CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

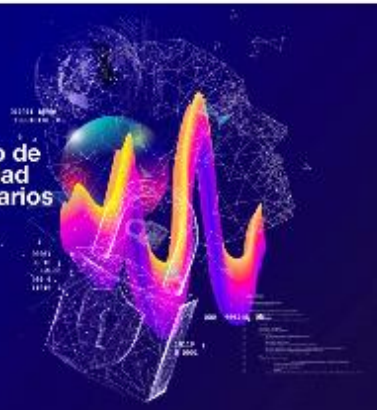
2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

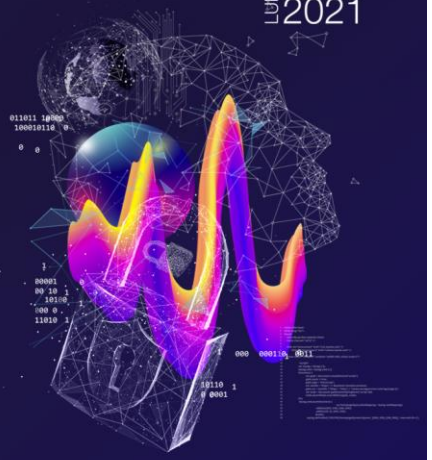
CSIRT

2do Seminario de Ciberseguridad para funcionarios públicos



Seguridad en sitio web:
Herramientas y verificación práctica

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



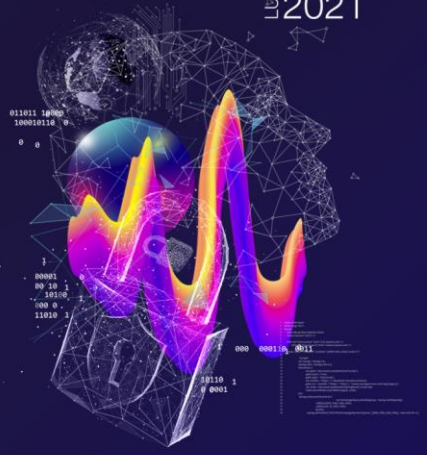
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Herramientas y verificación práctica

- El taller presente tiene como objetivo mostrar una introducción a herramientas y técnicas para corroborar la seguridad de una aplicación web.
- Para realizar esta labor, existen sistemas operativos diseñados para ejecutar labores de análisis de ciberseguridad:
  - Kali Linux
  - Parrot
- También se puede utilizar otra distribución de Linux y luego descargar e instalar las herramientas de forma independiente.

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

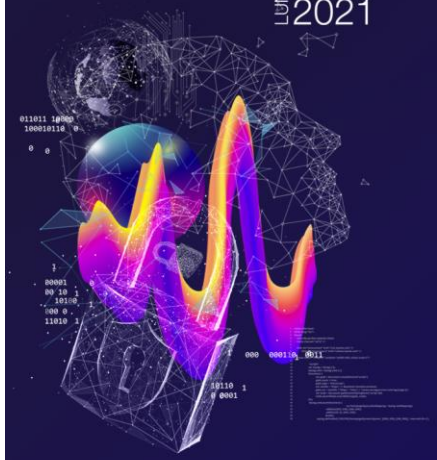
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Herramientas y verificación práctica

- Primero veamos una clasificación de las vulnerabilidades con el objetivo de obtener una imagen más general de los tipos de vulnerabilidades y su causa:

Ministerio del Interior y Seguridad Pública

Vulnerabilidad	Diseño	Programación	Operación	Mantención
XSS		X		
SQL		X		
CSRF	X			
Bypass de autenticación	X	X		
Software desactualizado			X	X
Clickjacking			X	
HSTS			X	
Versiones expuestas			X	
Configuración errónea de cookies		X	X	
Mal configurado WP			X	
Suites de cifrados débiles				X
Ausencia de protección contra fuerza bruta	X			
Credenciales en texto claro o cifrado débil	X			
Política de credenciales débiles	X			



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

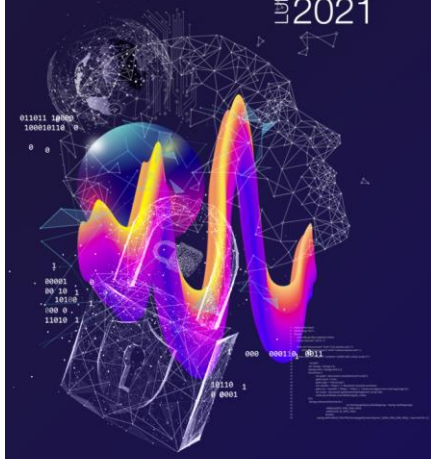
Taller de Seguridad Web

El taller se compone de las siguientes demostraciones:

- Búsqueda Web
  - Uso de amass y sublist3r
- Vulnerabilidades de Programación
  - Uso de OWASP ZAP Automático
  - Uso de OWASP Guiado
- Vulnerabilidades de Infraestructura
  - Uso de nikto y nmap

2do Seminario de Ciberseguridad para funcionarios públicos

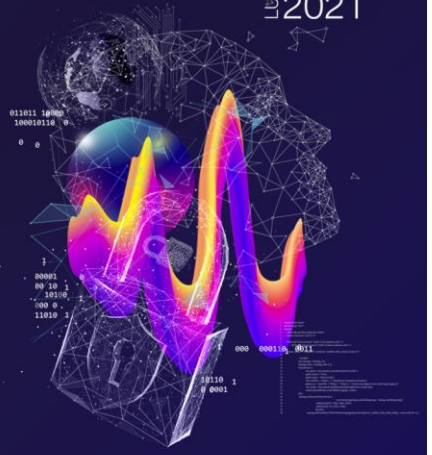
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



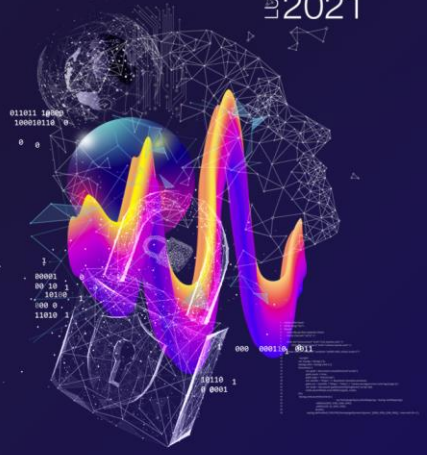
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Taller de Seguridad Web

- Vulnerabilidades de Software Externo
  - Uso de WPScan
- Vulnerabilidades de Diseño
  - Técnicas de Enumeración
  - Repositorios Git
  - Dirsearch
- Proxy Interceptor
  - Subida de archivos
  - XSS
  - Path Traversal
  - Hydra

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Búsqueda de presencia en la Web

- El primer paso a la hora de realizar un análisis web es definir el alcance. Para este caso, se define el alcance como una institución, por lo que es necesario obtener el listado de sitios y subdominios de la institución.
- Existe la posibilidad de que el área operativa no contenga un listado exhaustivo de los aplicativos web o que se haya olvidado de todos los aplicativos que poseen.
- Por lo tanto es siempre útil realizar una búsqueda de subdominios para determinar toda la superficie de ataque.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

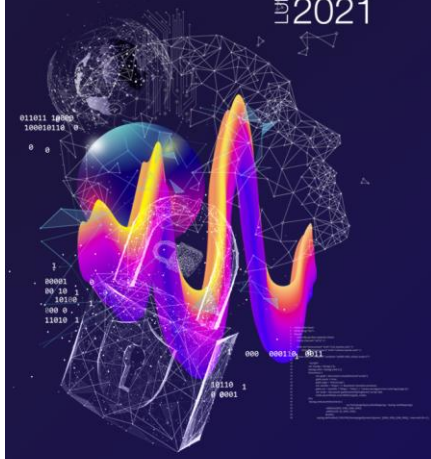
Búsqueda de Dominios y Subdominios

- Para buscar subdominios se recomienda utilizar las siguientes herramientas:
  - Amass
  - Sublist3r
- Las dos pueden encontrar resultados diferentes, por lo tanto se recomienda utilizar ambas:

```
amass intel -cidr CIDR -d gob.cl
amass enum -d sitio.cl
sublist3r -d sitio.cl
```

