



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto Tecnológico de San Juan del Río



TOPICOS DE CIBERSEGURIDAD

VALDES ARTEAGA LEONARDO

PRACTICA 4 EJECUTABLE SIN IMPORTAR EL USUARIO O CONTRASEÑA

P R E S E N T A:

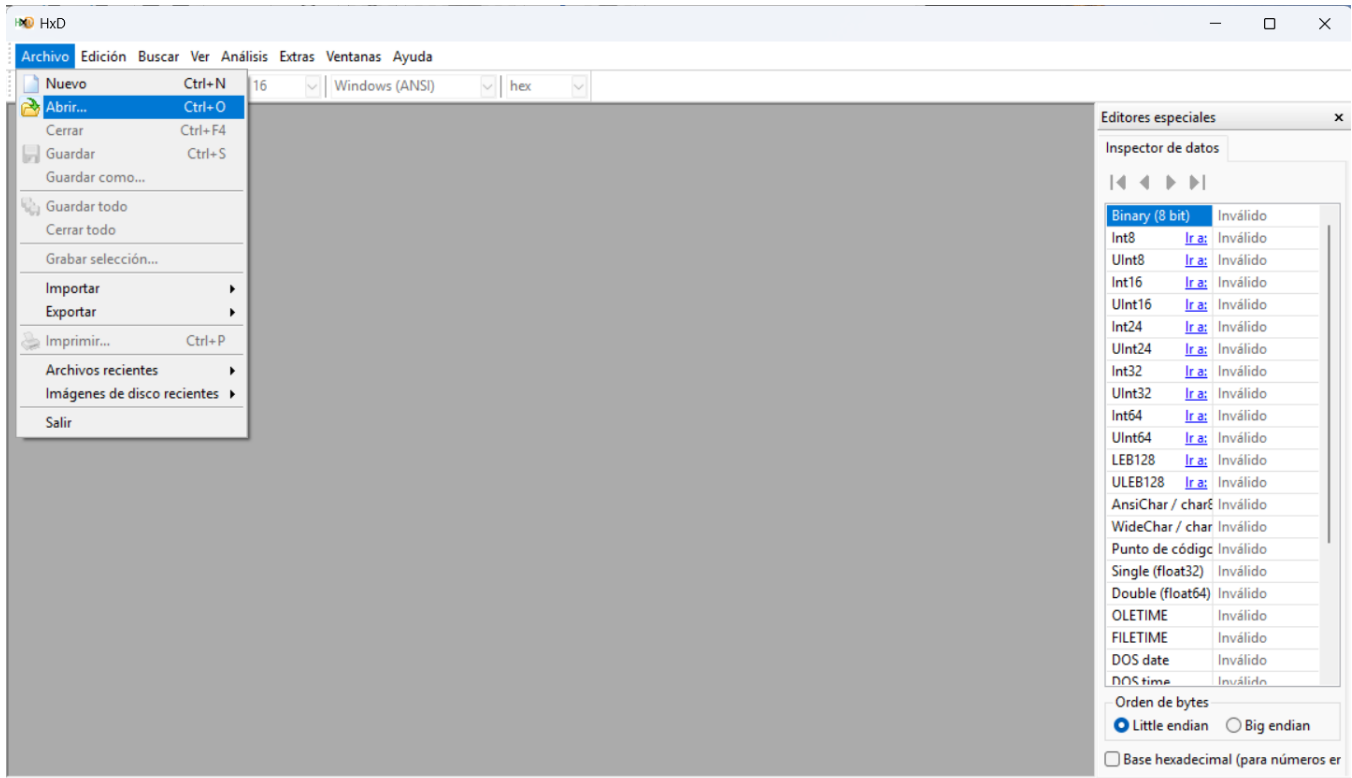
**María del Carmen Pérez Cruz, Emma Belen Marquez García, Karla
Daniela Pérez González**

Ingeniería en Sistemas Computacionales

NO. DE CONTROL: 21590485, 21590481, 21590486

PERIODO Enero-Junio

Primero abrimos un archivo nuevo en la aplicación de HxD para que podamos abrir nuestro ejecutable y analizar los hexadecimales



Después presionamos ctrl+f para buscar el http o sea la ip que está usando nuestro archivo

HxD - [C:\Users\maryp\Downloads\phackeame (3) - copia - copia.exe]

Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda

16 Windows (ANSI) hex

Sin título1 phackeame (3) - copia - copia.exe

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado

00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..

