**Universidad Nacional Abierta y a Distancia**

**Vicerrectoría Académica y de Investigación**

**Curso: Segura de la información**

**Código: 202016905**

**Guía de actividades y rúbrica de evaluación –** Tarea 4 Test de Penetración

1. **Descripción de la actividad**

|  |  |
| --- | --- |
| **Tipo de actividad: En grupo colaborativo** | |
| **Momento de la evaluación: Intermedio** | |
| **Puntaje máximo de la actividad: 100 puntos** | |
| **La actividad inicia el:** lunes, 22 de abril de 2024 | **La actividad finaliza el:** miércoles, 15 de mayo de 2024 |
| **Con esta actividad se espera conseguir los siguientes resultados de aprendizaje:**  Formular medidas de mitigación de riesgos de seguridad de la información en productos de software de acuerdo con metodologías, técnicas y buenas prácticas de desarrollo seguro. | |
| **La actividad consiste en:**  ***Trabajo Colaborativo***  Hacer una revisión de las lecturas correspondientes a la Unidad 3 que se encuentran en el entorno de aprendizaje. Los temas son:   * Estándares para la seguridad de las aplicaciones * Codificación Segura de Aplicaciones * Vulnerabilidad de seguridad en aplicaciones web (OWASP 2017) * Pruebas y seguridad online de las aplicaciones web * Seguridad en las fases del S-SDLC   Cada estudiante elige uno de los siguientes interrogantes, se documenta y publica en el foro de la actividad la pregunta y la respuesta argumentada, con base en las lecturas realizadas y su criterio personal.  Interrogantes:   1. ¿identifique al menos tres estándares para la seguridad de la información? 2. ¿Qué es la codificación segura de aplicaciones? 3. ¿Qué es un Test de Penetración? 4. ¿Cuáles son las buenas prácticas y malas prácticas de desarrollo seguro? 5. ¿Qué son las pruebas de seguridad basadas en el riesgo?   Cada estudiante elige uno de los interrogantes mencionados anteriormente, se documenta y publica en el foro de la actividad la pregunta y la respuesta argumentada, con base en las lecturas realizadas y su criterio personal. Adicionalmente, debe hacer un comentario por lo menos a una respuesta de un compañero, para expresar de manera respetuosa y argumentada su respaldo, complemento o desacuerdo.  Es importante citar las fuentes que soportan las opiniones en formato APA 7, con el fin de que los compañeros las puedan consultar para ampliar la información.  A partir de las participaciones realizadas en el foro, el grupo elabora una presentación electrónica en línea, presentando la información relevante de los temas desarrollados en las preguntas. La estructura es la siguiente  Diapositiva 1: Portada  Diapositiva 2: Estándares para la seguridad de la información.  Diapositiva 3: Codificación Segura de Aplicaciones.  Diapositiva 4: Test de Penetración.  Diapositiva 5: Buenas y malas prácticas de desarrollo seguro.  Diapositiva 6: pruebas de seguridad basadas en el riesgo.  Diapositiva 7. Conclusiones.  Diapositiva 8. Referencias bibliográficas  ***Trabajo Individual***  En esta actividad se debe realizar un test de penetración a la aplicación web BADSTORE. Para realizar la actividad debe descargar las siguientes herramientas:   * Descargar ORACLE, debe acceder a través de la siguiente dirección web: <https://www.virtualbox.org> * También tendrás que descargar e instalar ZAP. Debe acceder a través de la siguiente dirección web: <https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project> * Descarga la máquina virtual con la aplicación BADSTORE. Debe acceder a través de la siguiente dirección web: <https://www.dropbox.com/sh/7ewzuosszqslkok/AADL6CSiXkoFPWdmfnwjHDLYa?dl=0> * Importa el servicio virtualizado badstore.ova desde ORACLE virtualbox. * En configuración - almacenamiento, asocia la imagen BadStore-212.iso en el controlador IDE (cdrom) y configura la máquina virtual para que arranque primero desde el cdrom.     Figura 1. Configuración almacenamiento de BadStore-212.iso   * Crea una red virtualbox HOST ONLY en VIRTUALBOX → (Archivo → Administración redes solo anfitrión) o (Archivo- preferencias- red- redes solo anfitrión- añadir una red- habilitar DCHP) según versión y configurar de la siguiente forma:       Figura 2. Crea una red virtualbox HOST ONLY    Figura 3. Servidor DHCP   * Configura el adaptador de red solo-anfitrión con las siguientes direcciones:     Figura 4. Configurar adaptador de red   * Comprobar en la configuración de la máquina virtual BADSTORE → RED que el ADAPTADOR 1 está habilitado y conectado a ADAPTADOR SOLO ANFITRION. * Arrancar la máquina virtual y ejecutar ***ifconfig -a*** para comprobar la dirección IP asociada al dispositivo eth0. * Incluir en el fichero HOST de la máquina anfitriona la entrada correspondiente a la dirección IP de ETH0. Por ejemplo, si la dirección IP obtenida por DHCP para el dispositivo ETH0 es 192.168.56.110:   192.168.56.110, [www.badstore.net](http://www.badstore.net)   * Realiza el Test de penetración de la aplicación BADSTORE con el Scanner de vulnerabilidades ZAP atacando al nombre asociado a la dirección del dispositivo eth0 obtenida en el paso anterior: [www.badstore.net/cgi-bin/badstore.cgi](http://www.badstore.net/cgi-bin/badstore.cgi) * Audita manualmente al menos tres vulnerabilidades para comprobar la veracidad de las alertas por parte de ZAP e indicar la forma de como mitigarla. * Guardar el informe de la herramienta ZAP en formato html.   El estudiante debe realizar la entrega del documento del trabajo individual con la siguiente estructura: PortadaObjetivosDocumentación de como se ha llevado a cabo el procedimiento del Test:  * Configuración de la máquina virtual (evidencia) * Instalación de la herramienta OWASP ZAP (evidencia) * Configuración de la red de la maquina BADSTORE (evidencia) * Test de penetración (evidencia) * Configuración del navegador del proxy (evidencia) * ATAQUE 1: Spider (evidencia) * ATAQUE 2: scaneo (evidencia) * ATAQUE 3: Inyección SQL (evidencia)  Resultados de las vulnerabilidades encontradas y la forma de mitigar cada vulnerabilidad.Referencias bibliográficas Adicionalmente, debe adjuntar el informe de la herramienta ZAP en formato html. | |
| **Para el desarrollo de la actividad tenga en cuenta que:**  En el entorno de Información inicial debe:  Consultar la agenda del curso para revisar las fechas de entrega de la actividad  En el entorno de Aprendizaje debe:  Leer las lecturas sugeridas para la unidad 3.   * Ingresar al foro de la actividad para debatir con los compañeros sobre los temas referidos. * Compartir avances de la actividad individual.   En el entorno de Evaluación debe:  Cada estudiante envía un documento digital (un documento Word o PDF) que contiene el link de la presentación electrónica en línea y el documento del trabajo individual.­­ | |
| **Evidencias de trabajo independiente:**  Las evidencias de trabajo independiente para entregar son:   * Trabajo final individual * Informe de la herramienta ZAP en formato html. * Aportes en el foro | |
| **Evidencias de trabajo grupal:**  Las evidencias de trabajo grupal a entregar son:   * Participación en el foro de la actividad. * Documento digital con el link de la presentación electrónica | |