2do Seminario de Ciberseguridad para funcionarios públicos

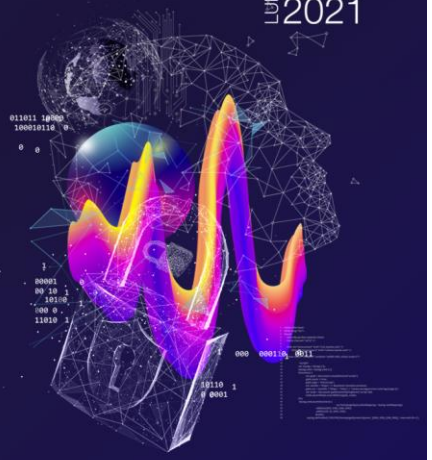
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Resultados de Búsqueda

```
┌──(kali㉿kali)-[~]
└─$ amass intel -cidr 163.247.0.0/16 -d gob.cl
interior.gob.cl
gov.cl
odepa.gob.cl
cnr.gob.cl
sag.gob.cl
achipia.gob.cl
ciren.cl
indap.cl
fucoa.cl
mbienes.cl
bienes.cl
bienesnacionales.cl
catastro.cl
defensa.cl
ns1.minagri.cl
gob.cl
supereduc.cl
mineduc.cl
consejodelacultura.cl
junaeb.cl
agenciaeducacion.cl
dipres.cl
casamoneda.cl
sbif.cl
odepa.cl
cde.cl
serviciocivil.cl
scj.cl
sigfe.cl
sename.cl
sml.cl
cajmetro.cl
clientebancario.cl
cochilco.cl
minmineria.cl
snit.cl
minjusticia.cl
defensoriapenal.cl
mideplan.cl
fosis.cl
```

```
└─$ amass enum -d interior.gob.cl
cmv.interior.gob.cl
patrimonio.interior.gob.cl
Querying ArchiveIt for interior.gob.cl subdomains
Querying Bing for interior.gob.cl subdomains
Querying LoCArchive for interior.gob.cl subdomains
Querying Baidu for interior.gob.cl subdomains
www.interior.gob.cl
f1.interior.gob.cl
api-cmv.interior.gob.cl
siregad.interior.gob.cl
n.interior.gob.cl
Querying Pastebin for interior.gob.cl subdomains
cuenta-publica.interior.gob.cl
www.diariooficial.interior.gob.cl
siac.interior.gob.cl
ns6.interior.gob.cl
mta03.interior.gob.cl
Average DNS queries performed: 1461/sec, Average retries required: 78.71%
Querying Crtsh for interior.gob.cl subdomains
mta04.interior.gob.cl
www.cmv.interior.gob.cl
mta01.interior.gob.cl
diariooficial.interior.gob.cl
siregad2.interior.gob.cl
f7.interior.gob.cl
Querying URLScan for interior.gob.cl subdomains
f6.interior.gob.cl
f3.interior.gob.cl
ns7.interior.gob.cl
mta02.interior.gob.cl
f8.interior.gob.cl
f5.interior.gob.cl
ns2.interior.gob.cl
f4.interior.gob.cl
f9.interior.gob.cl
newsletter.interior.gob.cl
```

Ministerio del Interior y Seguridad Pública

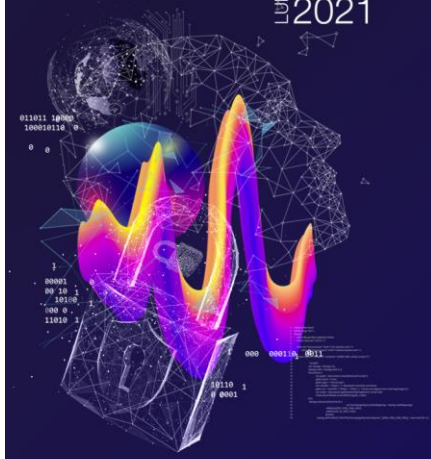
Gobierno de Chile

Resultados de Búsqueda

```
└─$ sublist3r -d interior.gob.cl

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for interior.gob.cl
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 46
www.interior.gob.cl
apadrinamiento.interior.gob.cl
ciberseguridad.interior.gob.cl
edge.interior.gob.cl<BR>prsksmi02.interior.gob.cl
edge.interior.gob.cl<BR>lyncdiscover.interior.gob.cl<BR>lyncdiscoverinternal.interior.gob.cl<BR>meet.interior.gob.cl<BR>prsksmi01.interior.gob.cl<BR>sip.interior.gob.cl
lyncdiscover.interior.gob.cl<BR>lyncdiscoverinternal.interior.gob.cl<BR>meet.interior.gob.cl<BR>prsksmi01.interior.gob.cl<BR>sip.interior.gob.cl
edge.interior.gob.cl<BR>prsksmi02.interior.gob.cl<BR>sip.interior.gob.cl
edge.interior.gob.cl<BR>sip.interior.gob.cl
interior.gob.cl<BR>www.interior.gob.cl
cmv.interior.gob.cl
correo.interior.gob.cl
diariooficial.interior.gob.cl
www.diariooficial.interior.gob.cl
divdecar.interior.gob.cl
edge.interior.gob.cl
extranet.interior.gob.cl
ga.interior.gob.cl
gb.interior.gob.cl
infoexone.interior.gob.cl
js.interior.gob.cl
mail.interior.gob.cl
mailcmv1.interior.gob.cl
mailcmv2.interior.gob.cl
mailcmv3.interior.gob.cl
mailcmv4.interior.gob.cl
mailer.interior.gob.cl
mon-4punto3.interior.gob.cl
```