00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....

00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00E.....

00000030 0E 1F BA 0E 00 B4 09 CD 21 B8 01 40 00 00 00 00 00

00000040 69 73 20 70 72 6F 67 72 61 6D 20 63 00 00 00 00

00000050 74 20 62 65 20 72 75 6E 20 69 6E 20 00 00 00 00

00000060 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00

00000070 50 45 00 00 64 86 09 00 00 00 00 00 00 00 00 00

00000080 00 00 00 00 F0 00 2F 00 0B 02 03 16 00 00 00 00

00000090 14 F4 01 00 28 EF 10 00 00 00 2D 00 00 00 00 00

000000A0 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00

000000B0 00 F0 3C 00 00 04 00 00 00 00 00 00 00 00 00 00

000000C0 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00

000000D0 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00

000000E0 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00

000000F0 00 30 39 00 DC 00 00 00 00 00 00 00 00 00 00 00

00000100 00 50 26 00 50 D8 01 00 00 00 00 00 00 00 00 00

00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000140 70 A0 19 00 28 00 00 00 00 00 00 00 00 00 00 00

00000150 00 00 00 00 00 00 00 00 5C 3F 39 00 80 0E 00 00

00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000170 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00

00000180 70 83 19 00 00 10 00 00 00 84 19 00 00 04 00 00

00000190 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60

000001A0 2E 64 61 74 61 00 00 14 F4 01 00 00 A0 19 00 00

000001B0 00 F6 01 00 00 88 19 00 00 00 00 00 00 00 00 00

000001C0 00 00 00 00 40 00 C0 2E 72 64 61 74 61 00 00

000001D0 2C A9 0A 00 00 A0 1B 00 00 A0 0A 00 00 7E 1B 00

000001E0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40

000001F0 2E 70 64 61 74 61 00 00 50 D8 01 00 00 50 26 00

Desplazamiento(h): AB Sobrecribir

Inspector de datos

Binary (8 bit) 00000000

Int8 Ir a: 0

UInt8 Ir a: 0

Int16 Ir a: 0

UInt16 Ir a: 0

Int24 Ir a: 1048576

UInt24 Ir a: 1048576

Int32 Ir a: 1048576

UInt32 Ir a: 1048576

Int64 Ir a: 1048576

UInt64 Ir a: 1048576

LEB128 Ir a: 0

ULEB128 Ir a: 0

AnsiChar / char

WideChar / char

Punto de código (U+0000)

Single (float32) 1.4693679385278

Double (float64) 5.1806537865363

OLETIME 30/12/1899

FILETIME 01/01/1601 12:00

DOS date Inválido

DOS time 12:00:00 a.m.

Orden de bytes

Little endian Big endian

Base hexadecimal (para números e

HxD - [C:\Users\maryp\Downloads\phackeame (3) - copia - copia.exe]

Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda

16 Windows (ANSI) hex

Sin título1 phackeame (3) - copia - copia.exe

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado

001C0B40 6F 6B C8 07 00 00 00 00 00 01 00 06 62 74 6E okE.....btn

001C0B50 79 65 70 D0 07 00 00 00 00 00 02 00 07 74 78 yepD.....tx

001C0B60 74 70 61 73 73 D8 07 00 00 00 00 00 03 00 07 tpass@.....

001C0B70 4C 62 6C 70 61 73 73 E0 07 00 00 00 00 00 02 Lblpass@.....

001C0B80 00 06 74 78 74 75 73 72 E8 07 00 00 00 00 00 00 ..txtusrè.....

001C0B90 04 00 03 47 42 31 F0 07 00 00 00 00 00 04 00 ..GB18.....

001C0BA0 03 47 42 32 F8 07 00 00 00 00 00 03 00 06 4C .GB2@.....L

001C0BB0 62 6C 75 73 72 00 00 00 68 22 1C 00 01 00 00 blusr...h.....

001C0BC0 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF

001C0BD0 08 00 00 00 00 00 00 00 7B 22 55 53 52 22 3A 22{"USR":.....

