Pentest Web

Clase 8: Cuestionario

Vulnerabilidad informática

Qué es una vulnerabilidad informática?

A. Un virus que ya está presente en el sistema.
B. Una ineficiencia que afecta el rendimiento del software de manera sistematica.
C. Un defecto en un sistema que puede ser explotado para comprometerlo.
D. Una funcionalidad que no sea necesaria y aumenta la superficie de exposición.

Vulnerabilidad informática

Qué es una vulnerabilidad informática?

A. Un virus que ya está presente en el sistema.
B. Una ineficiencia que afecta el rendimiento del software de manera sistematica.
C. Un defecto en un sistema que puede ser explotado para comprometerlo.
D. Una funcionalidad que no sea necesaria y aumenta la superficie de exposición.

ANSWER: C

Lenguajes backend

Cuáles de los siguientes lenguajes son todos exclusivamente del backend?

A. Java, JavaScript, Rust

B. Php, Perl, Python

C. Groovy, Markdown, HTML

D. C, C++, CSS

Lenguajes backend

Cuáles de los siguientes lenguajes son todos exclusivamente del backend?

A. Java, JavaScript, Rust

B. Php, Perl, Python

C. Groovy, Markdown, HTML

D. C, C++, CSS

ANSWER: B

Sintaxis URL

En la sintaxis del URL, que parte viene despues de la ruta?

A. El fragmento
B. El puerto
C. El esquema
D. La cadena de consulta

Sintaxis URL

En la sintaxis del URL, que parte viene despues de la ruta?

A. El fragmento
B. El puerto
C. El esquema
D. La cadena de consulta

ANSWER: D

Versión TLS

Cuál es la versión de TLS segura en uso hoy día (2025)?

A. 1.3
B. 1.6
C. 3.0
D. 3.2

Versión TLS

Cuál es la versión de TLS segura en uso hoy día (2025)?

A. 1.3
B. 1.6
C. 3.0
D. 3.2

ANSWER: A

Método HTTP

Cuál de los siguientes NO es un método estandar HTTP?

A. HEAD
B. PUT
C. SEND
D. TRACE

Método HTTP

Cuál de los siguientes NO es un método estandar HTTP?

A. HEAD
B. PUT
C. SEND
D. TRACE

ANSWER: C

cURL

En el comando cURL, cuál es la verión larga del flag «-i»?

A. «–ignore»
B. «–insecure»
C. «–ipv4»
D. «–include»

cURL

En el comando cURL, cuál es la verión larga del flag «-i»?

A. «–ignore»
B. «–insecure»
C. «–ipv4»
D. «–include»

ANSWER: D

Subfinder -d

Qué significa la opción «-d» de subfinder?

A. debug
B. domain
C. detach
D. direct

Subfinder -d

Qué significa la opción «-d» de subfinder?

A. debug
B. domain
C. detach
D. direct

ANSWER: B

Subfinder UChile

Cuántos subdominios encuentra subfinder para el dominio que pertenece a la Universidad de Chile (más o menos 200)?

A. 817
B. 1180
C. 2247
D. 2819

Subfinder UChile

Cuántos subdominios encuentra subfinder para el dominio que pertenece a la Universidad de Chile (más o menos 200)?

A. 817
B. 1180
C. 2247
D. 2819

ANSWER: C

Subfinder fuentes

Cuál de las siguientes es una fuente ABIERTA (i.e. gratis) de subfinder?

A. ctrsh
B. c99
C. shodan
D. whoisxmlapi

Subfinder fuentes

Cuál de las siguientes es una fuente ABIERTA (i.e. gratis) de subfinder?

A. ctrsh
B. c99
C. shodan
D. whoisxmlapi

ANSWER: A

Cronología de un Pentest web

Cuál es el orden cronológico posible de un Pentest desde el alto nivel al bajo nivel. Por lo menos el presentado en clase)?

A. burpsuite, nmap, ffuf, subfinder
B. ffuf, subfinder, burpsuite, nmap
C. subfinder, burpsuite, ffuf, nmap
D. subfinder, nmap, ffuf, burpsuite

Cronología de un Pentest web

Cuál es el orden cronológico posible de un Pentest desde el alto nivel al bajo nivel. Por lo menos el presentado en clase)?

A. burpsuite, nmap, ffuf, subfinder
B. ffuf, subfinder, burpsuite, nmap
C. subfinder, burpsuite, ffuf, nmap
D. subfinder, nmap, ffuf, burpsuite

ANSWER: D

Nmap velocidad

De los siguientes comandos de nmap, cual retorna más rápido?

A. sudo nmap -oA output ctf.tinmarino.com

B. sudo nmap -A -n ctf.tinmarino.com -p-

C. sudo nmap -sS -T5 -n -Pn ctf.tinmarino.com -p 9141

D. sudo nmap -sU -T1 -vvv –packet-trace –top-ports=10 ctf.tinmarino.com

Nmap velocidad

De los siguientes comandos de nmap, cual retorna más rápido?

A. sudo nmap -oA output ctf.tinmarino.com

B. sudo nmap -A -n ctf.tinmarino.com -p-

C. sudo nmap -sS -T5 -n -Pn ctf.tinmarino.com -p 9141

D. sudo nmap -sU -T1 -vvv –packet-trace –top-ports=10 ctf.tinmarino.com

ANSWER: C

Nmap *flag*

Cuál de los siguientes *flag* de Nmap NO se relaciona con la salida, es decir el formato del mensaje que reporta Nmap en la salida estandar?

A. -vvv
B. –packet-trace
C. -d
D. -n

Nmap *flag*

Cuál de los siguientes *flag* de Nmap NO se relaciona con la salida, es decir el formato del mensaje que reporta Nmap en la salida estandar?