2do Seminario de Ciberseguridad para funcionarios públicos

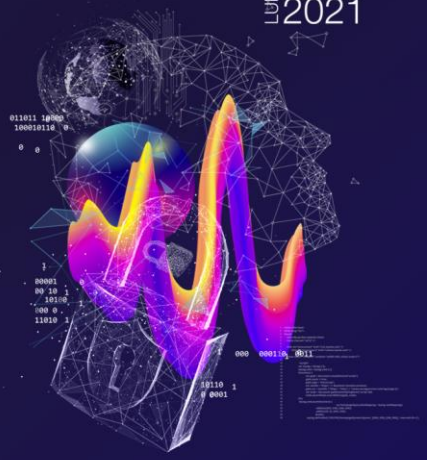
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidades introducidas por la programación

- Defectos genéricos efectuados por el equipo de Desarrollo.
- Se recomienda utilizar una herramienta como OWASP ZAP.
- Recordar que toda inspección de seguridad puede traer consigo consecuencias negativas como indisponibilidad del servicio e inyección de data basura.

Ministerio del Interior y Seguridad Pública

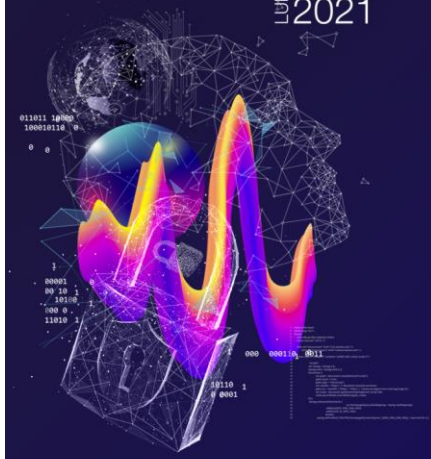
Gobierno de Chile

OWASP ZAP (Búsqueda rápida)

- La fortaleza de los escaneadores es que permiten cubrir mucho terreno rápidamente.
- Sin embargo se deben configurar y revisar correctamente para asegurar que realicen su labor de forma correcta. Esta revision se puede realizar examinando la cobertura.

2do Seminario de Ciberseguridad para funcionarios públicos

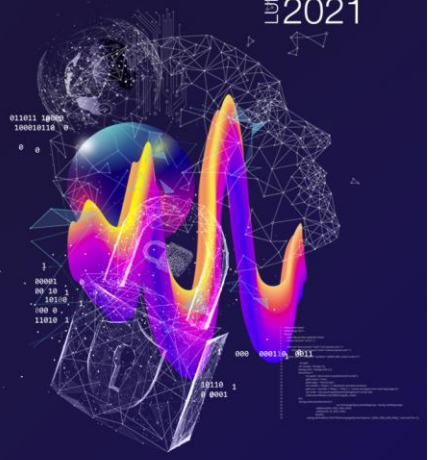
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

OWASP ZAP (Modo guiado)

- Si bien se obtienen vulnerabilidades de esta forma, no obtienen todas las que ZAP podría detectar. Esto es porque ZAP no tiene conocimiento para recorrer todo el sitio.
- Este problema puede ser resuelto si se le entrega a ZAP una manera de obtener una consulta válida en el sitio.
- Para esto se debe configurar el proxy interno en ZAP y luego configurar el navegador para que redirija las consultas hacia ZAP. Esto último se puede hacer con la configuración del proxy o utilizando un plugin como foxyproxy.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

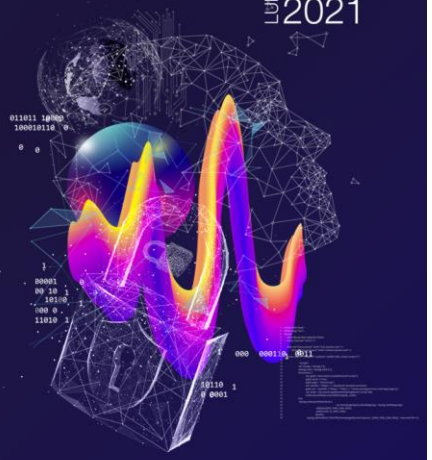
OWASP Zap (Modo guiado)

- Al recorrer el sitio ahora se puede ver como se guardan las consultas.
- Se puede realizar una revision guiada seleccionando la nueva consulta.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

OWASP ZAP (Modo guiado)

- Es muy importante detectar cuando el scanner puede haber fallado de forma que se pueda suplementar la revisión con una prueba guiada.
- Esto significa que el analista a cargo de revisar el sitio tenga conocimiento sobre el funcionamiento del sitio y sus posibles puntos de fallo.

