

Universidad de San Carlos de Guatemala

Facultad de Ingeniería

Escuela de Ciencias y Sistemas

Software avanzado

Práctica 2 – parte 1

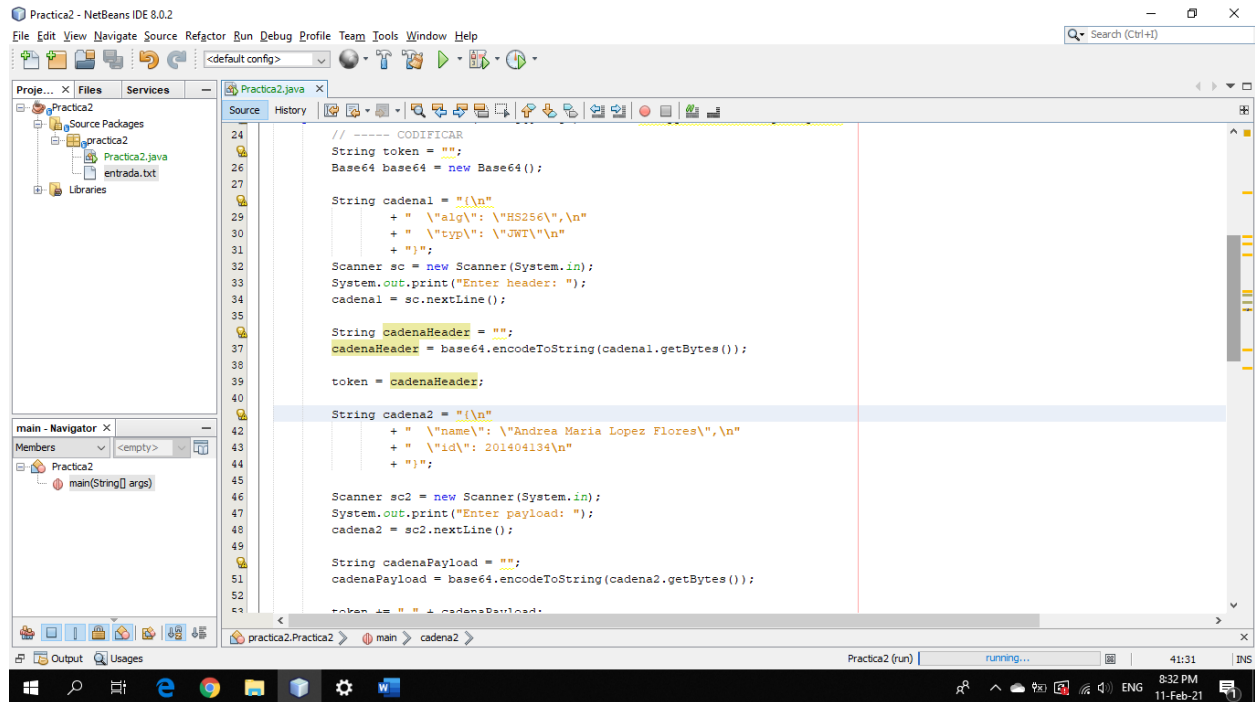
Andrea María López Flores

201404134

Guatemala, 11 de febrero de 2021

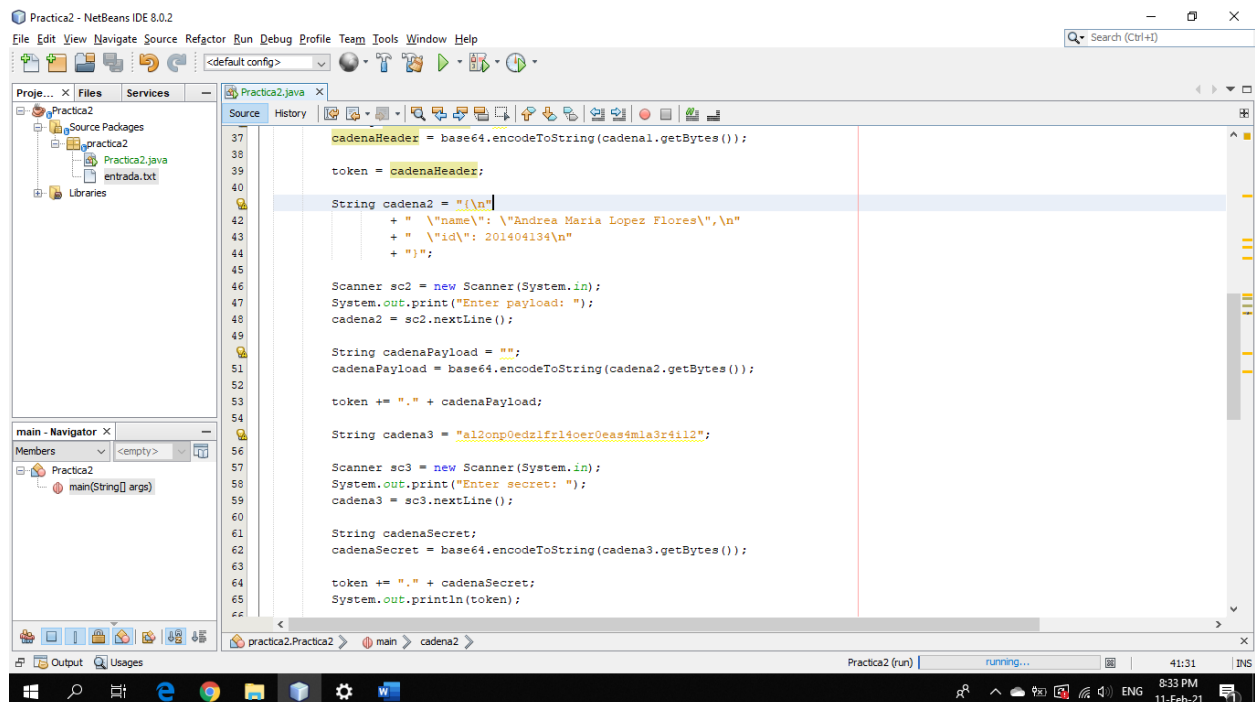
Generación de token

Código



The screenshot shows the NetBeans IDE with the file 'Practica2.java' open. The code defines a Base64 encoder and constructs a token by concatenating a header and a payload. The header contains algorithm, type, and issuer information. The payload contains user name and ID.

```
24 // ---- CODIFICAR
25 String token = "";
26 Base64 base64 = new Base64();
27
28 String cadena1 = "{\n"
29     + "  \"alg\": \"HS256\",\n"
30     + "  \"typ\": \"JWT\"\n"
31     + "}";
32 Scanner sc = new Scanner(System.in);
33 System.out.print("Enter header: ");
34 cadena1 = sc.nextLine();
35
36 String cadenaHeader = "";
37 cadenaHeader = base64.encodeToString(cadena1.getBytes());
38
39 token = cadenaHeader;
40
41 String cadena2 = "{\n"
42     + "  \"name\": \"Andrea Maria Lopez Flores\",\n"
43     + "  \"id\": \"201404134\"\n"
44     + "}";
45
46 Scanner sc2 = new Scanner(System.in);
47 System.out.print("Enter payload: ");
48 cadena2 = sc2.nextLine();
49
50 String cadenaPayload = "";
51 cadenaPayload = base64.encodeToString(cadena2.getBytes());
52
53 token += " " + cadenaPayload;
```