001C0BE0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00

001C0BF0 FF FF FF FF FF FF FF FF 0A 00 00 00 00 00 00

001C0C00 22 2C 22 50 41 53 53 22 3A 22 00 00 00 00 00

001C0C10 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF

001C0C20 02 00 00 00 00 00 00 00 22 7D 00 00 00 00 00

001C0C30 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF

001C0C40 1F 00 00 00 00 00 00 00 68 74 74 70 3A 2F 2F 34http://4

001C0C50 35 2E 37 36 2E 31 37 33 2E 31 31 34 3A 38 30 38 S.76.173.114:808

001C0C60 30 2F 6C 6F 67 69 6E 00 00 01 00 00 00 00 00 00 /login.....

001C0C70 FF FF FF FF FF FF FF FF 1F 00 00 00 00 00 00

001C0C80 4E 6F 20 73 65 20 70 75 64 6F 20 63 6F 6E 65 63 No se pudo conec

001C0C90 74 61 72 20 61 6C 20 73 65 72 76 69 64 6F 72 00 tar al servidor.

001C0CA0 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF

001C0CB0 01 00 00 00 00 00 00 00 52 00 00 00 00 00 00 00

001C0CC0 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF

001C0CD0 0C 00 00 00 00 00 00 00 4C 6F 20 6C 6F 67 72 61Lo logra

001C0CE0 73 74 65 21 00 00 00 00 0F 08 54 46 72 6D 70 72 ste!.....TFmpr

001C0CF0 69 6E 68 22 1C 00 01 00 00 00 70 20 1C 00 01 00 inh".....p

001C0D00 00 00 6F 00 0A 75 70 72 69 6E 63 69 70 61 6C 00

001C0D10 00 00 00 00 00 00 00 00 E8 2E 1C 00 01 00 00 00

001C0D20 01 00 00 00 18 BB 1C 00 16 02 03 00 00 00 00 00

001C0D30 08 00 00 00 00 00 00 00 F8 FF FF FF FF FF FF

001C0D40 50 26 00 00 00 00 00 00 3A 1C 00 01 00 00 00

Desplazamiento(h): 1C0C48 Bloque(h): 1C0C48-1C0C4B Tamaño(h): 4 Sobrecribir

Inspector de datos

Binary (8 bit) 01101000

Int8 Ir a: 104

UInt8 Ir a: 104

Int16 Ir a: 29800

UInt16 Ir a: 29800

Int24 Ir a: 7631976

UInt24 Ir a: 7631976

Int32 Ir a: 1886680168

UInt32 Ir a: 1886680168

Int64 Ir a: Inválido

UInt64 Ir a: Inválido

LEB128 Ir a: -24

ULEB128 Ir a: 104

AnsiChar / char h

WideChar / char 港

Punto de código h (U+0068)

Single (float32) 3.0262027567039

Double (float64) Inválido

OLETIME Inválido

FILETIME Inválido

DOS date 08/03/2038

DOS time 02:35:16 a.m.

Orden de bytes

Little endian Big endian

Base hexadecimal (para números e

Despues vamos a cambiar los dígitos uno a uno en el hexadecimal hasta lograr la ip que deseamos en este caso es 127.0.0.1, pero para que no se pierdan los bit vamos a hacer que sea de manera que sea 127.0.000.001

HxD - [C:\Users\maryp\Downloads\phackeame (3) - copia - copia.exe]

