Práctica 7.1 - Ataque Reflected XSS

Descripción del Ataque

El **Reflected XSS** es un tipo de vulnerabilidad donde el código malicioso se refleja inmediatamente desde el servidor sin ser almacenado. En este ataque se enviará un payload malicioso a través de parámetros URL que será reflejado y ejecutado en el navegador de la víctima.

Endpoint Vulnerable

Se ha creado un endpoint específicamente vulnerable en `app.py`:

```python
@app.route("/reflejar")
def reflejar():
    """
    Endpoint de prueba para permitir ataques Reflected XSS.
    """
    mensaje = request.args.get("mensaje", "")
    return f"<h1>{mensaje}</h1>"
```

Payload Utilizado

```
<script>alert('Has sido hackeado :(')</script>
```

URL de Ataque

```
http://localhost:5001/reflejar?mensaje=<script>alert('Has sido hackeado :(')</script>
```

Pasos del Ataque

1. **Ejecutar el ataque:**
   - Introducir la URL maliciosa en el navegador: http://localhost:5001/reflejar?mensaje=
2. **Resultado:**
   - Al cargar la página, se ejecuta inmediatamente el JavaScript
   - Se muestra una alerta con el texto “Has sido hackeado :(”
   - El código no se almacena, solo se muestra