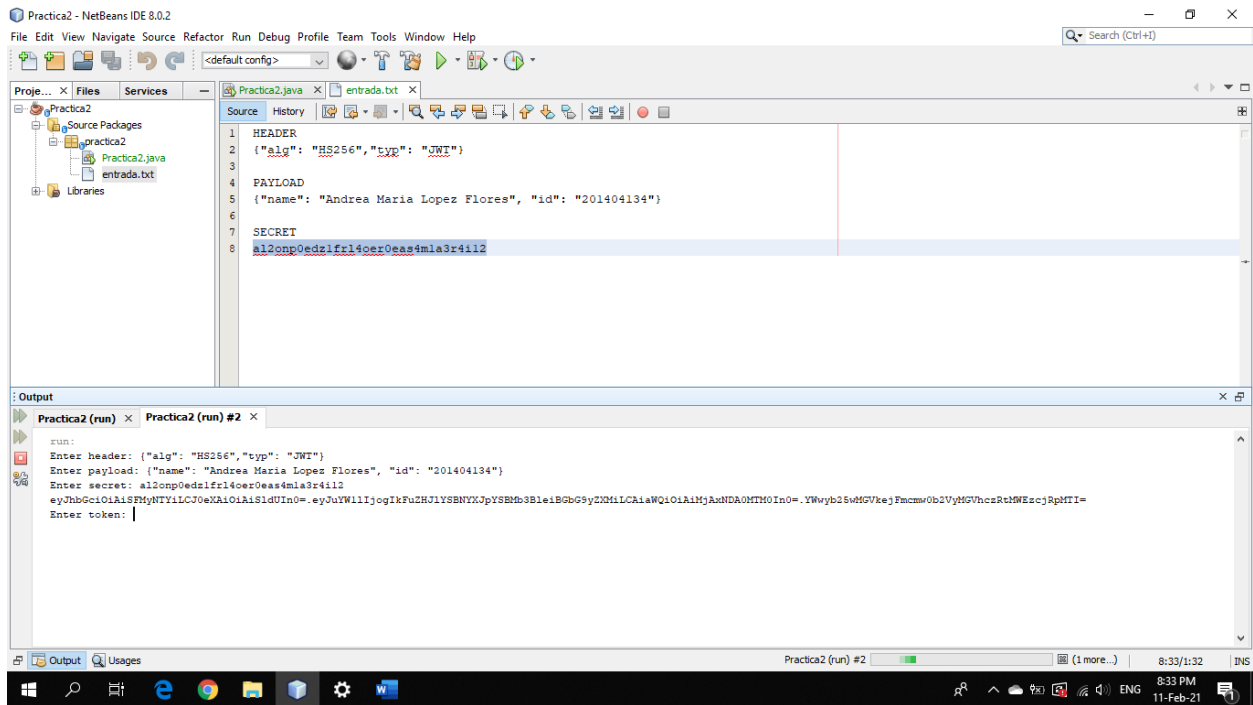


The screenshot shows the continuation of the Java code. It concatenates a secret key to the token and then encodes the entire token using Base64.

```
37 cadenaHeader = base64.encodeToString(cadena1.getBytes());
38
39 token = cadenaHeader;
40
41 String cadena2 = "{\n"
42     + "  \"name\": \"Andrea Maria Lopez Flores\",\n"
43     + "  \"id\": \"201404134\"\n"
44     + "}";
45
46 Scanner sc2 = new Scanner(System.in);
47 System.out.print("Enter payload: ");
48 cadena2 = sc2.nextLine();
49
50 String cadenaPayload = "";
51 cadenaPayload = base64.encodeToString(cadena2.getBytes());
52
53 token += " " + cadenaPayload;
54
55 String cadena3 = "al2onp0edzlfcl4oer0eas4mla3r4i1i2";
56
57 Scanner sc3 = new Scanner(System.in);
58 System.out.print("Enter secret: ");
59 cadena3 = sc3.nextLine();
60
61 String cadenaSecret;
62 cadenaSecret = base64.encodeToString(cadena3.getBytes());
63
64 token += " " + cadenaSecret;
65 System.out.println(token);
```