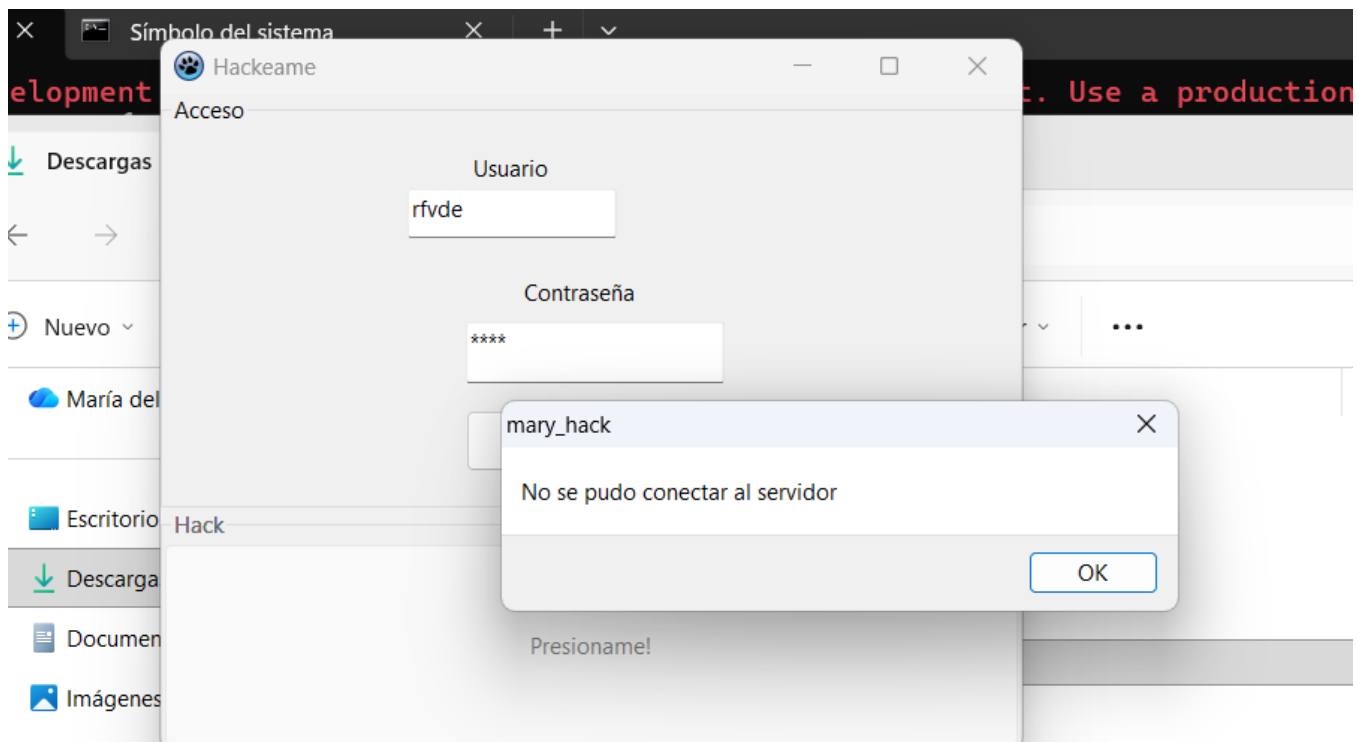
Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda

16 Windows (ANSI) hex

maryhackeo.exe phackeame (1).exe phackeame (3) - copia - copia.exe Pausar la grabación

