CONTROL DE CONOCIMIENTOS *(Exámen no oficial para orientación del Alumn@).*

Instrucciones: finalizar en 1hora, marcando una sóla posibilidad, sin que la respuesta errónea reste.
Poner nombre al archivo pdf, así: (Nombre_Apellidos_EXAMEN.pdf).
Envíar voluntariamente para evaluación y mucha suerte;)

Fecha: 21 Octubre 2024
PUESTA EN PRODUCCIÓN SEGURA.

NOMBRE: _____
APELLIDOS: _____

1. Relaciona *tipo de dato* personal con su nivel de sensibilidad: *(0,10 puntos cada uno)*

1. DNI	*Niveles de sensibilidad:*
2. Edad	
3. ADN	A. Alta Sensibilidad
4. Correo Electrónico	
5. Datos Biométricos	B. Media Sensibilidad
6. Dirección de casa	
7. Nombre de su mascota	C. Baja Sensibilidad
8. Viajes realizados	
9. Cosas en la web	
10. Historial médico	

2. *Desencripta* el siguiente código MD5: *(1punto)*

098f6bcd4621d373cade4e832627b4f6

3. Verdadero o Falso, *con razonamiento:* *(0,10 pts. cada. Con poesía 0,20 pts;)*
Ejemplo (no puntúa): 6. El archivo .htaccess sirve para configurar todos los servidores. FALSO, sólo para APACHE.

1. El DNI es considerado un dato de alta sensibilidad.
2. Las pruebas NO funcionales se enfocan en aspectos como la usabilidad, seguridad y rendimiento de un sistema.
3. El modelo SaaS permite que l@s usuari@s instalen y gestionen el Software en su infraestructura local.
4. La capa Física del modelo OSI siempre suelen ser l@s usuari@s.
5. Android es el Sistema Operativo propiedad y creado por Google.

4. Preguntas de Selección Múltiple: *(0,20 puntos cada uno)*

1. Qué capa del modelo OSI es responsable de la transmisión de datos entre dispositivos de red?

   a. Capa de Sesión

   b. Capa de Transporte

   c. Capa de Enlace de Datos

   d. Capa Física

2. El ciclo DEMING para la mejora continua en el desarrollo de software incluye las siguientes fases:

   a. Planificar, Desarrollar, Integrar, Probar

   b. Planificar, Hacer, Verificar, Actuar

   c. Establecer, Ejecutar, Optimizar, Monitorizar

   d. Diseñar, Construir, Desplegar, Mantener

3. Cuál NO es un servicio del modelo de arquitectura Cloud?

   a. SaaS

   b. IaaS

   c. PaaS

   d. BIOS

4. Son Estándares de Acceso de Sesión?

   a. Cookies, tokens y captchas

   b. Login, password y email

   c. Contraseñas largas

   d. Cifrar navegador

5. Puertos considerados seguros, según conoces:

   a. HTTP, FTP, Telnet

   b. SMTP, IMAP4, POP3

   c. HTTPs, FTPs, SSH

   d. Cpanel, LDAP

5. Relaciona los *conceptos* mejor emparejados: *(0,10 puntos cada uno)*

1. PaaS	a. https
2. http	b. allow
3. SSL	c. 27.001
4. deny	d. Privacidad
5. Nmap	e. mapeo de redes
6. Capa de aplicación	f. OSINT
7. ISO	g. Plataforma como Servicio
8. CVE	h. modelo OSI/TCP
9. VPN	i. puerto 80
10. Exift	j. MITRE.org

6. Completa los espacios: *(0,20 puntos cada uno)*

Las vulnerabilidades que afectan a formularios HTML mal protegidos y los ataques más representativos en relación a OWASP Top10 _____(WSTG) son:

1. *Inyección de Código A03:2021 (SQL Injection o Inyección en formularios):*

- Los atacantes pueden_____ código malicioso en los campos de entrada de formularios, como consultas SQL permitiendo acceder o modificar _____.
- Mitigación: Validación y saneamiento de entradas, y uso de consultas preparadas o parametrizadas en la interacción con bases de datos.

2. *Cross-Site Scripting A07:2021 (XSS):*

- Los formularios pueden ser utilizados para inyectar scripts maliciosos que se ejecutan en el _____ del user cuando la entrada no es adecuadamente filtrada.
- Mitigación: Saneamiento y codificación de las entradas de usuari@s, además de _____ la ejecución de scripts no confiables en la página.

7. Ordena el proceso de pruebas de intrusión o *Pentesting*: *(0, 20 puntos cada uno)*

A. EXPLOTAR SISTEMAS

B. LIMPIEZA O INFORME

C. ANALIZAR INFORMACIÓN

D. OBTENER DATOS

E. PERSISTENCIA

8. *Crea una lista con CINCO programas* o aplicaciones web vistas o utilizadas durante el curso y explica brevemente su funcionalidad dentro de la Puesta en Producción Segura: *(0,20 puntos cada uno)*

Ejemplo (no puntúa): 6. OSINT FRAMEWORKS: Portal de enlace a herramientas para búsquedas abiertas.

1.
2.
3.
4.
5.

9. Enumera 10 ataques de Ciberseguridad. *Dobla tu puntuación con sus contramedidas!* *(0,05 puntos cada uno.. 0,10 puntos con su corrección)*

Ejemplo (no puntúa): 11. Sniffing (extracción de datos en red). Proteger con puertos seguros (https/443)

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

10. Define los siguientes 10 *acrónimos* y significado : *(0,10 puntos cada uno)*

1. CVE
2. CSS
3. OSINT
4. HTTPS
5. SSL
6. OWASP
7. SGSI
8. CASB
9. VPN
10. NGFW