A. -vvv
B. –packet-trace
C. -d
D. -n

ANSWER: D

Equipo virtual

En el contexto de la red, un equipo virtual?

A. Es un equipo, todo es virtual en la red
B. Es una direción de red dominio y puerto en la cabecera VHOST
C. Es un equipo que sirve de proxy transparente
D. Es un sistem operativo que está en una máquina virtual

Equipo virtual

En el contexto de la red, un equipo virtual?

A. Es un equipo, todo es virtual en la red
B. Es una direción de red dominio y puerto en la cabecera VHOST
C. Es un equipo que sirve de proxy transparente
D. Es un sistem operativo que está en una máquina virtual

ANSWER: B

Cabecera JSON

De las siguientes cuál es una cabecera correcta para enviar datos JSON en el cuerpo de una solicitud POST?

A. Content-Type: application/json; charset=utf-8
B. Content: JSON
C. Content: application/json
D. Content.Type: JSON

Cabecera JSON

De las siguientes cuál es una cabecera correcta para enviar datos JSON en el cuerpo de una solicitud POST?

A. Content-Type: application/json; charset=utf-8
B. Content: JSON
C. Content: application/json
D. Content.Type: JSON

ANSWER: A

Printf

Qué hace el siguiente comando: «`printf "%%%X\n" {0..255}`»?

A. Imprime «X» 256 veces uno por nueva linea

B. Imprime numeros decimales 1, 2, 3, ..., 255 separados por nueva linea

C. Imprime numeros numeros hexadecimal precedidos por el caracter «%»: %01, %02 ... %FF separados por nueva linea

D. Tiene un error de sintaxis

Printf

Qué hace el siguiente comando: «`printf "%%%X\n" {0..255}`»?

A. Imprime «X» 256 veces uno por nueva linea

B. Imprime numeros decimales 1, 2, 3, ..., 255 separados por nueva linea

C. Imprime numeros numeros hexadecimal precedidos por el caracter «%»: %01, %02 ... %FF separados por nueva linea

D. Tiene un error de sintaxis

ANSWER: C

Proxy

Qué palabra es sinónimo de «proxy»?

A. Agente
B. Servidor
C. Intermediario
D. Cliente

Proxy

Qué palabra es sinónimo de «proxy»?

A. Agente
B. Servidor
C. Intermediario
D. Cliente

ANSWER: C

Burp Suite pugin

Qué plugin de Burp Suite permite cambiar de IP mediante la API Gateway de AWS?

A. IP Changer
B. IP Switcher
C. Proxy Chain
D. IP Rotate

Burp Suite pugin

Qué plugin de Burp Suite permite cambiar de IP mediante la API Gateway de AWS?

A. IP Changer
B. IP Switcher
C. Proxy Chain
D. IP Rotate

ANSWER: D

Autenticación

Que hace la autenticación?

A. Verificar la identidad de un usuario

B. Dar acceso a un recurso

C. Establecer los privilegios de un usuario

D. Bloquear un IP después de una cierta cantidad de solicitudes

Autenticación

Que hace la autenticación?

A. Verificar la identidad de un usuario

B. Dar acceso a un recurso

C. Establecer los privilegios de un usuario

D. Bloquear un IP después de una cierta cantidad de solicitudes

ANSWER: A

2FA

En qué categoría de autenticación entra el 2FA?

A. Conocimiento

B. Posesión

C. Inherencia

D. Protección

2FA

En qué categoría de autenticación entra el 2FA?

A. Conocimiento

B. Posesión

C. Inherencia

D. Protección

ANSWER: B

Cookie

La cookie es un mecanismo de control por

A. Firma
B. Intermediario
C. Básica
D. Sesión

Cookie

La cookie es un mecanismo de control por

A. Firma
B. Intermediario
C. Básica
D. Sesión

ANSWER: D

Pilares de la criptografía

De las siguientes, cuál NO es un pilar de la criptografía?

A. Integridad
B. Autenticidad
C. Rendimiento
D. Disponibilidad

Pilares de la criptografía

De las siguientes, cuál NO es un pilar de la criptografía?

A. Integridad
B. Autenticidad
C. Rendimiento
D. Disponibilidad

ANSWER: C

Cifrado de César

Cuál es el texto claro según el cifrado de César de este mensaje encriptado «qirweni»?

A. mensaje
B. secreto
C. cifrado
D. debil

Cifrado de César

Cuál es el texto claro según el cifrado de César de este mensaje encriptado «qirweni»?

A. mensaje
B. secreto
C. cifrado
D. debil

ANSWER: A

Cifrado de libreta única

Con un cifrado de libreta única, la clave es «`\xCF\x40\x9B\x31`», el cifrado es «`\xad\x2c\xf4\x53`» (notación Python). Cuál es el texto claro?

A. fuzz
B. nice
C. four
D. blob

Cifrado de libreta única

Con un cifrado de libreta única, la clave es «`\xCF\x40\x9B\x31`», el cifrado es «`\xad\x2c\xf4\x53`» (notación Python). Cuál es el texto claro?

A. fuzz
B. nice
C. four
D. blob

ANSWER: D

Cifrado ECB

Porque el modo de cifrado por bloque ECB es considerado inseguro?

A. Porque utiliza clave cortas, mejor utilizar ÆS

B. Porque es vulnerable a intercepciones, mejor utilizar TLS

C. Porque es vulnerable a análisis de frecuencia, mejor utilizar CBC

D. Porque tiene un sesgo en la matriz de premutación, mejor utilizar OpenSSL

Cifrado ECB

Porque el modo de cifrado por bloque ECB es considerado inseguro?

