Examen para HE05.

Intento1.

Pregunta 1

¿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. Para evitar ser rastreado.
b. A modo de VPN.
c. Para navegar más rápido.
d. Para poder interceptar y modificar peticiones HTTP.

Pregunta 2

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

Pregunta 3

Indica cuál de las siguientes afirmaciones NO es correcta a la hora de referirnos a una vulnerabilidad de Cross Site Scripting Almacenado:

a. Tiene un valor CVSS más bajo que una vulnerabilidad de tipo Cross Site Scripting Reflejado.
b. Se produce por una mala validación de los datos de entrada (la aplicación no elimina caracteres especiales):
c. El usuario del aplicativo web ejecutara el código inyectado cuando acceda visualice la información almacenada por el atacante.
d. El código inyectado se almacena en el aplicativo Web vulnerable.

Pregunta 4

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

Verdadero
Falso

Pregunta 5

¿Qué son los parámetros de una petición HTTP?:

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

Pregunta 6

¿Cuáles de las siguientes afirmaciones correspondientes con los atributos de las cookies es correcta?:

a. El atributo “HttpOnly” especifica que la cookie no puede ser consultada o transmitida desde scripts de cliente (como JavaScript).
b. El atributo “domain” indica que únicamente es posible conectarte al aplicativo web si te encuentras situado en la red interna de la oficina.
c. El atributo “secure” fuerza al navegador del usuario a transmitir la cookie sólo mediante canales cifrados HTTPS.
d. El atributo “Path” indica la ruta actual a la que se accede en cada momento.

Pregunta 7

¿Cuáles de las siguientes técnicas se pueden utilizar para detectar paneles de administración expuestos?:

a. Google Dorks.
b. Enumeración de directorios.
c. Fuerza bruta en el formulario de inicio de sesión.
d. Monitorizar las cabeceras “Server” de la respuesta HTTP.

Pregunta 8

En un aplicativo, la capa del controlador es con la que interactúa un usuario. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 9

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

Pregunta 10

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

Verdadero
Falso

Intento 2.

Pregunta 1

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

Pregunta 2

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

Pregunta 3

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

Pregunta 4

En el proxy de interceptación web BurpSuite se puede utilizar la funcionalidad del intruder para automatizar la autenticación de un usuario mediante tokens. ¿Verdadero o Falso?
Seleccione una:

Verdadero
Falso

Pregunta 5

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

Pregunta 6

Indica cuáles de estas técnicas pueden ser utilizadas para realizar pruebas de "Evasión del proceso de autenticación" en un aplicativo web:

a. Comprobar la existencia de un parámetro que indique si se está autenticado y modificar su valor para tratar de engañar al aplicativo web.
b. Acceso directo a la parte privada.
c. Inyección de código SQL en el formulario de acceso a la aplicación.
d. Intentar predecir cómo se generan los identificadores de sesión para localizar identificadores de sesión de otros usuarios.

Pregunta 7

¿Cuál de las siguientes medidas de seguridad es la más indicada para contener ataques de tipo fuerza bruta en un aplicativo web?:

a. Mantener los sistemas actualizados.
b. Bloquear los usuarios del aplicativo tras 3 intentos fallidos de inicio de sesión.
c. Identificar y bloquear la dirección IP que esté realizando el ataque.
d. Utilizar un sistema de tipo Captcha.

Pregunta 8

Indica cuáles de las siguientes afirmaciones sobre la vulnerabilidad Cross Site Scripting Reflejado es correcta:

a. Mediante esta vulnerabilidad se puede inyectar código JavaScript que será ejecutado en el navegador del usuario en caso de que no se validen los parámetros de entrada del aplicativo.
b. Se considera un tipo de ataque persistente que afecta al servidor que sustenta la aplicación.
c. El código inyectado se almacena en el servidor y es ejecutado por los navegadores de los usuarios al visitar la sección o funcionalidad afectada.
d. En ningún momento el código inyectado se guarda en el servidor, sino que habría que generar la dirección URL con la inyección en el parámetro y utilizar técnicas de ingeniería social para enviar el enlace a los usuarios e intentar que accedan al mismo.

Pregunta 9

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

Pregunta 10

Indica cuáles de estas vulnerabilidades son vulnerabilidades que afectan al servidor de un aplicativo web:

a. Suplantación de identidad.
b. Inyección remota de código.
c. Bloqueo de la cuenta de usuario.
d. Denegación de servicio.

Intento 3.

Pregunta 1

La cabecera "set-cookie" es una cabecera propia de la respuesta HTTP. ¿Verdadero o Falso?
Seleccione una:

Verdadero
Falso

Pregunta 2

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

Verdadero
Falso

Pregunta 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

Pregunta 4

Indica cuáles de las siguientes opciones se corresponden con las características más importantes que presenta un proxy de interceptación HTTP:

a. Interceptan toda la comunicación entre un navegador y el aplicativo web alojado en el servidor. Para ello se sitúan en medio de la comunicación.
b. Permiten modificar la petición HTTP realizada por el navegador antes de ser enviada al servidor.
c. Permiten modificar la respuesta HTTP realizada por el servidor antes de ser interpretada por el navegador.
d. Permiten conocer si un determinado usuario existe o no.

Pregunta 5

¿Qué definición se ajusta más para describir las vulnerabilidades “referencias inseguras a objetos de manera directa - IDOR” ?:

a. Un atacante puede acceder a información de otro usuario.
b. Un atacante puede modificar objetos del Sistema Operativo.
c. Un atacante puede acceder a información interna del Sistema Operativo.
d. Un atacante puede modificar el comportamiento del servidor web.

Pregunta 6

¿Cuál es la función del Modelo en la arquitectura Modelo Vista controlador?:

a. Realiza las operaciones lógicas de la aplicación, se apoya en el código del aplicativo para esta tarea.
b. Gestiona y mantiene los datos de la aplicación, se apoya en la Base de Datos para esta tarea.
c. Recoger y gestionar los datos de los usuarios para que sean tratados.
d. Es la representación visual de los datos y como son presentados al cliente.

Pregunta 7

Indica cuáles de estas vulnerabilidades son vulnerabilidades que afectan al cliente de un aplicativo web:

a. HTTP Splitting.
b. Cross Site Scripting almacenado.
c. Escalada de privilegios.

Pregunta 8

Indica cuáles de las siguientes se consideran vulnerabilidades de lógica de negocio:

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

Pregunta 9

¿Cuáles de los siguientes tipos de autenticación presentan más riesgos en caso de sufrir un ataque de tipo Man in the Middle?:

a. Autenticación basada en tokens.
b. Autenticación basada en cookies.
c. Uso de APIKey.
d. Autenticación HTTP Basic.