

Introducción a la Criptografía y a la Seguridad de la Información

Proyecto Final del Curso

El proyecto final del curso consiste en elegir un prototipo de software que se haya desarrollado o se esté desarrollando en otro curso para implementar requerimientos no funcionales (RNF) de seguridad. El proyecto se desarrollará en grupo de hasta 4 estudiantes, quienes deben seguir los siguientes lineamientos:

- Proponer un sistema (objeto de estudio)
- Proponer un conjunto RNF de seguridad para ser implementados en el objeto de estudio
- Diseñar de casos de prueba de seguridad que verificarán el funcionamiento de los RNF implementados
- Implementar los requisitos de seguridad propuestos
- Ejecutar los casos de prueba de seguridad de forma manual o automatizada
- Realizar un pequeño laboratorio de hacking ético para evaluar los componentes del sistema (sistema operativo, red, base de datos)

Ejemplos de RNF

- Validación de datos de entrada (sanitization)
- Logs auditoría a nivel de aplicación
- SSL para servidor seguro
- Delegación de autenticación a servidor LDAP, servicio OAUTH
- Soportar ataques de Denegación de Servicio
- Manejo de cambio de clave utilizando tokens que expiran en el tiempo
- Autenticación de doble factor
- Integración de Captcha
- Implementar alguno de los controles para evitar los Top 10 de riesgos de seguridad que plantea OWASP

Cada grupo realizará una corta exposición de lo desarrollado en el proyecto. La fecha será anunciada por el profesor.