A. Porque utiliza clave cortas, mejor utilizar ÆS

B. Porque es vulnerable a intercepciones, mejor utilizar TLS

C. Porque es vulnerable a análisis de frecuencia, mejor utilizar CBC

D. Porque tiene un sesgo en la matriz de premutación, mejor utilizar OpenSSL

ANSWER: C

Cifrado por bloque

Que esquema de cifrado por bloque es más seguro?

A. DES
B. ÆS
C. 3DES
D. RC2

Cifrado por bloque

Que esquema de cifrado por bloque es más seguro?

A. DES
B. ÆS
C. 3DES
D. RC2

ANSWER: B

Criptografía asimetrica

Cuál es el uso fundamental de la criptografía asimetrica?

A. Generar claves
B. Derivar claves
C. Enviar claves
D. Almacenar claves

Criptografía asimetrica

Cuál es el uso fundamental de la criptografía asimetrica?

A. Generar claves
B. Derivar claves
C. Enviar claves
D. Almacenar claves

ANSWER: C

Generación de aleatorio

Removiendo «cat /dev/random», de los siguientes, qué comando genera el random el más seguro?

A. echo $RANDOM
B. cat /dev/urandom
C. random
D. openssl rand 1000000000

Generación de aleatorio

Removiendo «cat /dev/random», de los siguientes, qué comando genera el random el más seguro?

A. echo $RANDOM
B. cat /dev/urandom
C. random
D. openssl rand 1000000000

ANSWER: D

CAPTCHA

De que sirven los CAPTCHA?

A. Dificultar los ataques automatizados
B. Optimizar la cantidad de tráfico web
C. Asegurar la correcta autenticación
D. Evitar el ClickJacking

CAPTCHA

De que sirven los CAPTCHA?

A. Dificultar los ataques automatizados
B. Optimizar la cantidad de tráfico web
C. Asegurar la correcta autenticación
D. Evitar el ClickJacking

ANSWER: A

Cabecera de cookie

El navegador envváa un cookie sistemáticamente para las solicitudes en un cierto dominio después de recibir la cabecera ...

A. Access-Control-Allow-Origin-Cookie
B. Set-Cookie
C. Cookie
D. Server-Cookie

Cabecera de cookie

El navegador enváa un cookie sistemáticamente para las solicitudes en un cierto dominio después de recibir la cabecera ...

A. Access-Control-Allow-Origin-Cookie
B. Set-Cookie
C. Cookie
D. Server-Cookie

ANSWER: B

JWT

Cuál de los siguientes es un JWT?

A. eyJzdWIiOiAiM-
TIzNDU2Nzg5MCIsIm5hbWUiOiAidG90byIsCiAgImdyb3VwIjoiYWRtaW4iLAogICJleHAiC
B. eyJhbGciOiJI-
UzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6InRvdG8iLCJncm9
C. eyAiYWxnIjoglkhT-
MjU2IiwgInR5cCI6IC.JKV1QiICJzdWIiOiAiMTIzNDU2Nzg5MCIsICJuYW1lIjogInRvdG8iLCAiZ
D. eyJhbGciOiJI-
UzI1NiIsInR5cCI6IkpXVCJ9.JKV1QiICJzdWIiOiAiMTIzNDU2Nzg5MCIsICJuYW1lIjogInRvdG8

JWT

Cuál de los siguientes es un JWT?

A. eyJzdWIiOiAiM-
TIzNDU2Nzg5MCIsIm5hbWUiOiAidG90byIsCiAgImdyb3VwIjoiYWRtaW4iLAogICJleHAiC
B. eyJhbGciOiJI-
UzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6InRvdG8iLCJncm9
C. eyAiYWxnIjoglkhT-
MjU2IiwgInR5cCI6IC.JKV1QiICJzdWIiOiAiMTIzNDU2Nzg5MCIsICJuYW1lIjogInRvdG8iLCAiZ
D. eyJhbGciOiJI-
UzI1NiIsInR5cCI6IkpXVCJ9.JKV1QiICJzdWIiOiAiMTIzNDU2Nzg5MCIsICJuYW1lIjogInRvdG8

ANSWER: B

IDOR

De los siguientes comandos cURL exitosos, qué endpoint es potencialmente vulnerable a un IDOR?

A. curl https://www.uc.cl/user?id?9832
B. curl -X POST -H “Content-Type: application/json” -d ‘{ “rut”: 19 }’ https://www.uc.cl/getcertificate
C. curl https://www.uc.cl/user/tinmarino
D. todos los anteriores

IDOR

De los siguientes comandos cURL exitosos, qué endpoint es potencialmente vulnerable a un IDOR?

A. curl https://www.uc.cl/user?id?9832
B. curl -X POST -H “Content-Type: application/json” -d ‘{ “rut”: 19 }’ https://www.uc.cl/getcertificate
C. curl https://www.uc.cl/user/tinmarino
D. todos los anteriores

ANSWER: D

CVSS divulgación

Cuál es la escala CVSS de una divulgación masiva de información PII (es decir confidencialidad alta) no autenticada? (todo lo demás siendo por defecto, la métrica subsecuente siendo nula)

A. 6.4
B. 7.1
C. 8.7
D. 9.2

CVSS divulgación

Cuál es la escala CVSS de una divulgación masiva de información PII (es decir confidencialidad alta) no autenticada? (todo lo demás siendo por defecto, la métrica subsecuente siendo nula)

A. 6.4
B. 7.1
C. 8.7
D. 9.2

ANSWER: C

CVSS RCE

Cuál es la escala CVSS de una ejecución remota de código autenticada como usuario (no admin)? (todo lo demás siendo al máximo, la métrica subsecuente siendo máxima)?

A. 9.1
B. 9.4
C. 9.7
D. 10

CVSS RCE

Cuál es la escala CVSS de una ejecución remota de código autenticada como usuario (no admin)? (todo lo demás siendo al máximo, la métrica subsecuente siendo máxima)?