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texto decodificado
001C0B00	04	00	18	FF	20	00	01	00	00	00	08	D7	20	00	01	00	...ÿ* ...
001C0B10	00	00	98	29	21	00	01	00	00	00	10	A2	20	00	01	00	..")!.....c ...
001C0B20	00	00	00	00	00	00	00	00	00	08	00	00	2D	1C	00	01-....
001C0B30	00	00	C0	07	00	00	00	00	00	00	01	00	05	62	74	6E	..A.....btn
001C0B40	6F	6B	C8	07	00	00	00	00	00	00	01	00	06	62	74	6E	okE.....btn
001C0B50	79	65	70	D0	07	00	00	00	00	00	00	02	00	07	74	78	yepB.....tx
001C0B60	74	70	61	73	73	D8	07	00	00	00	00	00	00	03	00	07	tpass@.....
001C0B70	4C	62	6C	70	61	73	73	E0	07	00	00	00	00	00	00	02	Lblpassà.....
001C0B80	00	06	74	78	74	75	73	72	E8	07	00	00	00	00	00	00	..txtusrè.....
001C0B90	04	00	03	47	42	31	F0	07	00	00	00	00	00	00	00	04	...GB1ð.....
001C0BA0	03	47	42	32	F8	07	00	00	00	00	00	00	03	00	06	4C	.GB2ø.....L
001C0BB0	62	6C	75	73	72	00	00	00	68	22	1C	00	01	00	00	00	blusr...h".....
001C0BC0	00	00	01	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FFÿÿÿÿÿÿÿÿ
001C0BD0	08	00	00	00	00	00	00	00	7B	22	55	53	52	22	3A	22{"USR":
001C0BE0	00	00	00	00	00	00	00	00	00	00	01	00	00	00	00	00
001C0BF0	FF	FF	FF	FF	FF	FF	FF	FF	0A	00	00	00	00	00	00	00	ÿÿÿÿÿÿÿ.....
001C0C00	22	2C	22	50	41	53	53	22	3A	22	00	00	00	00	00	00	", "PASS": ".....
001C0C10	00	00	01	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FFÿÿÿÿÿÿÿ
001C0C20	02	00	00	00	00	00	00	00	22	7D	00	00	00	00	00	00"}.....
001C0C30	00	00	01	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FFÿÿÿÿÿÿÿ
001C0C40	1F	00	00	00	00	00	00	00	68	74	74	70	3A	2F	2F	31http://1
001C0C50	32	37	2E	30	2E	30	30	30	2E	30	30	31	3A	38	30	30	27.0.000.001:800
001C0C60	30	2F	6C	6F	67	69	6E	00	00	00	00	01	00	00	00	00	p/login.....
001C0C70	FF	FF	FF	FF	FF	FF	FF	FF	1F	00	00	00	00	00	00	00	ÿÿÿÿÿÿÿ.....
001C0C80	4E	6F	20	73	65	20	70	75	64	6F	20	63	6F	6E	65	63	No se pudo conec
001C0C90	74	61	72	20	61	6C	20	73	65	72	76	69	64	6F	72	00	tar al servidor.
001C0CA0	00	00	01	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FFÿÿÿÿÿÿÿ
001C0CB0	01	00	00	00	00	00	00	00	52	00	00	00	00	00	00	00R.....
001C0CC0	00	00	01	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FFÿÿÿÿÿÿÿ
001C0CD0	0C	00	00	00	00	00	00	00	4C	6F	20	6C	6F	67	72	61Lo logra
001C0CE0	73	74	65	21	00	00	00	00	0F	08	54	46	72	6D	70	72	ste!.....TFmpr
001C0CF0	69	6E	68	22	1C	00	01	00	00	00	70	20	1C	00	01	00	inh".....p
001C0D00	00	00	6F	00	0A	75	70	72	69	6E	63	69	70	61	6C	00	..O..uprincipal.
001C0D10	00	00	00	00	00	00	00	00	E8	2E	1C	00	01	00	00	00è.....
001C0D20	01	00	00	00	18	BB	1C	00	16	02	03	00	00	00	00	00».....
001C0D30	08	00	00	00	00	00	00	00	F8	FF	FF	FF	FF	FF	FF	FFøÿÿÿÿÿÿÿ

Guardamos nuestro ejecutable con .exe al final para que no haya problemas con el ejecutable después



Abrimos nuestro geany con nuestro código previamente realizado ya solo para ejecutar



