🔧 Ejercicio Práctico: Exploración de Encabezados HTTP con Python

📝 Descripción

El objetivo de este ejercicio es que el estudiante utilice Python para realizar una consulta sencilla a un sitio web y observe los encabezados de respuesta HTTP. Estos encabezados pueden revelar información técnica valiosa, como el servidor utilizado, políticas de seguridad, tecnologías en uso y más.

🎯 Objetivos del ejercicio

- Comprender qué es una respuesta HTTP y qué tipo de metadatos contiene.
- Realizar una solicitud HTTP a un sitio web conocido y confiable.
- Visualizar y analizar los encabezados de respuesta.
- Iniciar la reflexión sobre cómo esta información puede formar parte de la superficie de ataque.

👨‍💻 Instrucciones

1. Selecciona un sitio web público y legítimo (por ejemplo, https://www.python.org).
2. Abre tu entorno de trabajo con Python.
3. Realiza una solicitud HTTP tipo GET al sitio seleccionado.
4. Imprime por pantalla todos los encabezados de la respuesta (ejemplo: `Server`, `Content-Type`, `X-Powered-By`, etc.).
5. Observa e identifica posibles pistas sobre las tecnologías utilizadas en el backend del sitio.

6. Anota tres encabezados que podrían ser útiles durante una fase de reconocimiento real.

🔐 Consideraciones Éticas

- Este ejercicio es **totalmente pasivo**: no afecta ni modifica el sitio web.
- Solo se debe realizar sobre sitios públicos y con fines educativos.
- Nunca automatices este tipo de consultas contra sitios que no controles sin permiso explícito.

💡 Ejemplo de resultado esperado (solo salida):

Server: nginx
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Powered-By: WSGI/1.1

✅ Solución: `explorador_encabezados.py`

```
import requests

# URL del sitio a analizar (se puede cambiar por otro sitio legítimo)
url = "https://www.python.org"

# Realizamos la solicitud HTTP tipo GET
respuesta = requests.get(url)

# Imprimimos todos los encabezados de respuesta
print("📦 Encabezados de respuesta HTTP:")
print("---------------------------------")
for clave, valor in respuesta.headers.items():
    print(f"{clave}: {valor}")
```

🧪 Posible salida al ejecutar el script:

📦 Encabezados de respuesta HTTP:

Server: nginx

Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Powered-By: WSGI/1.1
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Encoding: gzip

🔎 Reflexión sugerida para el estudiante:

- ¿Qué tecnologías se pueden inferir de estos encabezados?
- ¿Aparecen cabeceras relacionadas con la seguridad (por ejemplo, `X-Frame-Options`, `Strict-Transport-Security`)?
- ¿Qué podría deducir un atacante a partir del encabezado `X-Powered-By`?