A. 9.1
B. 9.4
C. 9.7
D. 10

ANSWER: B

CVSS DOS

Cuál es la escala CVSS de una denegación de servicio total no autenticada? (todo lo demás siendo por defecto, la métrica subsecuente siendo nula)

A. 6.4
B. 7.1
C. 8.7
D. 9.2

CVSS DOS

Cuál es la escala CVSS de una denegación de servicio total no autenticada? (todo lo demás siendo por defecto, la métrica subsecuente siendo nula)

A. 6.4
B. 7.1
C. 8.7
D. 9.2

ANSWER: C

Vulnerabilidad cliente

Qué vulnerabilidad afecta el cliente (y no el servidor)?

A. SSRF
B. CSRF
C. LFI
D. RFI

Vulnerabilidad cliente

Qué vulnerabilidad afecta el cliente (y no el servidor)?

A. SSRF

B. CSRF

C. LFI

D. RFI

ANSWER: B

Vulnerabilidad servidor

Qué vulnerabilidad afecta el servidor (y no el cliente)?

A. XSS
B. DOM-based injection
C. ClickJacking
D. Path traversal

Vulnerabilidad servidor

Qué vulnerabilidad afecta el servidor (y no el cliente)?

A. XSS
B. DOM-based injection
C. ClickJacking
D. Path traversal

ANSWER: D

CVSS limitación

Qué NO considera la escala CVSS?

A. El impacto para el negocio
B. El vector de ataque
C. El impacto sobre la disponibilidad
D. Los privilegios requeridos para la explotación

CVSS limitación

Qué NO considera la escala CVSS?

A. El impacto para el negocio
B. El vector de ataque
C. El impacto sobre la disponibilidad
D. Los privilegios requeridos para la explotación

ANSWER: A

Concurrencia en Python

De los siguientes módulos Python, cuál NO tiene que ver con la concurrencia?

A. aiohttp
B. requests
C. concurrent
D. asyncio

Concurrencia en Python

De los siguientes módulos Python, cuál NO tiene que ver con la concurrencia?

A. aiohttp
B. requests
C. concurrent
D. asyncio

ANSWER: B

Concurrencia en español

De las siguientes palabras, cuál NO tiene que ver con la concurrencia?

A. Sesión
B. Multitarea
C. Paralelismo
D. Asincronismo

Concurrencia en español

De las siguientes palabras, cuál NO tiene que ver con la concurrencia?

A. Sesión
B. Multitarea
C. Paralelismo
D. Asincronismo

ANSWER: A

Git Dumper

De qué sirve la herramienta Git Dumper?

A. Para hacer respaldo de su repositorio Git
B. Para limpiar la cache de su repositorio Git
C. Para divulgar el contenido de una carpeta .Git presente en un servicio web
D. Para buscar información en fuentes pública (OSINT)

Git Dumper

De qué sirve la herramienta Git Dumper?

A. Para hacer respaldo de su repositorio Git
B. Para limpiar la cache de su repositorio Git
C. Para divulgar el contenido de una carpeta .Git presente en un servicio web
D. Para buscar información en fuentes pública (OSINT)

ANSWER: C

Regex RUT

De las siguientes regex, cuál permite buscar un RUT?

A. `[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}`

B. `AIza[0-9A-Za-z-_]{35}`

C. `ey[A-Za-z0-9-_=]+\.[A-Za-z0-9-_=]+\.?[A-Za-z0-9-_.+/=]*$`

D. `(\d{1,3}(?:\.\d{1,3}){2}-[\dkK])`

Regex RUT

De las siguientes regex, cuál permite buscar un RUT?

A. `[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}`

B. `AIza[0-9A-Za-z-_]{35}`

C. `ey[A-Za-z0-9-_=]+\.[A-Za-z0-9-_=]+\.?[A-Za-z0-9-_.+/=]*$`

D. `(\d{1,3}(?:\.\d{1,3}){2}-[\dkK])`

ANSWER: D

XSS tipos

De qué tipo oficial puede ser un XSS?

A. Remoto
B. Profundo
C. Cruzado
D. Almacenado

XSS tipos

De qué tipo oficial puede ser un XSS?

A. Remoto
B. Profundo
C. Cruzado
D. Almacenado

ANSWER: D

XSS impacto

Cuál es el impacto directo de un XSS?

A. Ejecución de código JS
B. Ejecución de código PHP
C. Intercepción de solicitudes
D. Brute Forcing de claves

XSS impacto

Cuál es el impacto directo de un XSS?

A. Ejecución de código JS
B. Ejecución de código PHP
C. Intercepción de solicitudes
D. Brute Forcing de claves

ANSWER: A

Recorrido de ruta

Cuál de los siguientes URLs es un intento de recorrido de ruta?

A. http://uc.cl/user/getinfo?id=5432

B. http://uc.cl/..%2f..%2f..%2fetc%2fpasswd

C. http://uc.cl/?cmd=ping

D. http://uc.cl/%0a'+or1=1+--+

Recorrido de ruta

Cuál de los siguientes URLs es un intento de recorrido de ruta?

A. http://uc.cl/user/getinfo?id=5432

B. http://uc.cl/..%2f..%2f..%2fetc%2fpasswd

C. http://uc.cl/?cmd=ping

D. http://uc.cl/%0a'+or1=1+--+

ANSWER: B

Carga de archivos inseguros

Los métodos HTTP de explotación de la vulnerabilidad canónica de carga de archivos inseguros vistos en clase, en orden cronologico son:

A. HEAD, GET
B. GET, POST
C. POST, GET
D. GET, GET

Carga de archivos inseguros

Los métodos HTTP de explotación de la vulnerabilidad canónica de carga de archivos inseguros vistos en clase, en orden cronologico son:

A. HEAD, GET
B. GET, POST
C. POST, GET
D. GET, GET

ANSWER: C

Local File Inclusion

Cuál de los siguientes acrónimos es de una vulnerabilidad muy similar al Local File Inclusion?

