De: Sergi
Enviado: jueves, 13 de enero de 2022 17:30
Para: yokran@live.com
CC: administracion@keepcoding.io
Asunto:

Hola David,

Te envío el feedback sobre tu práctica de Criptografía:

Ejercicio 1. Repeating-key XOR

Aunque tienes razón en que el problema se trata de que la clave en OTP debe ser del mismo tamaño que el mensaje para ser seguro, no explicas en este caso cómo aplicarías el análisi de frecuencia, y el código no funciona.

Ejercicio 2. CTR bit-flipping

Has identificado correctamente que se trata de un ataque de bit-flipping, pero no has explicado cómo se aplicaría al problema en cuestión. Cuales són los bits que “flipearías”? No necesito que el código funcione, pero si el código no funciona, al menos explícame bien en el documento cuales son los pasos que seguirías en el código para aplicar el ataque.

Ejercicio 3. Autenticación

Correcto que lo que solucionaría el problema sería autenticación. Podrías haber dado un ejemplo de authentication code, o cual de ellos habrías escogido en este caso.

Ejercicio 4.

Respuesta correcta.

Ejercicio 5 y 6.

No es cierto que se deba enviar al servidor el hash del password. Si fuera así entonces no se necesitaría la contraseña para hacer login de otro usuario, solo necesitaríamos el hash. Por lo que no protegería de una filtración de la base de datos.

Me sorprende que en el ejercicio 6 la solución que entregas usa PBKDF2 en vez de sha1, que sería la solución correcta al problema de usar un hash inseguro. Por qué no me has explicado eso en el ejercicio 5, en vez de lo que has puesto?

Ejercicio 7.

Correcto, http es inseguro para un servidor de autenticación, y se debería usar siempre HTTPS.

Ejercicio 8.

Respuesta correcta. La seguridad de https depende de los CAs guardados en el sistema. Y si el sistema ha sido comprometido, entonces la seguridad de SSL también.

Considero tu práctica NO APTA. Hay varios ejercicios en los que no me queda claro si entiendes la solución o no. Si no entregas código que funcione no hay problema, pero entonces tienes que

dar una descripción en el documento detallada de lo que harías en el código y los pasos que seguiría tu ataque. Tus respuestas son muy genéricas y no explican el ataque de manera que yo vea que lo entiendes. En la reentrega me gustaría ver descripciones más detalladas.

Sergi