1. **Lineamientos generales para la elaboración de las evidencias de aprendizaje a entregar.**

|  |
| --- |
| Para evidencias elaboradas **en grupo colaborativamente**, tenga en cuenta las siguientes orientaciones   1. Antes de construir la presentación electrónica es importante analizar y organizar la información. 2. A medida que selecciona la información construya la bibliografía. 3. Puede usar el software para presentaciones en línea que prefiera, algunas opciones son: canva, emaze, prezi, genially. 4. Después de construir la presentación electrónica, copie el link de la presentación en un documento Word y envíe este documento por el entorno de evaluación. Verifique que el link funcione correctamente y no tenga restricciones de acceso. |
| Tenga en cuenta que todos los productos escritos individuales o grupales deben cumplir con las normas de ortografía y con las condiciones de presentación que se hayan definido.  En cuanto al uso de referencias considere que el producto de esta actividad debe cumplir con las normas **APA** |
| En cualquier caso, cumpla con las normas de referenciación y evite el plagio académico, para ello puede apoyarse revisando sus productos escritos mediante la herramienta Turnitin que encuentra en el campus virtual.  Considere que en el acuerdo 029 del 13 de diciembre de 2013, artículo 99, se considera como faltas que atentan contra el orden académico, entre otras, las siguientes: literal e) “El plagiar, es decir, presentar como de su propia autoría la totalidad o parte de una obra, trabajo, documento o invención realizado por otra persona. Implica también el uso de citas o referencias faltas, o proponer citad donde no haya coincidencia entre ella y la referencia” y liberal f) “El reproducir, o copiar con fines de lucro, materiales educativos o resultados de productos de investigación, que cuentan con derechos intelectuales reservados para la Universidad”  Las sanciones académicas a las que se enfrentará el estudiante son las siguientes:   1. En los casos de fraude académico demostrado en el trabajo académico o evaluación respectiva, la calificación que se impondrá será de cero puntos sin perjuicio de la sanción disciplinaria correspondiente. 2. En los casos relacionados con plagio demostrado en el trabajo académico cualquiera sea su naturaleza, la calificación que se impondrá será de cero puntos, sin perjuicio de la sanción disciplinaria correspondiente. |