Ministerio del Interior y Seguridad Pública

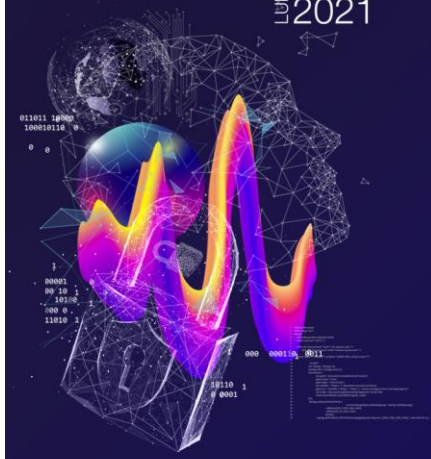
Gobierno de Chile

OWASP ZAP (Debilidades)

- OWASP ZAP tiene dos grandes problemas lo cual significa no poder depender solamente de esta solución para verificar la seguridad del sitio:
  - Entrega una gran cantidad de falsos positivos, por lo tanto requiere de tiempo para verificar las vulnerabilidades reportadas.
  - Está hecho para encontrar vulnerabilidades relacionadas al “OWASP”, por lo tanto no puede encontrar problemas específicos a las tecnologías implementadas.

2do Seminario de Ciberseguridad para funcionarios públicos

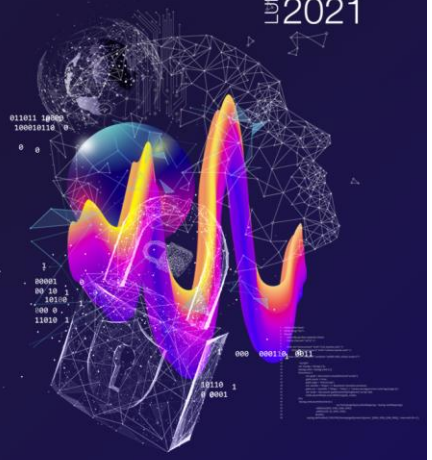
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidades Externas

- Para examinar este último punto, es conveniente dividir las vulnerabilidades externas en dos categorías:
  - Vulnerabilidades de Infraestructura
  - Vulnerabilidades de Software Externo

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

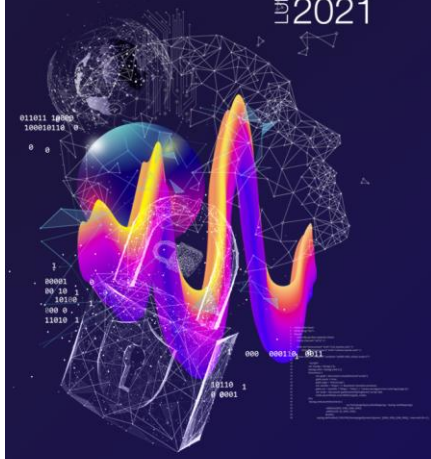
Vulnerabilidades de Infraestructura

- Si bien este punto queda fuera del alcance de la presentación, se recomienda utilizar una combinación de nikto, nmap y openVAS. También se podrían utilizar software dedicado de escaneo que tengan una versión gratuita como Nessus.

```
nikto -host sitio.cl
nmap -sS -p- sitio.cl
nmap -sV -sC -p80,443,3306 -O sitio.cl
```

2do Seminario de Ciberseguridad para funcionarios públicos

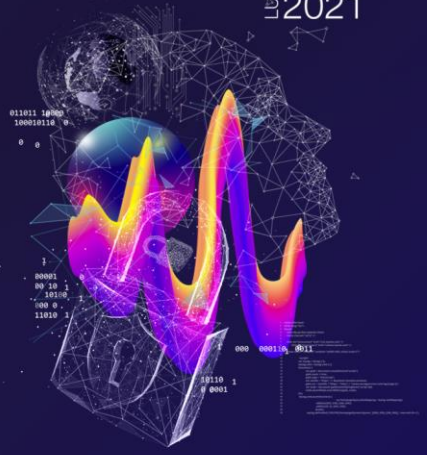
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidades de Software Externo

- Una gran cantidad del software actualmente instalado es externo. Ejemplos de esto son las instalaciones de Wordpress, Drupal o Moodle.
- Si bien utilizar software externo puede significar ahorro en tiempo y costo de la implementación, así como acceso a un mayor nivel de calidad, se debe tener un plan de actualización para estos.
- Recordar que estos software externos pueden tener vulnerabilidades, las cuales pueden ser descubiertas, publicadas y luego explotadas en el sitio.