yp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE - Geany

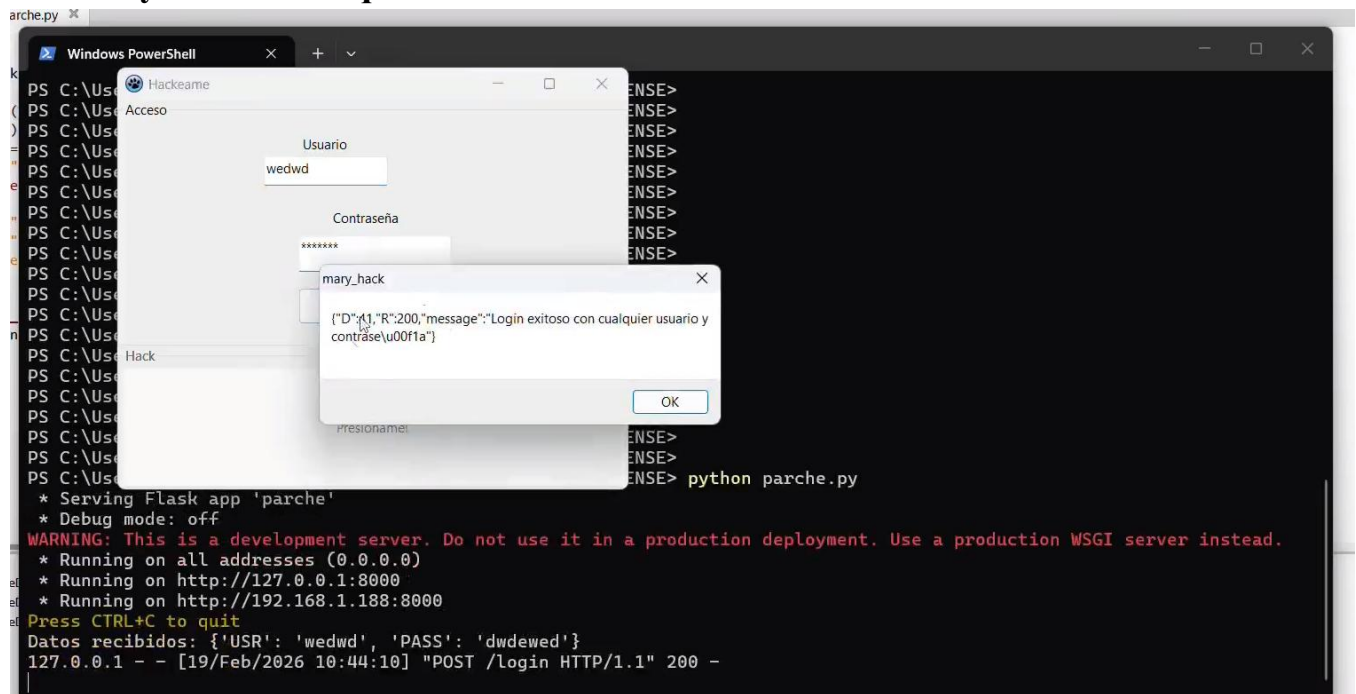
Ver Documento Proyecto Construir Herramientas Ayuda

```
soloPares.py x parche.py x
1 from flask import Flask, request, jsonify
2
3 app = Flask(__name__)
4
5 @app.route('/login', methods=['POST'])
6 def login():
7     datos = request.json
8     print("Datos recibidos:", datos) # sigue mostrando lo que envían
9     # Puedes personalizar la respuesta si quieres
10    return jsonify({
11        "R": 200, # código de éxito
12        "D": 41, # valor que quieras mantener
13        "message": "Login exitoso con cualquier usuario y contraseña"
14    })
15
16 if __name__ == '__main__':
17     app.run(host='0.0.0.0', port=8000)
18
```

Ejecutamos nuestro script de Python

```
Windows PowerShell
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE> python parche.py
* Serving Flask app 'parche'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8000
* Running on http://192.168.224.125:8000
Press CTRL+C to quit
Datos recibidos: {'USR': 'naranja', 'PASS': 'Cyber123456'}
127.0.0.1 - - [19/Feb/2026 17:40:50] "POST /login HTTP/1.1" 200 -
Datos recibidos: {'USR': 'naranja', 'PASS': 'Cyber123456651651+'}
127.0.0.1 - - [19/Feb/2026 17:40:58] "POST /login HTTP/1.1" 200 -
Datos recibidos: {'USR': 'naranja', 'PASS': 'Cyber123456651651+'}
127.0.0.1 - - [19/Feb/2026 17:41:30] "POST /login HTTP/1.1" 200 -
Datos recibidos: {'USR': 'bggb', 'PASS': 'btbg'}
127.0.0.1 - - [19/Feb/2026 18:00:58] "POST /login HTTP/1.1" 200 -
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE> python parche.py
* Serving Flask app 'parche'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8000
* Running on http://192.168.224.125:8000
Press CTRL+C to quit
```

Comprobamos en el ejecutable si esta correcto y podemos acceder con cualquier usuario y contraseña que deseemos



Y para corroborar que si es verdad que solo es con el c\u00f3digo de Python nos salimos y comprobamos que el ejecutable ya no funciona con cualquier usuario y contrase\u00f1a

soloPares.py x parche.py x

```
1 from flask import Flask, request, jsonify
2
3 app = Flask(__name__)
4
5 @app.route('/login', methods=['POST'])
6 def login():
7     datos = request.json
8     print("Datos recibidos")
9     # Puedes personalizar la respuesta
10    return jsonify({
11        "R": 200, # codigo de respuesta
12        "D": 41, # mensaje de respuesta
13        "message": "Login exitoso"
14    })
15
16 if __name__ == '__main__':
17     app.run(host='0.0.0.0', port=5000)
```

Hackeame

Acceso

Usuario

wedwd

Contraseña

mary_hack

No se pudo conectar al servidor

OK

Presione!

esto es Geany 2.1.

archivo C:\Users\marvp\OneDrive\Documentos\10_TEC\PROGRAMACIÓN LOGICA Y FUNCIONAL\soloPares.py abierto (1)