3.2

CODIFICACIÓN DE SALIDAS

¿QUÉ LO DIFERENCIA DE LA VALIDACIÓN DE ENTRADAS?

- Las entradas de datos son impredecibles y esto hace imposible la validación de entrada perfecta
- Debido al funcionamiento de la aplicación, puede ser necesario admitir caracteres *raros*
- Los datos recibidos pueden ser empleados en muchos contextos (JS, CSS, HTML...)

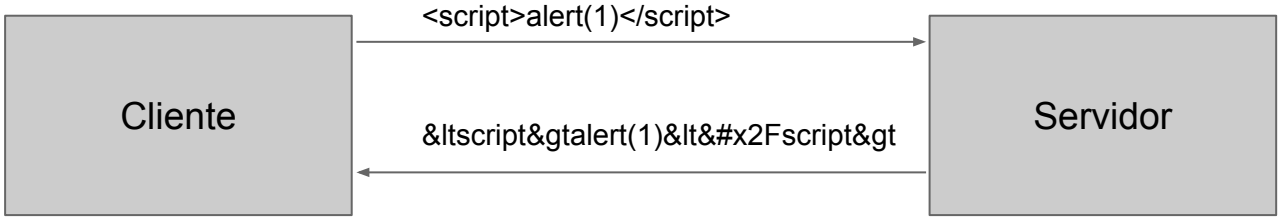
Esas tres razones hacen necesario emplear la codificación de las salidas

XSS - CROSS SITE SCRIPTING

- Ataque de inyección de código
- Permite a un atacante ejecutar código javascript malicioso

CODIFICACIÓN DE SALIDAS

- El mejor método para prevenir XSS y SQLi
- El objetivo principal es convertir entradas de datos no confiables en datos seguros que mostrar



CODIFICACIÓN DE SALIDAS

- Hacer toda la codificación en un sistema de confianza
- Utilizar una rutina testeada y estándar para la codificación de cada tipo de datos
- Codificar todos los caracteres a menos que sean seguros para el intérprete previsto
- Sanitizar todas las salidas de datos no confiables destinadas a comandos o consultas: OS, SQL, XML o LDAP