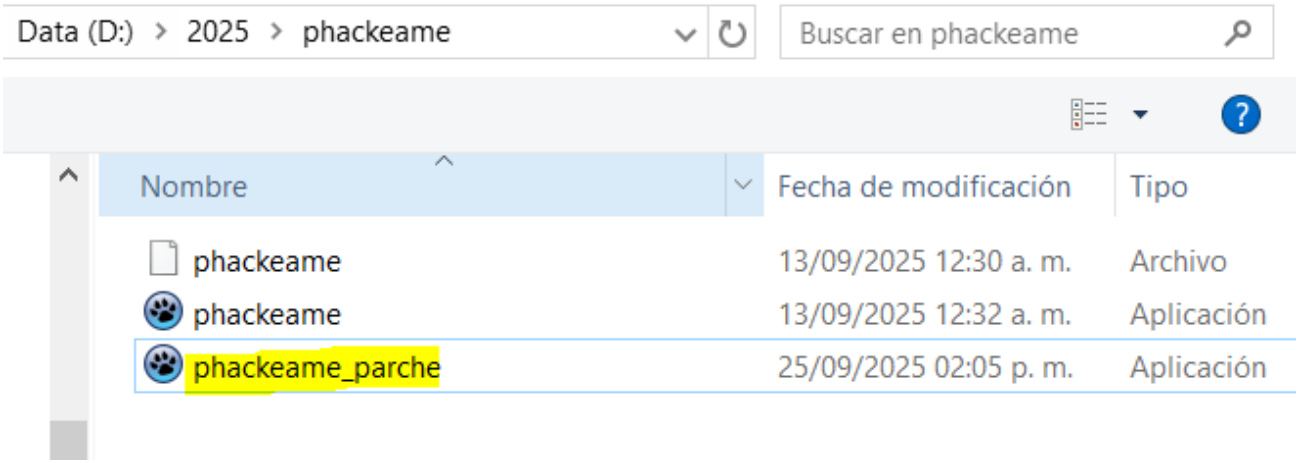


Una vez hecho esto, se observa que los cambios se visualizan en el código y ahora se puede parchar, para ello se debe dar clic derecho y seleccionar “Patches” y luego en “Patch File”.