Ministerio del Interior y Seguridad Pública

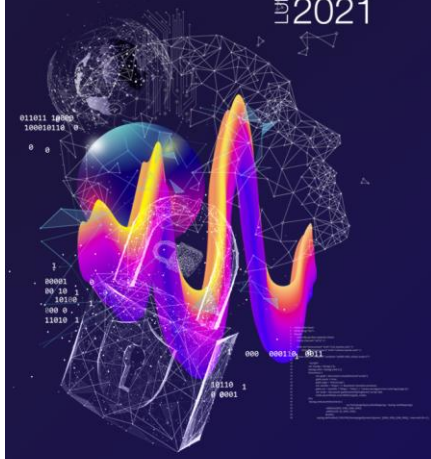
Gobierno de Chile

Vulnerabilidades de Software Externo

- Existen varios sitios con información sobre vulnerabilidades descubiertas en software público, algunas con exploits. Por ejemplo:
  - cvedetails
  - exploit-db
  - Rapid7
  - Packet Storm Security
  - Etc.
- La explotación de muchas de estas vulnerabilidades se encuentran automatizadas, permitiendo a bots atacar grandes cantidades de sitios al mismo tiempo

2do Seminario de Ciberseguridad para funcionarios públicos

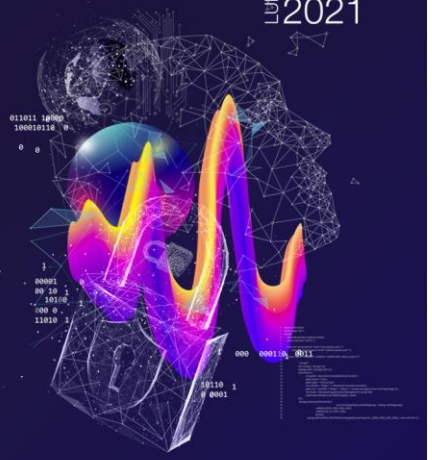
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Vulnerabilidades de Software Externo

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- Todo lo anterior no solo aplica para los software base (ej. Wordpress), sino también para sus plugins.
- Muchos plugins no son elaborados por un equipo de desarrollo maduro y, por lo tanto, no necesariamente siguen las mejores prácticas de desarrollo seguro.
- Como consecuencia, se debería tener una política con respecto a la instalación de plugins y software externo complementario al sitio.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

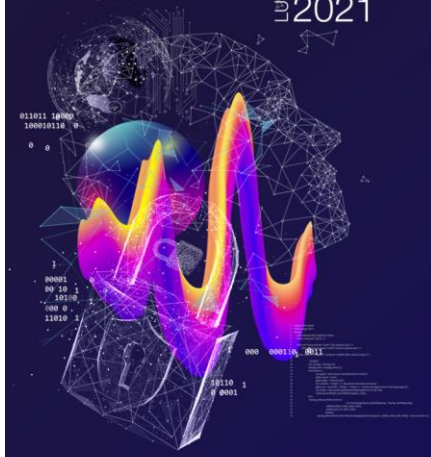
Vulnerabilidades de Wordpress

- Wordpress es probablemente el software más utilizado al momento de levantar un sitio.
- Para revisar el sitio de forma automatizada existe software especializado como WPScan, el cual puede entregar un pequeño reporte de lo encontrado.
- Comando Recomendado:

```
Wpscan --url http://www.sitio.gob.cl -e ap,at,tt,cb,dbe,u
--plugin-detection mixed
```

