

**(20221Q) 72.44 - Criptografía y Seguridad - Comisión: S**

Material Didáctico

Revisar entrega de examen: Parcial 2

## Revisar entrega de examen: Parcial 2

Usuario	OCTAVIO JAVIER SERPE
Curso	(20221Q) 72.44 - Criptografía y Seguridad - Comisión: S
Examen	Parcial 2
Iniciado	23/06/22 16:02
Enviado	23/06/22 17:32
Estado	Completado
Puntuación del intento	80 de 100 puntos
Tiempo transcurrido	1 hora, 29 minutos de 1 hora y 30 minutos
Resultados mostrados	Todas las respuestas, Respuestas enviadas, Respuestas correctas, Comentarios, Preguntas respondidas incorrectamente


**Pregunta 1**

10 de 10 puntos



Su prima comenta que quiere empezar un kiosco. Por lo que consulta si le puede hacer un presupuesto del equipo necesario para funcionar. Usted que cursa Criptografía y Seguridad le muestra un presupuesto de 1K USD. Cuando su prima le pregunta por qué tanto, le contesta que es lo necesario para evitar que un atacante externo robe datos confidenciales o realice interrupción del servicio. ¿Cree que es correcto el nivel de protección? En caso de que no, ¿Qué etapa del diseño cree que se realizó mal?

Respuesta seleccionada: considero que para un kiosco de barrio, por ejemplo, inicialmente invertir en datos confidenciales (cuales habria?) o DoS (quien se va a gastar en atacar un kiosco de barrio?) es algo innecesario al principio, al menos hasta que hablemos de un kiosco a nivel mundial con multiples sucursales, exito rotundo y alta popularidad, por lo que considero que es completamente desproporcionado el nivel de proteccion que se quiere brindar la etapa que fallo profundamente fue el relevamiento de requisitos

Respuesta correcta:  Se realizó un mal Threat Modelling, en donde se plantea qué tipo de atacante va a ser el más común para amenazar mi modelo de negocios. En el caso de un quiosco, no me preocupa que me hackee la NSA sino que me roben la mercadería. En caso de que no funcione el sistema, siempre puedo cobrar en efectivo

Comentarios [No se ha dado ninguna] para respuesta:

**Pregunta 2**

7 de 10 puntos



Se le pide realizar una auditoría de una aplicación para Android. Para ello, su jefe le pide que haga el setup de un laboratorio para poder interceptar y modificar todo el tráfico \*desencriptado\* que la app realice. La aplicación se conecta a un DNS por SSL con un certificado X.509. Teniendo en cuenta que pueden tener control total en el laboratorio (servidor de DNS, IPs, etc). ¿ Pensar un bosquejo de cómo esto podría implementarse y verificarse ?

Respuesta seleccionada: mediante man in the middle puedo interceptar cualquier tipo de request que no viaje por canales seguros (por ejemplo HTTP, TELNET, FTP) y loggearla a una base de datos por ejemplo respecto a la verificación se podría realizar una verificación formal partiendo como precondition la hipótesis del estado del sistema (algun log o valor auditado podría ser también) y como poscondición el resultado obtenido al someter al input a varias operaciones, donde precisamente la poscondición debe cumplir con las restricciones establecidas desde el momento inicial (esto es un nivel más profundo y puede ser que no sea necesario sino que ya estoy yendo al otro extremo) simultáneamente podría realizar pruebas muy sencillas como: utilizar la aplicación, ejecutar una request que no viaje por canales seguros y verificar que efectivamente se este capturando lo que deseo

Respuesta correcta: [None]

Comentarios para respuesta: La verificación formal es más compleja en este caso.

El punto es que deberías montar un servidor de DNS en la red, a la cuál accedería el dispositivo android y firmas con un certificado firmado por un certificado que tenés que agregar a la configuración de dispositivo android como certificado válido raíz. Luego generarás un certificado firmado con ese que coincida con el dns al que se conecta la aplicación android que es el man-in-the-middle. Desde ahí reestablecés una conexión al servidor real por internet pero pudiendo controlar y acceder a todo el tráfico.

### Pregunta 3

10 de 10 puntos



La Autenticación de un usuario implica verificar que un usuario tiene una pieza de información que puede contrastarse contra la que tiene un sistema y con eso decidir si la verificación fue correcta o incorrecta.

