ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
CCPG1003 – INFORMATION ASSURANCE AND SECURITY
EXAMEN 2 - SEGUNDA EVALUACIÓN - I TÉRMINO 2017-2018/ Septiembre 1, 2017

Nombre: _____ ***Matrícula:*** _____

COMPROMISO DE HONOR: Al firmar este compromiso, reconozco que el presente examen está diseñado para ser resuelto de manera individual, que puedo usar un lápiz o esferográfico; que sólo puedo comunicarme con la persona responsable de la recepción del examen; y, cualquier instrumento de comunicación que hubiere traído, debo apagarlo y depositarlo en la parte anterior del aula, junto con algún otro material que se encuentre acompañándolo. Además, no debo usar calculadora alguna, consultar libros, notas, ni apuntes adicionales a los que se entreguen en esta evaluación. Los temas debo desarrollarlos de manera ordenada.
Firmo el presente compromiso, como constancia de haber leído y aceptado la declaración anterior. "Como estudiante de ESPOL me comprometo a combatir la mediocridad y actuar con honestidad, por eso no copio ni dejo copiar".

_____
Firma

Tiempo de duración: 2 horas

Tema 1 (12 puntos)

Para cada par de ataque-contramedida, indique si la contramedida es “no efectiva”, “algo efectiva” o “muy efectiva” y *justifique en máximo 5 líneas* sus respuestas.

1. Rapto de sesión mediante cookies robadas - HTTPS.
   a. No efectiva b. Algo efectiva c. Muy efectiva

2. SQL Injection - Sanear los datos proporcionados por el usuario al generar una página HTML.
   a. No efectiva b. Algo efectiva c. Muy efectiva

3. Cross Site Scripting - Sanear los datos proporcionados por el usuario al generar una página HTML.
   a. No efectiva b. Algo efectiva c. Muy efectiva

Tema 2 (18 puntos)

Suponga que hay una Autoridad de Certificado (CA) con una clave pública bien conocida. Supongamos además que cada usuario recibe un certificado para su clave pública. Para mayor comodidad, usamos PK_u y SK_u para representar la clave pública y la clave privada del usuario *u*, respectivamente. Dibuje diagramas para contestar las siguientes preguntas.

a. Suponga que Alicia quiere enviar un mensaje secreto grande M a Bob. Describa cómo Alice debería enviar M de una manera autenticada.
b. Suponga que Bob recibe el mensaje enviado por Alice. Describa cómo Bob debe procesar el mensaje.
c. Suponga que Alice necesita enviar una serie de grandes mensajes secretos a Bob. A Alice le gustaría evitar firmar digitalmente cada uno de estos mensajes. Desarrolle un protocolo para Alice y Bob para que todos los mensajes puedan ser enviados de manera confidencial y autenticada. Describa brevemente (3 líneas máximo) la idea de su protocolo y luego dibuje un diagrama.