A. RFI
B. DDOS
C. RCE
D. SQLI

Local File Inclusion

Cuál de los siguientes acrónimos es de una vulnerabilidad muy similar al Local File Inclusion?

A. RFI
B. DDOS
C. RCE
D. SQLI

ANSWER: A

Nombre lógica de negocio

Cuál es otro nombre de las vulnerabilidiades de lógica de negocio?

A. vulnerabilidades de lógica de aplicación
B. pérdida de control de acceso
C. condiciones de carrera
D. funcionalidades secretas

Nombre lógica de negocio

Cuál es otro nombre de las vulnerabilidiades de lógica de negocio?

A. vulnerabilidades de lógica de aplicación
B. pérdida de control de acceso
C. condiciones de carrera
D. funcionalidades secretas

ANSWER: A

Factores de errores

Qué factor incrementa la probabilidad de tener errores lógicos?

A. Sistema más simple
B. Pentesters dentro del equipo de desarollo
C. Diversidad de los lenguajes
D. Sistema más complejo

Factores de errores

Qué factor incrementa la probabilidad de tener errores lógicos?

A. Sistema más simple
B. Pentesters dentro del equipo de desarollo
C. Diversidad de los lenguajes
D. Sistema más complejo

ANSWER: D

Asunción arriesgada

Cuál es la asunción más arriesgada que pueden hacer los desarrolladores?

A. Que nadie lo va a ver
B. Que todos los usuarios son legitimos
C. Que los colegas hacen un buen trabajo
D. Que el código es privado

Asunción arriesgada

Cuál es la asunción más arriesgada que pueden hacer los desarrolladores?

A. Que nadie lo va a ver
B. Que todos los usuarios son legitimos
C. Que los colegas hacen un buen trabajo
D. Que el código es privado

ANSWER: B

Exceso de confianza

Cuál de las siguientes podría ser una vulnerabilidad de lógica debido a un exceso de confianza en los usuarios?

A. Múltiples dispositivos 2FA
B. Verificación adicional del certificado SSL en JavaScript
C. Parámetro de negocio accesible al usuario
D. Autenticación con multiples desafios respuestas para detectar los proxies

Exceso de confianza

Cuál de las siguientes podría ser una vulnerabilidad de lógica debido a un exceso de confianza en los usuarios?

A. Múltiples dispositivos 2FA
B. Verificación adicional del certificado SSL en JavaScript
C. Parámetro de negocio accesible al usuario
D. Autenticación con multiples desafios respuestas para detectar los proxies

ANSWER: C

Listas de denegaciones

Cuál es el principal defecto de las listas de denegaciones?

A. Pueden ser incompletas
B. Pueden verse como mala onda
C. Pueden generar denegación de servicio por rebotes
D. Pueden divulgar la lógica del negocio

Listas de denegaciones

Cuál es el principal defecto de las listas de denegaciones?

A. Pueden ser incompletas
B. Pueden verse como mala onda
C. Pueden generar denegación de servicio por rebotes
D. Pueden divulgar la lógica del negocio

ANSWER: A

Validación de número

Para validar un número de entrada, qué solución es la menos insegura?

A. Verificar que se puede adicionar con cero y que es igual a sí mismo
B. Verificar que es del tipo entero, superior a cero e inferior a doce
C. Verificar que es de tipo numérico y superior a cero
D. Verificar que no es 666, para evitar problemas con saben quién

Validación de número

Para validar un número de entrada, qué solución es la menos insegura?

A. Verificar que se puede adicionar con cero y que es igual a sí mismo
B. Verificar que es del tipo entero, superior a cero e inferior a doce
C. Verificar que es de tipo numérico y superior a cero
D. Verificar que no es 666, para evitar problemas con saben quién

ANSWER: B

Falsa sensación

Si bien las siguientes dificultan el trabajo del atacante mediante la defensa en profundidad, podrían dar una falsa sensación de seguridad, excepto una. Cuál?

A. Un WAF (Web Application Firewall)
B. Una lista de denegación de parámetros
C. Un ciclo de desarrollo seguro
D. Un 2FA (Second Factor of Authentication)

Falsa sensación

Si bien las siguientes dificultan el trabajo del atacante mediante la defensa en profundidad, podrían dar una falsa sensación de seguridad, excepto una. Cuál?

A. Un WAF (Web Application Firewall)
B. Una lista de denegación de parámetros
C. Un ciclo de desarrollo seguro
D. Un 2FA (Second Factor of Authentication)

ANSWER: C

Flujo de negocio

Cuál es lo recomendado en clase como primer paso para encontrar vulnerabilidades en el flujo de la lógica de la aplicación?

A. Mezclar flujos
B. Saltar etapas
C. Buscar condiciones de carrera
D. Recorrer etapas del flujo legitimamente

Flujo de negocio

Cuál es lo recomendado en clase como primer paso para encontrar vulnerabilidades en el flujo de la lógica de la aplicación?

A. Mezclar flujos
B. Saltar etapas
C. Buscar condiciones de carrera
D. Recorrer etapas del flujo legitimamente

ANSWER: D

Condiciones de carrera

A qué se deben las condiciones de carrera?

A. A la falta de sincronización en el acceso a recursos compartidos
B. A la validación insuficiente de entradas de usuario
C. A errores en la lógica de negocio de la aplicación
D. A la implementación de medidas de seguridad inadecuadas

Condiciones de carrera

A qué se deben las condiciones de carrera?