Resultado en consola

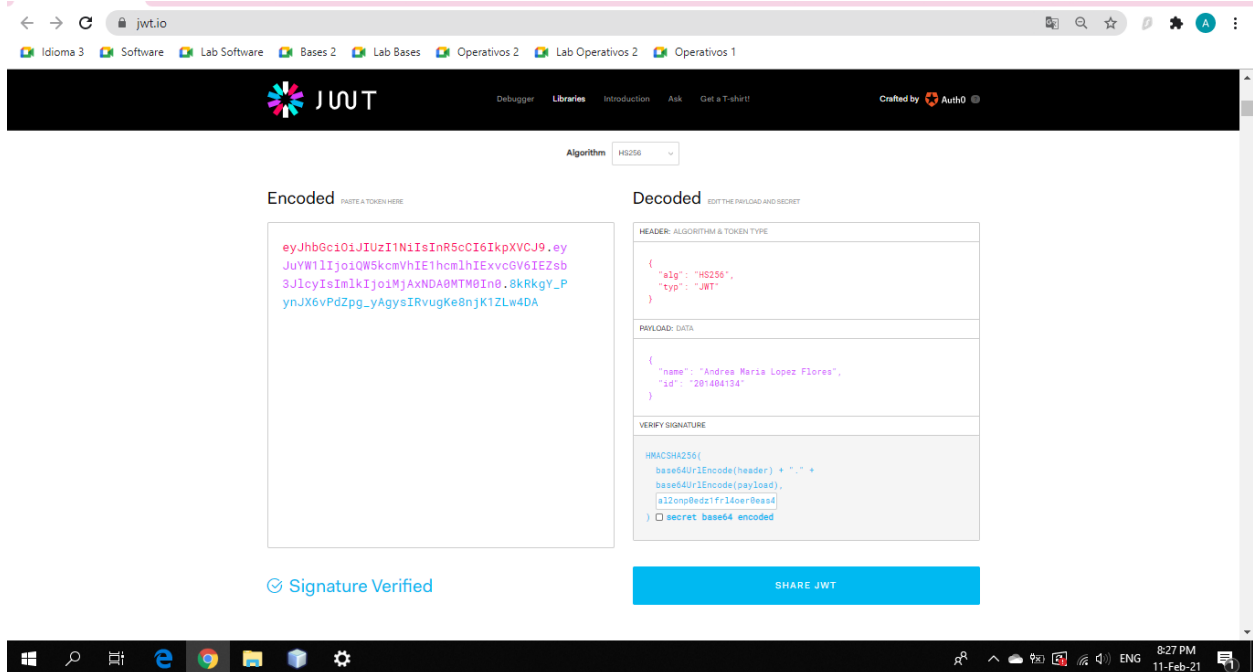
Luego de ingresar toda la información que se solicita se mostrará el token



```
1 HEADER
2 {"alg": "HS256","typ": "JWT"}
3
4 PAYLOAD
5 {"name": "Andrea Maria Lopez Flores", "id": "201404134"}
6
7 SECRET
8 a120np0edz1fr140er0eas4mla3r4i12
```

```
run:
Enter header: {"alg": "HS256","typ": "JWT"}
Enter payload: {"name": "Andrea Maria Lopez Flores", "id": "201404134"}
Enter secret: a120np0edz1fr140er0eas4mla3r4i12
eyJhbGciOiAiS256IiwiaXNjaW50IjoiIn0=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bWw1IjoiQW5kcmVhIE1hcm1hIEVxc6V6IEZsb3JlcyIsImkiOiMjAxNDA0MTM0In0=.YWwyb35vM0VkejFmcms0b2V5MGVhcnRtMWEscjRpbMTI=
Enter token:
```

Prueba de funcionamiento



Algorithm: HS256

Encoded: `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bWw1IjoiQW5kcmVhIE1hcm1hIEVxc6V6IEZsb3JlcyIsImkiOiMjAxNDA0MTM0In0=.8kRkgY_PynJX6vPdZpg_yAgysIRvugKe8njK1ZLw4DA`

Decoded: `HEADER: ALGORITHM & TOKEN TYPE`
`{`
 `"alg": "HS256",`
 `"typ": "JWT"`
`}`

`PAYLOAD: DATA`
`{`
 `"name": "Andrea Maria Lopez Flores",`
 `"id": "201404134"`
`}`

`VERIFY SIGNATURE`
`HS256`
`base64urlEncode(header) + "." +`
`base64urlEncode(payload)`
`a120np0edz1fr140er0eas4mla3r4i12`
`secret: base64 encoded`

Signature Verified

SHARE JWT

Código

Practica2 - NetBeans IDE 8.0.2

File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help

Search (Ctrl+I)

Project: X Files Services

Source Packages

Practica2

Practica2.java

entrada.txt

Libraries

main - Navigator

Members

Practica2

main(String[] args)

Source

```

67 // ----- DECODIFICAR
68 Scanner sc4 = new Scanner(System.in);
69 System.out.print("Enter token: ");
70 token = sc4.nextLine();
71
72 String nueva = token.replace(".", "-");
73 String[] partes = nueva.split("-");
74
75 String deco_header = partes[0];
76 String deco_payload = partes[1];
77 String deco_secret = partes[2];
78
79 byte[] decodedHeader = Base64.decodeBase64(deco_header);
80 System.out.println(new String(decodedHeader, "UTF-8") + "\n");
81 String cadena_header = new String(decodedHeader, "UTF-8");
82
83 byte[] decodedPayload = Base64.decodeBase64(deco_payload);
84 System.out.println(new String(decodedPayload, "UTF-8") + "\n");
85 String cadena_payload = new String(decodedPayload, "UTF-8");
86
87 byte[] decodedSecret = Base64.decodeBase64(deco_secret);
88 System.out.println(new String(decodedSecret, "UTF-8") + "\n");
89 String cadena_secret = new String(decodedSecret, "UTF-8");
90
91 if (cadena_header.equals(cadenal) && cadena_payload.equals(cadena2) && cadena_secret.equals(cadena3)) {
92     System.out.println("TOKEN VALIDO");
93 } else {
94     System.out.println("TOKEN NO VALIDO");
95 }
96