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

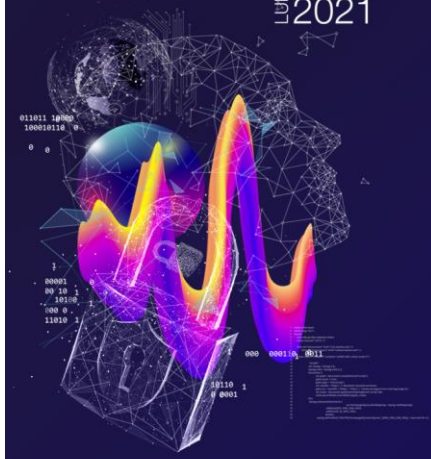
Gobierno de Chile

Vulnerabilidades de Wordpress

```
[+] akismet
 | Location: http://192.168.56.102/wordpress/wp-content/plugins/akismet/
 | Last Updated: 2021-09-03T16:53:00.000Z
 | Readme: http://192.168.56.102/wordpress/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 4.1.12
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.56.102/wordpress/wp-content/plugins/akismet/, status: 200
 |
 | Version: 3.1.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.56.102/wordpress/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.56.102/wordpress/wp-content/plugins/akismet/readme.txt

[+] wp-file-upload
 | Location: http://192.168.56.102/wordpress/wp-content/plugins/wp-file-upload/
 | Last Updated: 2021-09-18T09:19:00.000Z
 | Readme: http://192.168.56.102/wordpress/wp-content/plugins/wp-file-upload/readme.txt
 | [!] The version is out of date, the latest version is 4.16.0
 | [!] Directory listing is enabled
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Known Locations (Aggressive Detection)
 |  - http://192.168.56.102/wordpress/wp-content/plugins/wp-file-upload/, status: 200
 |
 | Version: 4.3.3 (50% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.56.102/wordpress/wp-content/plugins/wp-file-upload/readme.txt

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:05 <=========================================================================> (2575 / 2575) 100.00% Time: 00:00:05

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=========================================================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00 <=========================================================================> (71 / 71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=========================================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