Respuesta seleccionada: ☒ Verdadero

Respuestas: ☒ Verdadero  
☐ Falso

Comentarios para respuesta: Si

### Pregunta 4

10 de 10 puntos



En un sistema de control industrial muy importante (equipos embebidos que controlan desde cintas transportadoras hasta bombas de gases tóxicos), existe una metodología para realizar los cambios. El encargado del equipo tiene una llave puesta en este en modo "RUN" y cuando quiere realizar un cambio, debe salir de su estación de trabajo, cambiar de edificio, ponerse las protecciones necesarias y girar la llave a modo "CHANGE", luego volver a la estación de trabajo, realizar el cambio y repetir el operativo para poner el sistema en modo "RUN" nuevamente. Para ahorrar tiempo, muchos operarios dejan la llave puesta en modo "CHANGE" e ignoran los carteles de alerta para que el sistema funcione igual. ¿Qué principios de diseños se están violando en esta situación? Tanto por parte del operario como por parte del diseñador del sistema. ¿Por qué?

Respuesta seleccionada: aceptacion psicologica: los mecanismos de seguridad no tienen porque dificultar el acceso al recurso, esto justamente genera lo que realizan los muchos operarios, el "ahorrar tiempo" e ignorar los carteles de alerta

economia de mecanismos: los mecanismos de seguridad deben ser simples, asi se previenen la mayor cantidad de fallas y en caso que haya una se puede solucionar mas rapido, en el caso del enunciado no parece simple todo el procedimiento que debe realizar el operario para simplemente girar una llave, se podria solucionar poniendo la estacion de trabajo del operario en el mismo edificio donde este se encuentra por ejemplo

mediacion completa: la verificacion del usuario para acceder a un recurso se debe realizar en todo momento, en el caso del enunciado con el simple hecho de ponerse protecciones y girar una llave puede modificar el comportamiento de un equipo embebido que controla bombas de gases toxicos, deberia verificarse que es alguien con permisos para realizar cada operacion, no es una operacion que se pueda realizar sin chequeos

adicionalmente se podria agregar a la lista separacion de privilegios: para otorgar acceso/permiso se deben utilizar mas de una condicion, en el caso del enunciado un solo operario alcanza para cambiar el modo de operacion de un equipo embebido que controla bombas de gases toxicos, nuevamente deberia ser una operacion que requiera algun otro operador o entidad que valida la accion a realizar, es algo muy peligroso

Respuesta [None]

correcta:

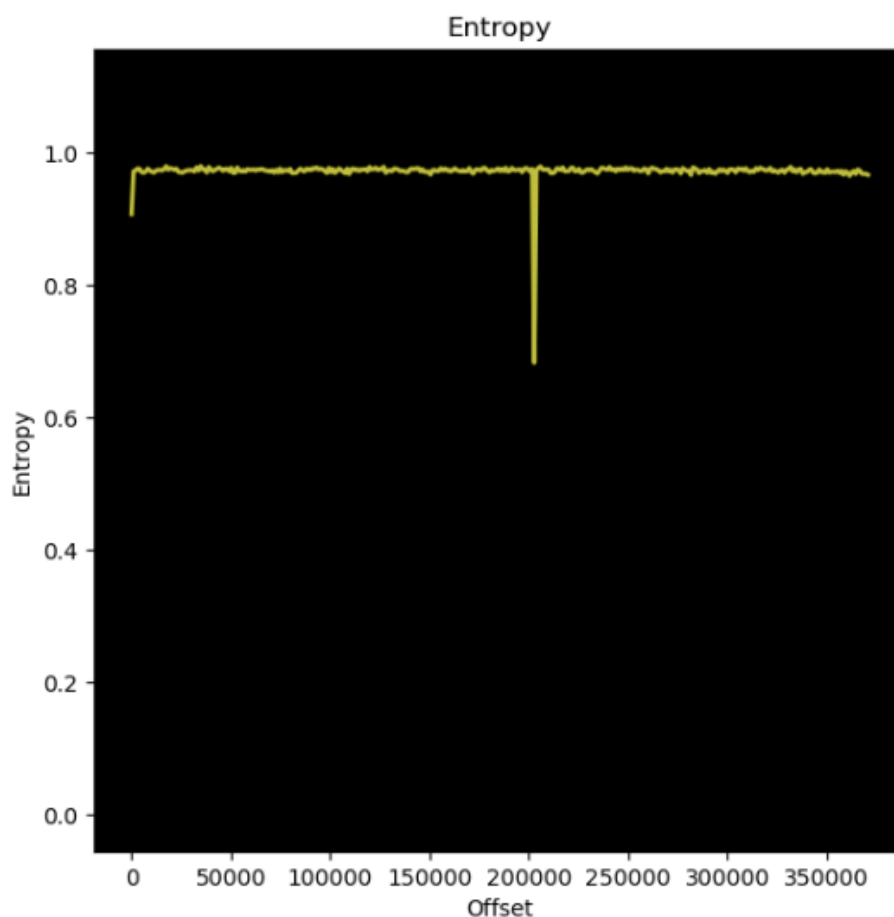
Comentarios [No se ha dado ninguna]  
para  
respuesta:

## Pregunta 5

10 de 10 puntos



La siguiente imagen es el resultado de un análisis sobre una imagen adjunta en un mail sospechoso. En el eje X se presenta el offset en bytes desde el principio del archivo y el eje Y la entropía sobre ese byte. ¿Qué puede decir sobre el archivo? Fundamente por qué el sistema pudo detectarlo como sospechoso. ¿Qué representa la Entropía ?



Respuesta seleccionada: se podría decir que el archivo brinda información del mismo, dado que la entropía se encarga de representar la incertidumbre respecto de una variable (a mayor entropía menos se conoce, y a menor entropía más información se dispone) el byte de ese offset que sufre un pico está dando información sobre el contenido (podría tener contenido esteganografiado o algo embebido por ejemplo) la detección como sospechosa es debido a que la entropía disminuye (pasa de valer 1 a 0.65 aproximadamente)

Respuesta correcta: [None]

Comentarios para respuesta: [No se ha dado ninguna]

## Pregunta 6

5 de 10 puntos



Para un trabajo práctico de la universidad, con su grupo concuerdan realizar un “hosteador de CVs”. La idea es que una persona suba su CV como un archivo HTML y su servicio simplemente hostearía el archivo, garantizando su disponibilidad y ofreciendo que esté bajo el nombre de dominio que usted elija. ¿Ve algún problema de seguridad en la idea? Argumente su respuesta.

Respuesta seleccionada:

el principal problema es que al redirigir a un sitio completamente desconocido pierdo control (redirection to untrusted sites), por ende allí puede suceder absolutamente cualquier cosa (por ejemplo podría ser una pagina maliciosa o imitar una pagina del estilo facebook/gmail etc, se abre un abanico de posibles ataques al usuario ingenuo que simplemente queria ver un CV, es como que lo estamos mandando a una trampa desde el vamos dado que desconocemos completamente el contenido del HTML subido, a menos que lo analicemos)

Respuesta



correcta:

Es una muy mala idea desde el punto de vista de seguridad porque un usuario podría subir un HTML con código malicioso y nosotros los estaríamos hosteando para que cualquier persona que entre, lo active. Habría que \*mínimo\* sanitizar la entrada y aún así, revisar todos los links que utilice.

Comentarios  
para

El principal problema es una situación de XSS explotada desde el HTML.

respuesta:

## Pregunta 7

6 de 10 puntos



Se encuentra en una página de “filas virtuales” para poder comprar entradas a un recital. Viendo que está en la posición N°86 y los tickets se agotan, decide ver si puede apurar el trámite. En eso, se da cuenta que el servicio web utiliza una librería de javascript que corre en el browser para realizar el mecanismo de fila. ¿Es correcto esto? En caso de que no lo sea, ¿Qué tipo de vulnerabilidad sería? ¿Podría abusarse para saltarse la fila?

Respuesta

seleccionada:

no es correcto dado que todo tipo de manejo/comportamiento del lado del cliente es completamente modificable/alterable, por ende se podría saltar la posición en la fila (asumiendo que la misma no utiliza un backend para ir modificando las filas, sino que depende todo meramente de los clientes)

Respuesta

[None]

correcta:

Comentarios

para

respuesta:

Vulnerabilidad de incorrecta implementación de mecanismos de autorización

## Pregunta 8

10 de 10 puntos



Dado el siguiente snippet de código, indicar qué errores encuentra. En caso de encontrar algún bug, indicar por qué es un bug y qué input lo explotaría. (Ayuda: El número ASCII de las letras mayúsculas comienza en 0x41 = 'A').

```

1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main(){
5     int sectest = 0;
6     char buffer[10];
7
8     printf("User Login\n");
9     printf("Please insert password:\n");
10    fgets(buffer, 15, stdin); //extra space just in case
11    if(sectest==0x41424241){
12        printf("Access granted!\n");
13    }else{
14        printf("Keep trying %x\n", sectest);
15    }
16 }