```

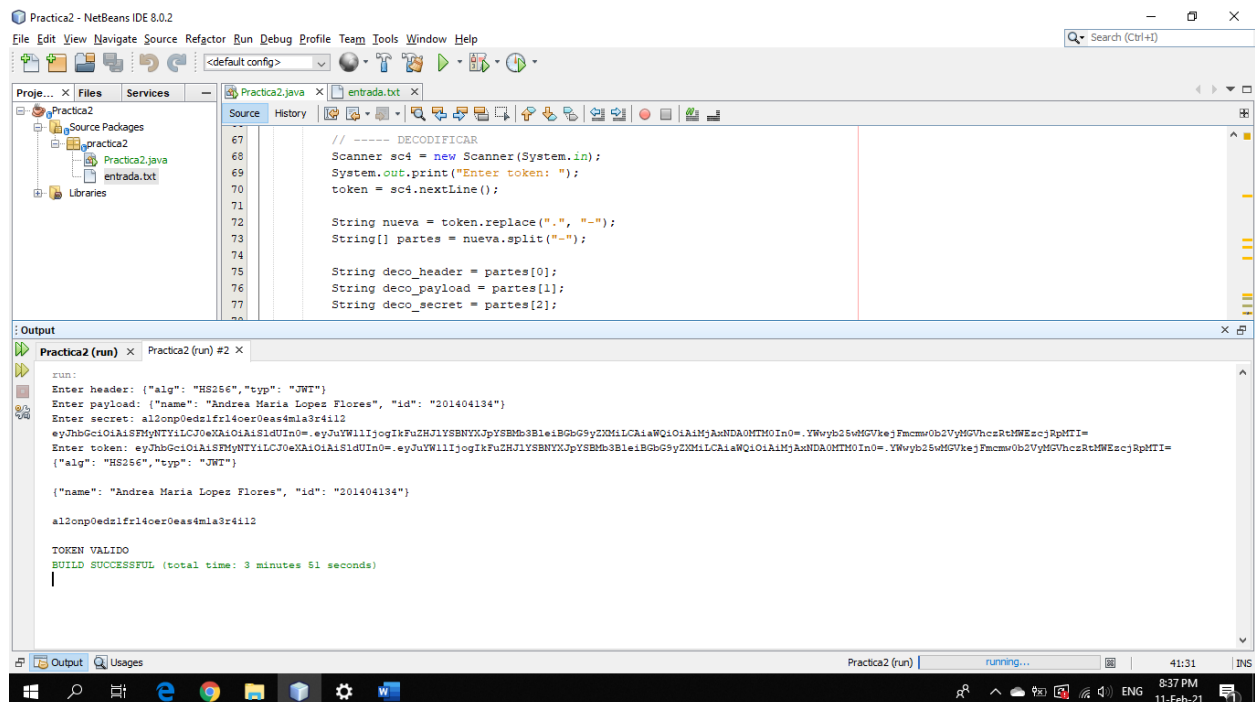
practica2.Practica2> main> cadena2>

practica2 (run) #2 running... (1 more...)