A. A la falta de sincronización en el acceso a recursos compartidos
B. A la validación insuficiente de entradas de usuario
C. A errores en la lógica de negocio de la aplicación
D. A la implementación de medidas de seguridad inadecuadas

ANSWER: A

Mensajes de errores

Cuál de las siguientes afirmaciones describe mejor los mensajes de error en relación con las vulnerabilidades de lógica de negocio?

A. Los mensajes de error siempre deben ser genéricos para evitar revelar información sensible
B. Los mensajes de error deben ser lo suficientemente explícitos para que el usuario pueda entender el flujo legítimo
C. Los mensajes de error no tienen impacto en la seguridad de la aplicación
D. La validación de entradas es suficiente para prevenir vulnerabilidades de lógica de negocio

Mensajes de errores

Cuál de las siguientes afirmaciones describe mejor los mensajes de error en relación con las vulnerabilidades de lógica de negocio?

A. Los mensajes de error siempre deben ser genéricos para evitar revelar información sensible
B. Los mensajes de error deben ser lo suficientemente explícitos para que el usuario pueda entender el flujo legítimo
C. Los mensajes de error no tienen impacto en la seguridad de la aplicación
D. La validación de entradas es suficiente para prevenir vulnerabilidades de lógica de negocio

ANSWER: A

Redondeo

Por qué el redondeo puede ser considerado un error lógico?

A. Porque podría generar condiciones de carrera.

B. Porque genera una diferencia entre el número de la asunción lógica y el almacenado.

C. Porque convierte el tipo y podría llevar a un comportamiento indefinido.

D. Porque complejiza los cálculos matemáticos.

Redondeo

Por qué el redondeo puede ser considerado un error lógico?

A. Porque podría generar condiciones de carrera.

B. Porque genera una diferencia entre el número de la asunción lógica y el almacenado.

C. Porque convierte el tipo y podría llevar a un comportamiento indefinido.

D. Porque complejiza los cálculos matemáticos.

ANSWER: B

Redondeo con sesgo

En caso de deber redondear, porque a veces se debe, ¿cuál de las siguientes funciones de Python generará un sesgo hacia abajo para los números positivos y podría asegurar a una parte no perder dinero?

A. int(42.5)
B. round(42.5)
C. math.floor(value + 0.5)
D. math.modf(42.5)

Redondeo con sesgo

En caso de deber redondear, porque a veces se debe, ¿cuál de las siguientes funciones de Python generará un sesgo hacia abajo para los números positivos y podría asegurar a una parte no perder dinero?

A. int(42.5)
B. round(42.5)
C. math.floor(value + 0.5)
D. math.modf(42.5)

ANSWER: A

Definición del infinito

Cuál es una definición correcta del infinito?

A. El número que dividido por cero es un número finito.

B. El número que al agregarle uno es igual a sí mismo.

C. El número inverso de cero en el dominio de los enteros.

D. El número que al restarle a sí mismo es igual a NaN.

Definición del infinito

Cuál es una definición correcta del infinito?

A. El número que dividido por cero es un número finito.
B. El número que al agregarle uno es igual a sí mismo.
C. El número inverso de cero en el dominio de los enteros.
D. El número que al restarle a sí mismo es igual a NaN.

ANSWER: B

Cambio de divisas 1

La tasa de cambio internacional es de 969 pesos por 1 dólar. Un cliente vende 10 pesos por 0.01 dólares (mientras que debería recibir 0.00969 dólares). Quién ganó dinero?

A. El cliente
B. El banco
C. Ningunó
D. Ambos

Cambio de divisas 1

La tasa de cambio internacional es de 969 pesos por 1 dólar. Un cliente vende 10 pesos por 0.01 dólares (mientras que debería recibir 0.00969 dólares). Quién ganó dinero?

A. El cliente
B. El banco
C. Ningunó
D. Ambos

ANSWER: B

Cambio de divisas 2

La tasa de cambio internacional es de 969 pesos por 1 dólar. Un cliente vende 7 pesos por 0.01 dólares. ¿Cuánto debería recibir lógicamente en caso de que existieran fracciones de centavos de dólares?

A. 0.0072... (= 7 / 969)
B. 0.0969 (= 0.01 * 969 / 100)
C. 0.0135 (= (0.01 * 969 - 7) / 100 / 2)
D. 0.01 (= int(7 / 969))

Cambio de divisas 2

La tasa de cambio internacional es de 969 pesos por 1 dólar. Un cliente vende 7 pesos por 0.01 dólares. ¿Cuánto debería recibir lógicamente en caso de que existieran fracciones de centavos de dólares?

A. 0.0072... (= 7 / 969)
B. 0.0969 (= 0.01 * 969 / 100)
C. 0.0135 (= (0.01 * 969 - 7) / 100 / 2)
D. 0.01 (= int(7 / 969))

ANSWER: A

Cambio de divisas 3

La tasa de cambio internacional es de 969 pesos por 1 dólar. Un cliente vende 7 pesos por 0.01 dólares. Quíen ganó dinero?

A. El cliente
B. El banco
C. Estados unidos
D. Chile

Cambio de divisas 3

La tasa de cambio internacional es de 969 pesos por 1 dólar. Un cliente vende 7 pesos por 0.01 dólares. Quíen ganó dinero?

A. El cliente
B. El banco
C. Estados unidos
D. Chile

ANSWER: A

Errores de redondeo pervasivas

Por qué los errores de redondeo son pervasivos en el sector financiero? (Nota que ChatGPT se equivoca majestuosamente).

A. Porque generan pérdidas infinitesimales, entonces menospreciables.
B. Porque el redondeo es un proceso complejo.
C. Porque nuestros antepasados informáticos aseguraron un redondeo hacia arriba por defecto.
D. Porque estadísticamente, no generan ninguna pérdida, según la ley de los grandes números; al hacer infinitas transferencias, el balance sería nulo.