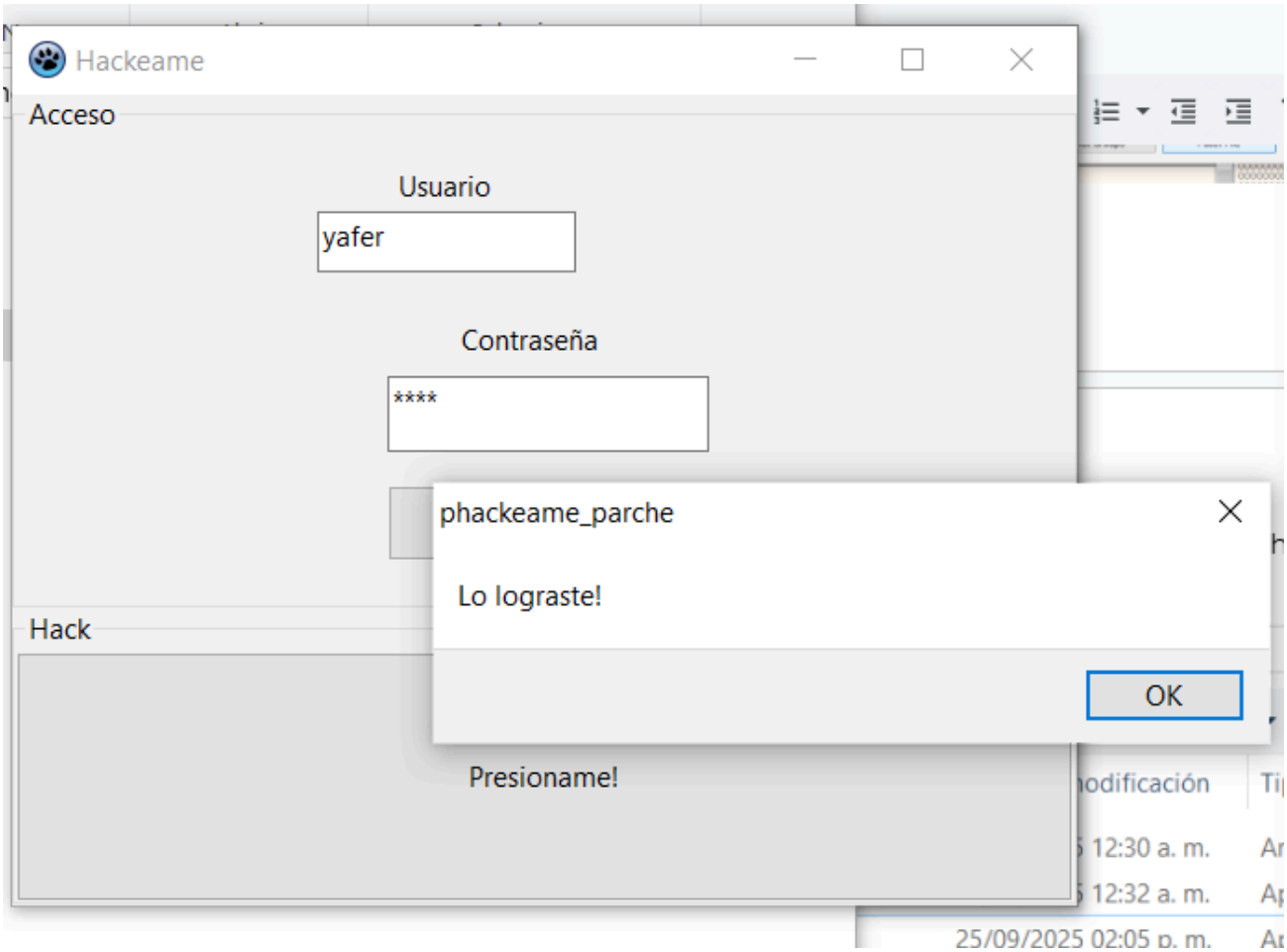


R005

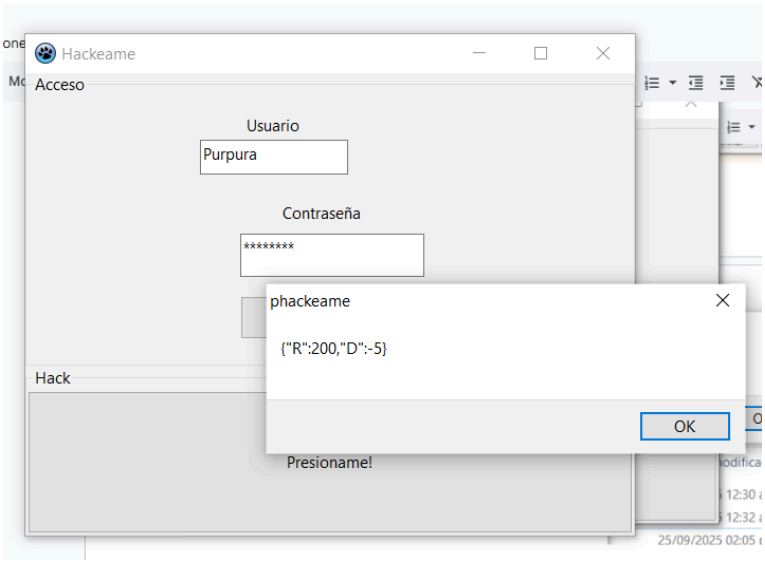
Se nombra el ejecutable y se puede verificar lo que se acaba de realizar haciendo algunas pruebas que se muestran a continuación.



Sin importar si ya no quedan intentos o si se ingresaron datos incorrectos, el ejecutable permite el acceso. Por lo que el parche ha funcionado.



R005


Hackeame
Acceso
Usuario
Purpura
Contraseña
****
phackeame
{"R":200,"D":-5}
OK
Hack
Presioname!