**3. Formato de Rúbrica de evaluación**

|  |  |
| --- | --- |
| **Tipo de actividad: En grupo colaborativo** | |
| **Momento de la evaluación: Intermedio** | |
| **La máxima puntuación posible es de 100 puntos** | |
| **Primer criterio de evaluación:**  **Contenido:**  Apropiación de conceptos de los estándares para la seguridad, codificación segura, Test de Penetración, desarrollo seguro y pruebas basadas en el riesgo.  **Este criterio representa 30 puntos del total de 100 puntos de la actividad.** | **Nivel alto:**  Apropia los conceptos de estándares para la seguridad de la información, codificación segura, Test de Penetración, practicas de desarrollo seguro y pruebas basadas en el riesgo y lo refleja en la presentación electrónica en línea.  **Si su trabajo se encuentra en este nivel puede obtener entre 21 puntos y 30 puntos.**  **Nivel Medio:**  Algunas ideas que expresa en la presentación electrónica no son coherentes o no se presenta la totalidad de conceptos solicitados.  **Si su trabajo se encuentra en este nivel puede obtener entre 11 puntos y 20 puntos.**  **Nivel bajo:** Las ideas plasmadas en la presentación no presentan comprensión del concepto los conceptos de estándares para la seguridad de la información, codificación segura, Test de Penetración, practicas de desarrollo seguro y pruebas basadas en el riesgo.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 10 puntos.** |
| **Segundo criterio de evaluación:**  **Forma:**  Presentación del documento.  **Este criterio representa 5 puntos del total de 100 puntos de la actividad** | **Nivel alto:** La presentación se estructura de forma adecuada, se realiza mediante un software de presentaciones electrónicas en línea e incluye referencias en formato APA.  **Si su trabajo se encuentra en este nivel puede obtener entre 4 puntos y 5 puntos.**  **Nivel Medio:**  La presentación no incluye referencias, no se estructura de manera ordenada totalmente o no se realiza en un software de presentaciones electrónicas en línea.  **Si su trabajo se encuentra en este nivel puede obtener entre 2 puntos y 3 puntos.**  **Nivel bajo:**  La presentación no se estructura de forma. organizada **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 1 punto.** |
| **Tercer criterio de evaluación:**  **Participación:**  Participación en el foro.  **Este criterio representa 5 puntos del total de 100 puntos de la actividad** | **Nivel alto:**  Promueve la generación de diversos puntos de vista relacionados con la temática, enriqueciendo la discusión y agregando valor a la misma.  **Si su trabajo se encuentra en este nivel puede obtener entre 4 puntos y 5 puntos.**  **Nivel Medio:**  Los contenido de algunos mensajes no son coherentes con la temática tratada, no todos son originales o no siempre promueven la generación de diversos puntos de vista, enriqueciendo la discusión y agregando valor a la misma  **Si su trabajo se encuentra en este nivel puede obtener entre 2 puntos y 3 puntos.**  **Nivel bajo:**  Los contenidos de los mensajes no son coherentes con la temática tratada, no son originales o no promueven la generación de diversos puntos de vista para la discusión y agregando valor a la misma.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 1 punto.** |
| **Cuarto criterio de evaluación:**  **Contenido:**  Realiza el Test de Penetración en una aplicación WEB.  **Este criterio representa 50 puntos del total de 100 puntos de la actividad** | **Nivel alto:** Cada estudiante realiza el Test de penetración de una aplicación propuestacon las evidencias de la configuración de la aplicación, los ataques y las vulnerabilidades encontradas.  **Si su trabajo se encuentra en este nivel puede obtener entre 26 puntos y 50 puntos.**  **Nivel Medio:** El estudiante realiza de forma parcial el Test de penetración de una aplicación propuestacon algunas de las evidencias de la configuración de la aplicación, los ataques y las vulnerabilidades encontradas.  **Si su trabajo se encuentra en este nivel puede obtener entre 10 puntos y 25 puntos.**  **Nivel bajo:** El estudiante no realiza de forma adecuada el Test de Penetración o no realiza la entrega la actividad.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 9 puntos.** |
| **Quinto criterio de evaluación:**  **Forma:**  Presentación del documento del trabajo independiente.  **Este criterio representa 10 puntos del total de 100 puntos de la actividad** | **Nivel alto:** El estudiante presenta un documento en Word o PDF con todos los elementos: Portada, objetivos, Portada, Objetivos, Documentación de como se ha llevado a cabo el procedimiento del Test, resultados de las vulnerabilidades y salvaguardas, e incluye referencias bibliográficas en formato APA y sin errores de ortografía y buena redacción.  **Si su trabajo se encuentra en este nivel puede obtener entre 6 puntos y 10 puntos.**  **Nivel Medio:**  El estudiante presenta un documento en Word o PDF con algunos los elementos solicitados e incluye referencias bibliográficas en formato APA y/o con errores de ortografía y/o buena redacción.  **Si su trabajo se encuentra en este nivel puede obtener entre 3 puntos y 5 puntos.**  **Nivel bajo:**  El documento no se estructura de forma organizada, tiene errores de ortografía y mala redacción, no incluye las normas APA o no fue realizada la actividad.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 2 puntos.** |