Errores de redondeo pervasivas

Por qué los errores de redondeo son pervasivos en el sector financiero? (Nota que ChatGPT se equivoca majestuosamente).

A. Porque generan pérdidas infinitesimales, entonces menospreciables.
B. Porque el redondeo es un proceso complejo.
C. Porque nuestros antepasados informáticos aseguraron un redondeo hacia arriba por defecto.
D. Porque estadísticamente, no generan ninguna pérdida, según la ley de los grandes números; al hacer infinitas transferencias, el balance sería nulo.

ANSWER: B

Igualdad de flotantes

¿Cuál de las siguientes implementaciones es correcta para verificar la igualdad de 0.1 + 0.2 - 0.3?

A. `result = 0.1 + 0.2 - 0.3; is_equal = result == 0`

B. `result = 0.1 + 0.2 - 0.3; is_equal = abs(result) < 1`

C. `result = 0.1 + 0.2 - 0.3; is_equal = result == 0.0`

D. `result = 0.1 + 0.2 - 0.3; is_equal = abs(result) < 1e-10`

Igualdad de flotantes

¿Cuál de las siguientes implementaciones es correcta para verificar la igualdad de 0.1 + 0.2 - 0.3?

A. `result = 0.1 + 0.2 - 0.3; is_equal = result == 0`

B. `result = 0.1 + 0.2 - 0.3; is_equal = abs(result) < 1`

C. `result = 0.1 + 0.2 - 0.3; is_equal = result == 0.0`

D. `result = 0.1 + 0.2 - 0.3; is_equal = abs(result) < 1e-10`

ANSWER: D

Representación binaria 1

Cuánto vale en decimal el número binario 11000110?

A. 70 = (0 * 128) + (1 * 64) + (0 * 32) + (0 * 16) + (0 * 8) + (1 * 4) + (1 * 2) + (0 * 1)

B. 128 = (1 * 128) + (0 * 64) + (0 * 32) + (0 * 16) + (0 * 8) + (0 * 4) + (0 * 2) + (0 * 1)

C. 198 = (1 * 128) + (1 * 64) + (0 * 32) + (0 * 16) + (0 * 8) + (1 * 4) + (1 * 2) + (0 * 1)

D. 204 = (1 * 128) + (1 * 64) + (0 * 32) + (0 * 16) + (1 * 8) + (1 * 4) + (0 * 2) + (0 * 1)

Representación binaria 1

Cuánto vale en decimal el número binario 11000110?

A. 70 = (0 * 128) + (1 * 64) + (0 * 32) + (0 * 16) + (0 * 8) + (1 * 4) + (1 * 2) + (0 * 1)
B. 128 = (1 * 128) + (0 * 64) + (0 * 32) + (0 * 16) + (0 * 8) + (0 * 4) + (0 * 2) + (0 * 1)
C. 198 = (1 * 128) + (1 * 64) + (0 * 32) + (0 * 16) + (0 * 8) + (1 * 4) + (1 * 2) + (0 * 1)
D. 204 = (1 * 128) + (1 * 64) + (0 * 32) + (0 * 16) + (1 * 8) + (1 * 4) + (0 * 2) + (0 * 1)

ANSWER: C

Repesentación binaria 2

Cuánto vale en decimal el número binario 0.0101? (nota el punto, es un binario fracional).

A. 0.0625 = (0 * 1/2) + (0 * 1/4) + (0 * 1/8) + (1* 1/16)
B. 0.3125 = (0 * 1/2) + (1 * 1/4) + (0 * 1/8) + (1* 1/16)
C. 0.7500 = (1 * 1/2) + (1 * 1/4) + (0 * 1/8) + (0* 1/16)
D. 0.9375 = (1 * 1/2) + (1 * 1/4) + (1 * 1/8) + (1* 1/16)

Repesentación binaria 2

Cuánto vale en decimal el número binario 0.0101? (nota el punto, es un binario fracional).

A. 0.0625 = (0 * 1/2) + (0 * 1/4) + (0 * 1/8) + (1* 1/16)
B. 0.3125 = (0 * 1/2) + (1 * 1/4) + (0 * 1/8) + (1* 1/16)
C. 0.7500 = (1 * 1/2) + (1 * 1/4) + (0 * 1/8) + (0* 1/16)
D. 0.9375 = (1 * 1/2) + (1 * 1/4) + (1 * 1/8) + (1* 1/16)

ANSWER: B

Flotante máximo

En Python 64 bits, el flotante máximo es 1.8e308. Cuál es el resultado de la siguiente ecuación: 2e308 - 1e308 - 1e308? (Nota: en caso de duda, ejecuta). (Nota 2: en caso de más duda, lee la clase). (Nota 3: en última instancia, piensa).

A. 0
B. nan
C. inf
D. -inf

Flotante máximo

En Python 64 bits, el flotante máximo es 1.8e308. Cuál es el resultado de la siguiente ecuación: 2e308 - 1e308 - 1e308? (Nota: en caso de duda, ejecuta). (Nota 2: en caso de más duda, lee la clase). (Nota 3: en última instancia, piensa).

A. 0
B. nan
C. inf
D. -inf

ANSWER: C

Inyeción SQL

Cuál de las siguiente es un parámetro de intento de inyeción SQL?

A. 42

B. 42|18

C. admin' or 1=1 –

D. admin"%20&echo toto

Inyeción SQL

Cuál de las siguiente es un parámetro de intento de inyeción SQL?

A. 42

B. 42|18

C. admin' or 1=1 –

D. admin"%20&echo toto

ANSWER: C

SQL concatenar resultados

Cuál de los siguientes comandos SQL permite concatenar los resultados de dos consultas?