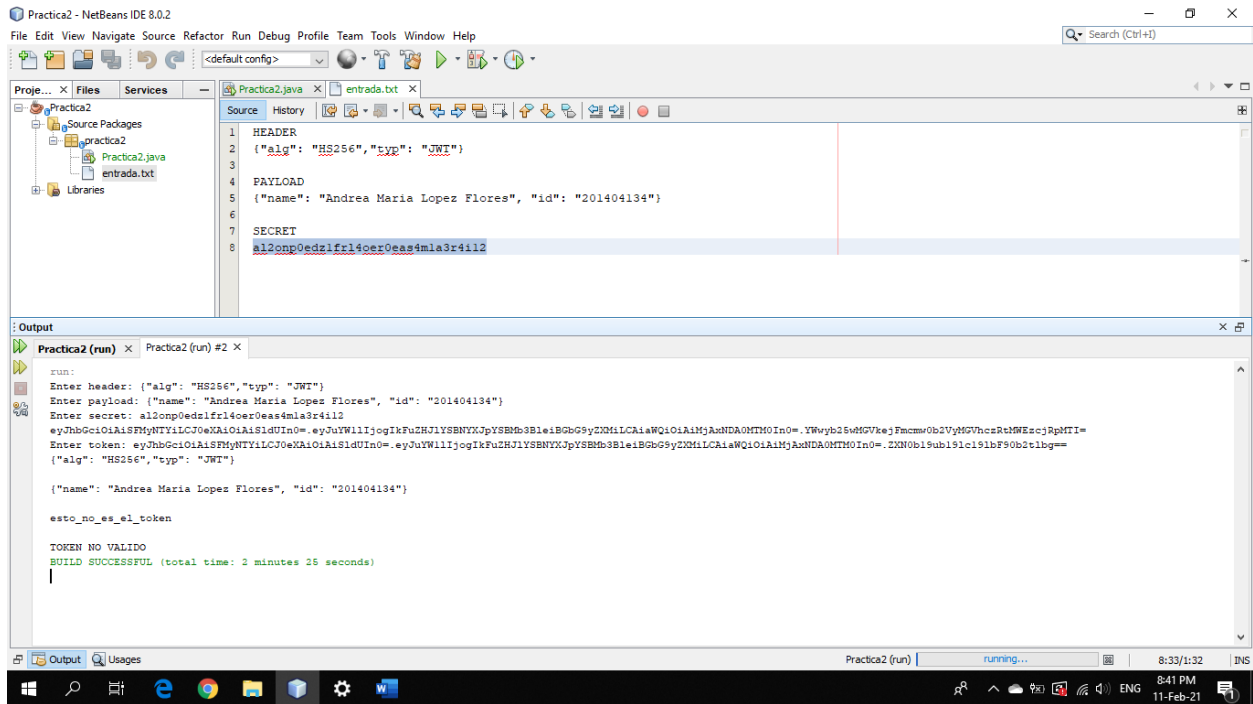
41:31 11-Feb-21

Resultado en consola

Se pide ingresar el token a decodificar y se muestra el resultado



De ingresar un token incorrecto o que el secret no coincida con el establecido, se mostrará el siguiente mensaje



The screenshot shows the NetBeans IDE interface. The main editor displays the source code for a JWT token generation process. The code is as follows:

```
1 HEADER
2 {"alg": "HS256", "typ": "JWT"}
3
4 PAYLOAD
5 {"name": "Andrea Maria Lopez Flores", "id": "201404134"}
6
7 SECRET
8 a120np0edz1fx140er0eag4mla3r4i12
```

The Output window shows the execution of the program. The output is as follows:

```
run:
Enter header: {"alg": "HS256", "typ": "JWT"}
Enter payload: {"name": "Andrea Maria Lopez Flores", "id": "201404134"}
Enter secret: a120np0edz1fx140er0eag4mla3r4i12
eyJhbGciOiAiSFMyNTYiLCJ0eXAiOiAiS1dUIn0=eyJ0YW11Ijoia120np0edz1fx140er0eag4mla3r4i12IiwiaWF0Ijoi201404134In0=.YXwyb35wMGVkeiJFcmw0b2VpMGVhczRtMWEscjRpMTI=
Enter token: eyJhbGciOiAiSFMyNTYiLCJ0eXAiOiAiS1dUIn0=eyJ0YW11Ijoia120np0edz1fx140er0eag4mla3r4i12IiwiaWF0Ijoi201404134In0=.YXwyb35wMGVkeiJFcmw0b2VpMGVhczRtMWEscjRpMTI=
{"alg": "HS256", "typ": "JWT"}

{"name": "Andrea Maria Lopez Flores", "id": "201404134"}

esto_no_es_el_token

TOKEN NO VALIDO
BUILD SUCCESSFUL (total time: 2 minutes 25 seconds)
```

The output window also shows the status of the build and the time taken to complete the process. The status is "BUILD SUCCESSFUL" and the time taken is "2 minutes 25 seconds".