1-En la versión Community del proxy de interceptación web BurpSuite se puede utilizar el escáner de vulnerabilidades. ¿Verdadero o Falso?:
Seleccione una:
Verdadero
Falso

2- La vulnerabilidad de Cross Site Scripting Almacenado se considera una vulnerabilidad persistente. ¿Verdadero o falso?:
Seleccione una:
Verdadero
Falso

3- ¿Para qué se utiliza un servidor proxy como Burp Suite a la hora de realizar un análisis de hacking ético en un aplicativo web?:
a.A modo de VPN.
b.Para evitar ser rastreado.
c.Para navegar más rápido.
d.Para poder interceptar y modificar peticiones HTTP.

4- En la versión Community del proxy de interceptación web BurpSuite se puede utilizar el navegador web chromium que viene integrado. ¿Verdadero o Falso?:
Seleccione una:
Verdadero
Falso

5- Las vulnerabilidades de lógica de negocio tienen la misma criticidad y riesgo en cualquier aplicativo y no dependen de la naturaleza del aplicativo web ni de los datos que maneje. ¿Verdadero o falso?:
Seleccione una:
Verdadero
Falso

6- ¿Qué indica el error HTTP de tipo 403 devuelto en la primera línea de la respuesta del servidor?:
a.“Redirect” – La navegación del usuario se redirige a otra página distinta.
b.“Not Found”- La página solicitada no existe.
c.“Forbidden” – La página solicitada existe pero no tienes privilegios para acceder a la misma.
d.“Service Unavailable” – Ha habido un error en el servidor y no se puede procesar la petición.

7- ¿Cuál de las siguientes medidas de seguridad es la más indicada para contener ataques de tipo fuerza bruta en un aplicativo web?:
a.Identificar y bloquear la dirección IP que esté realizando el ataque.
b.Utilizar un sistema de tipo Captcha.
c.Mantener los sistemas actualizados.
d.Bloquear los usuarios del aplicativo tras 3 intentos fallidos de inicio de sesión.

8- ¿Qué indican los códigos de estado de tipo 500 del protocolo HTTP?:
a.Respuestas de redirección. Indica que el cliente necesita realizar otra petición a la dirección URL indicada por el servidor en la cabecera de respuesta.

b.Respuestas que han sido procesadas correctamente y no retornan ningún tipo de error.
c.Errores causados por el servidor.
d.Errores causados por el cliente.

9- (Respuesta multiple) Indica cuáles de estas vulnerabilidades son vulnerabilidades que afectan al cliente de un aplicativo web:
a.HTTP Scripting.
b.HTTP Splitting.
c.Cross Site Scripting almacenado.
d.Escalada de privilegios.

10- El proxy de interceptación web ZAProxy dispone de una versión web y de una versión de pago. ¿Verdadero o Falso?:
Seleccione una:
Verdadero
Falso

Segundo intento
1- ¿Qué son los parámetros de una petición HTTP?:
a.Es un par clave/valor que utiliza el protocolo HTTP para entregar los datos de entrada a la funcionalidad indicada.
b.Representan la ruta dentro del dominio al que se quiere acceder.
c.Son los datos que indican la versión del navegador utilizado por el cliente.
d.Protegen los identificadores de sesión para que no puedan ser usurpados.

2- (respuesta multiple) Indica cuáles de estas técnicas pueden ser utilizadas para realizar pruebas de “Evasión del proceso de autenticación” en un aplicativo web:
a.Intentar predecir cómo se generan los identificadores de sesión para localizar identificadores de sesión de otros usuarios.
b.Comprobar la existencia de un parámetro que indique si se está autenticado y modificar su valor para tratar de engañar al aplicativo web.
c.Inyección de código SQL en el formulario de acceso a la aplicación.
d.Acceso directo a la parte privada.

3- En las pruebas de recolección de información podemos extraer información que nos puede ser de utilidad en los metadatos de los archivos que maneja la aplicación. ¿Verdadero o Falso?:
Seleccione una:
Verdadero
Falso

4- El atributo de las cookies "HttpOnly" disminuye el riesgo en caso de localizar una vulnerabilidad de tipo Cross Site Scripting. ¿Verdadero o falso?:
Seleccione una:
Verdadero
Falso

5- (respuesta multiple) Indica cuáles de las siguientes se consideran vulnerabilidades de lógica de negocio:
a.Vulnerabilidad presente en una aplicación bancaria por la cual un atacante puede enviar transferencias internacional evitando pagar la comisión establecida.

b.Vulnerabilidad presente en una tienda online, a través de la vulnerabilidad identificada un atacante puede ejecutar comandos en el Sistema Operativo de manera remota.
c.Vulnerabilidad presente en una tienda online, a través de la vulnerabilidad identificada, un atacante, generar códigos de descuento.
d.Vulnerabilidad presente en una aplicación bancaria por la cual un atacante puede hacerse pasar por otro usuario legítimo de la plataforma.

6- ¿Qué método HTTP permite que podamos incluir datos en el cuerpo de la petición?:
a.GET
b.POST
c.INCLUDE
d.TRACE

7- Cuál de las siguientes herramientas nos permite obtener rápidamente las tecnologías, librerías, frameworks, etc. que se utilizan en un aplicativo web:
a.Whatweb
b.Wpscan
c.Joomscan
d.CMSMap

8- ¿Qué definición se ajusta más para describir las vulnerabilidades “referencias inseguras a objetos de manera directa - IDOR”?:
a.Un atacante puede acceder a información interna del Sistema Operativo.
b.Un atacante puede modificar objetos del Sistema Operativo.
c.Un atacante puede modificar el comportamiento del servidor web.
d.Un atacante puede acceder a información de otro usuario.

9- ¿Cuál es la función del Modelo en la arquitectura Modelo Vista controlador?:
a.Recoger y gestionar los datos de los usuarios para que sean tratados.
b.Es la representación visual de los datos y como son presentados al cliente.
c.Realiza las operaciones lógicas de la aplicación, se apoya en el código del aplicativo para esta tarea.
d.Gestiona y mantiene los datos de la aplicación, se apoya en la Base de Datos para esta tarea.

10- (respuesta multiple) Indica cuáles de estas vulnerabilidades son vulnerabilidades que afectan al servidor de un aplicativo web:
a.Inyección remota de código.
b.Suplantación de identidad.
c.Bloqueo de la cuenta de usuario.
d.Denegación de servicio.