A. DELETE
B. INSERT
C. NOT
D. UNION ALL

SQL concatenar resultados

Cuál de los siguientes comandos SQL permite concatenar los resultados de dos consultas?

A. DELETE
B. INSERT
C. NOT
D. UNION ALL

ANSWER: D

SQL JOIN

Cuál de los siguientes JOIN permite obtener todos los registros de ambas tablas, sin omitir ninguno?

A. INNER JOIN
B. FULL JOIN
C. LEFT JOIN
D. RIGHT JOIN

SQL JOIN

Cuál de los siguientes JOIN permite obtener todos los registros de ambas tablas, sin omitir ninguno?

A. INNER JOIN
B. FULL JOIN
C. LEFT JOIN
D. RIGHT JOIN

ANSWER: B

MySQL finalidad

Qué tabla siempre existe en una base de datos MySQL?

A. INFORMATION_SCHEMA
B. USERS
C. TABLES
D. DATABASES

MySQL finalidad

Qué tabla siempre existe en una base de datos MySQL?

A. INFORMATION_SCHEMA
B. USERS
C. TABLES
D. DATABASES

ANSWER: A

SQL NOP

Cuál de los siguientes es un comando que siempre se ejecuta sin realizar ninguna operación, similar al NOP (No Operation)?

A. 1=1
B. SELECT 1; -
C. INSERT 0 INTO NULL;
D. DELETE NULL;

SQL NOP

Cuál de los siguientes es un comando que siempre se ejecuta sin realizar ninguna operación, similar al NOP (No Operation)?

A. 1=1
B. SELECT 1; -
C. INSERT 0 INTO NULL;
D. DELETE NULL;

ANSWER: B

SQLMap -u -p

Qué significa el -u y el -p de SQLMap, respectivamente?

A. URL y PID
B. Unsafe y Parámetro
C. URL y Parámetro
D. Unsafe y PID

SQLMap -u -p

Qué significa el -u y el -p de SQLMap, respectivamente?

A. URL y PID
B. Unsafe y Parámetro
C. URL y Parámetro
D. Unsafe y PID

ANSWER: C

Ordenal

Cuál es el valor ordinal del carácter «A» en hexadecimal?

A. 0x01
B. 0x41
C. 0x61
D. 0x65

Ordenal

Cuál es el valor ordinal del carácter «A» en hexadecimal?

A. 0x01
B. 0x41
C. 0x61
D. 0x65

ANSWER: C

Find callback

Cuál de los siguientes comandos podría imprimir el contenido del archivo «/etc/passwd»?

A. find ./legit/ /etc/passwd
B. find ./legit/ –callback ../../etc/passwd
C. find ../../../
D. find ./legit/ -exec cat /etc/passwd ;

Find callback

Cuál de los siguientes comandos podría imprimir el contenido del archivo «/etc/passwd»?

A. find ./legit/ /etc/passwd
B. find ./legit/ –callback ../../etc/passwd
C. find ../../../
D. find ./legit/ -exec cat /etc/passwd ;

ANSWER: D

Inyección Bash

Cuál de los siguientes comandos intrínsecos de Bash es vulnerable a la inyección de código a través de sus parámetros (después de todas la expanciones de linea)?

A. exit
B. pwd
C. pushd
D. printf

Inyección Bash

Cuál de los siguientes comandos intrínsecos de Bash es vulnerable a la inyección de código a través de sus parámetros (después de todas la expanciones de linea)?

A. exit
B. pwd
C. pushd
D. printf

ANSWER: D

Evasión de WAF

De las siguientes expresiones, cuál es un intento de evasión de un WAF que bloquearía los espacios mediante una lista de denegación?

A. cat flag
B. catflag
C. cat$flagD.cat${IFS}flag

Evasión de WAF

De las siguientes expresiones, cuál es un intento de evasión de un WAF que bloquearía los espacios mediante una lista de denegación?

A. cat flag
B. catflag
C. cat$flagD.cat${IFS}flag

ANSWER: D

Reflejo al conectarse

Cuál es el comando recomendado en la clase que se debe ejecutar inmediatamente después de establecer una conexión de un shell inverso?

A. clear
B. unset HISTFILE
C. whoami
D. exit

Reflejo al conectarse

Cuál es el comando recomendado en la clase que se debe ejecutar inmediatamente después de establecer una conexión de un shell inverso?

A. clear
B. unset HISTFILE
C. whoami
D. exit

ANSWER: B

Python getattr

Qué realiza la función builtin de Python «getattr»?

A. Evaluación
B. Encapsulación
C. Refleción
D. Deserialización

Python getattr

Qué realiza la función builtin de Python «getattr»?

A. Evaluación
B. Encapsulación
C. Refleción
D. Deserialización

ANSWER: C

Python pickle

De qué sirve el módulo «pickle» de Python?

A. Evaluación
B. Encapsulación
C. Refleción
D. Deserialización

Python pickle

De qué sirve el módulo «pickle» de Python?

A. Evaluación
B. Encapsulación
C. Refleción
D. Deserialización

ANSWER: D

Vulnerabilidad IA

De las siguientes vulnerabilidades, cuál tiene una relación directa con la inteligencia artificial?

A. Server-Side Request Forgery
B. Inyección de Entidades Externas XML
C. Inyección en el Prompt
D. Cross-Site Scripting (XSS)

Vulnerabilidad IA

De las siguientes vulnerabilidades, cuál tiene una relación directa con la inteligencia artificial?

A. Server-Side Request Forgery
B. Inyección de Entidades Externas XML
C. Inyección en el Prompt
D. Cross-Site Scripting (XSS)

ANSWER: C