```

Respuesta seleccionada: primero el programa lee 15 bytes de stdin y los deposita en un buffer de 10 bytes, lo cual destaca el primer error: buffer overflow, explotando direcciones de memoria por como se maneja C y la memoria, las variables se van pusheando en el stack, por lo que por debajo de los 10 bytes reservados para el buffer se encuentran los 4 bytes para almacenar la variable sectest (la cual se compara contra los bytes formados por los valores ASCII de las letras ABBA) con estos conocimientos podemos ejecutar el programa pasandole 10 caracteres basura y al final concatenarle la representacion ASCII de los valores que utiliza en la comparacion, quedando como ese parametro, por ejemplo, que le pasamos por stdin algo como "xxxxxxxxxxABBA", y esto bypasseara la linea 11, debido a que gracias al exploit de la vulnerabilidad buffer overflow, hemos pisado la variable sectest con nuestro string de input por stdin

Respuesta [None]

correcta:

Comentarios [No se ha dado ninguna]  
para  
respuesta:

## Pregunta 9

2 de 10 puntos



Suponiendo el software del controlador de las barras de grafito de la central nuclear de Chernobyl, ¿Se puede asegurar que un sistema cómo este es seguro mediante algún mecanismo?

Respuesta seleccionada:

tomando como hecho que Chernobyl es completamente radioactiva, nadie podria acercarse a la central en cuestion, por ende asumiendo que algun robot o ente pueda acercarse y depositar un chip del estilo IoT que wireless se comunice con una central informando reportes, no se podria poner un controlador de barras de grafico en la central nuclear de Chernobyl  
ahora bien, asumiendo que dicho dispositivo se encuentra alli presente, el mismo genera reportes y los debe enviar de alguna forma a los operarios, por ende tiene una salida a internet, se debe comunicar, por lo tanto ya esto representa una via para poder atacarlo, todo sistema embebido corre riesgo tarde o temprano debido a que se lo debe actualizar constantemente (un claro ejemplo es el caso del muchacho que se hizo apodar Janitor, que consideraba que IoT era una cancer para internet debido a las grandes vulnerabilidades que presentaban los dispositivos y como la gente no los actualizaba, por ende los hackers los explotaban para realizar ataques DDoS, a lo que Janitor decidio corromper miles de dispositivos bajo la justificacion que era un bien necesario para que la internet este sana de nuevo)

Respuesta [None]  
correcta:

Comentarios Chernobyl es todavía operacional, hay operadores adentro de la central e incluso la central produce energía ! El area alrededor no está habitada.  
para  
respuesta:

De todas formas, la pieza de código que actua de controlador se puede verificar por métodos formales siempre que sea acotada. Es decir se verifica que para todas las entradas posibles produce el resultado esperado.

## Pregunta 10

10 de 10 puntos



Considerar una política de contraseñas de 8 caracteres, entre ellas letras del alfabeto inglés en minúscula y números. ¿Cuál sería la probabilidad de que un atacante pueda obtener la contraseña en menos de un año si este contase con una tasa de pruebas de 23.000 pruebas por segundo y si se cuenta con 5 bits de salt?

Respuesta # letras alfabeto ingles = 26  
seleccionada: # numeros = 10  
 $N = 36^8$   
 $T = 365 * 24 * 60 * 60 = 31536000$   
 $G = 23000 / 2^5 = 23000 / 32 = 718.75$   
 $P = T * G / N = 8.0346 \times 10^{-3} = 0.0080346$   
lo cual es un porcentaje del 0.8% (0.008) aproximadamente para obtener la contraseña bajo las condiciones indicadas

ACLARACION PUNTO 3)  
por autenticacion y contastar entiendo que refiere a los elementos involucrados en la autenticacion  
-A: informacion de autenticacion  
-C: informacion complementaria  
-F: funcion de derivacion de informacion complementaria ( $F:A \rightarrow C$ )  
-L: funcion de autenticacion, verifica el par  $AxC$  ( $L:AxC \rightarrow \{true, false\}$ )  
-S: funcion de seleccion, crea o actualiza A y C  
por lo que mi respuesta final es verdadero, dado que levanta la informacion complementaria y la utiliza en conjunto a la informacion de autenticacion para decidir si la verificacion fue correcta o incorrecta

Respuesta [None]  
correcta:

Comentarios [No se ha dado ninguna]  
para

respuesta:

miércoles 29 de junio de 2022 18H37' ART

← **Aceptar**