2do Seminario de Ciberseguridad para funcionarios públicos

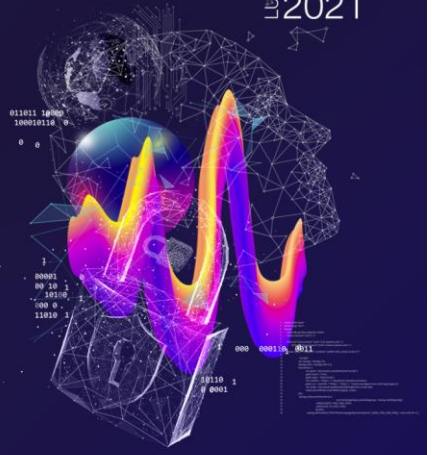
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidades de Software Externo

- Por supuesto, además de actualizar el sitio y sus componentes se deberían seguir reglas generales de sitios seguros de wordpress como evitar la enumeración de usuarios, deshabilitar el acceso a wp-login o eliminar los listados de directorio.
- En el caso de que el CMS sea Joomla se puede utilizar Joomscan, droopescan para drupal o moodlescan para moodle. Tener en consideración que estos proyectos no tienen el mismo alcance que WPScan.
- Es fundamental mantener un monitoreo de las vulnerabilidades asociadas a sistemas instalados

Ministerio del Interior y Seguridad Pública

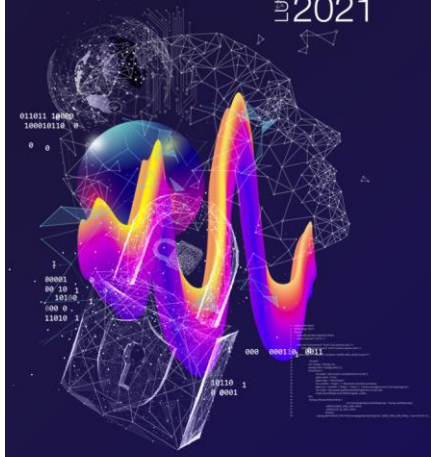
Gobierno de Chile

Vulnerabilidades introducidas en el Diseño

- Un tipo común de error de diseño es la falta de claridad y explicitud en la lógica de negocio lo cual puede resultar en escalamientos horizontales o verticales.
- Primero, realicemos la distincion entre Autenticación y Autorización
  - Autenticación: Usuario es quien dice ser (usuario Gestor es realmente Gestor).
  - Autorización: Usuario puede acceder a aquello que puede acceder (privilegios del usuario Gestor son sólo los del usuario Gestor).

2do Seminario de Ciberseguridad para funcionarios públicos

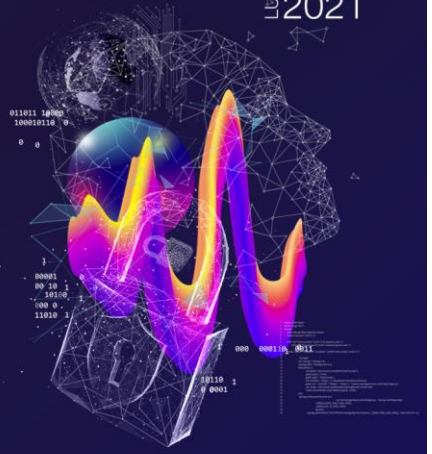
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

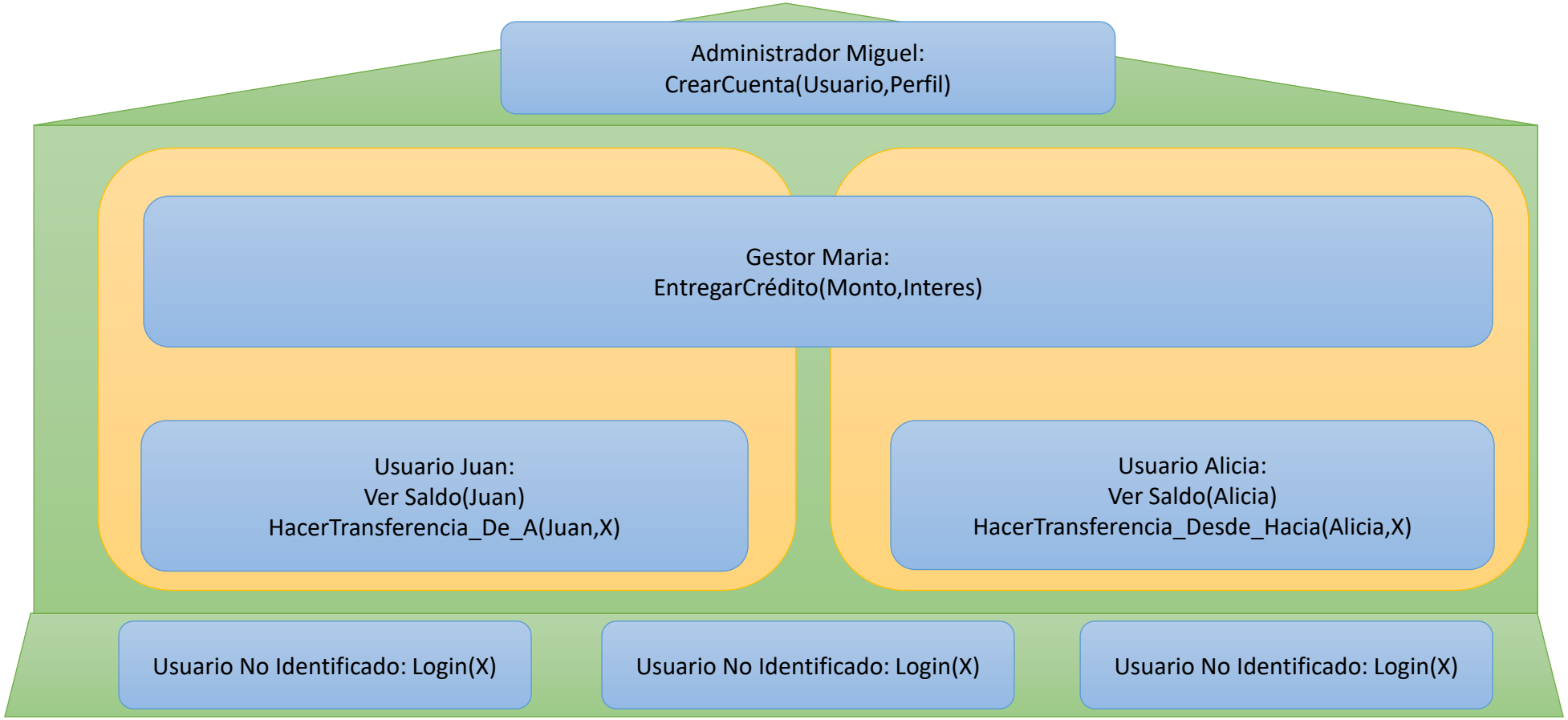
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



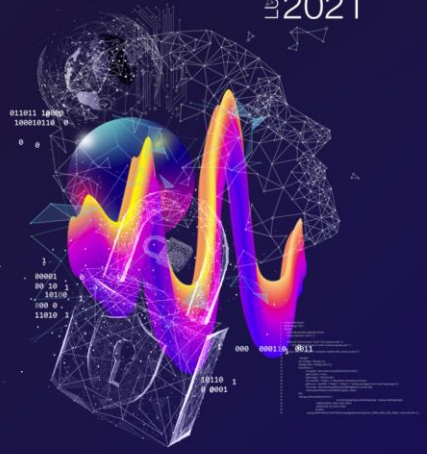
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Lógica de Negocio (Ejemplo)



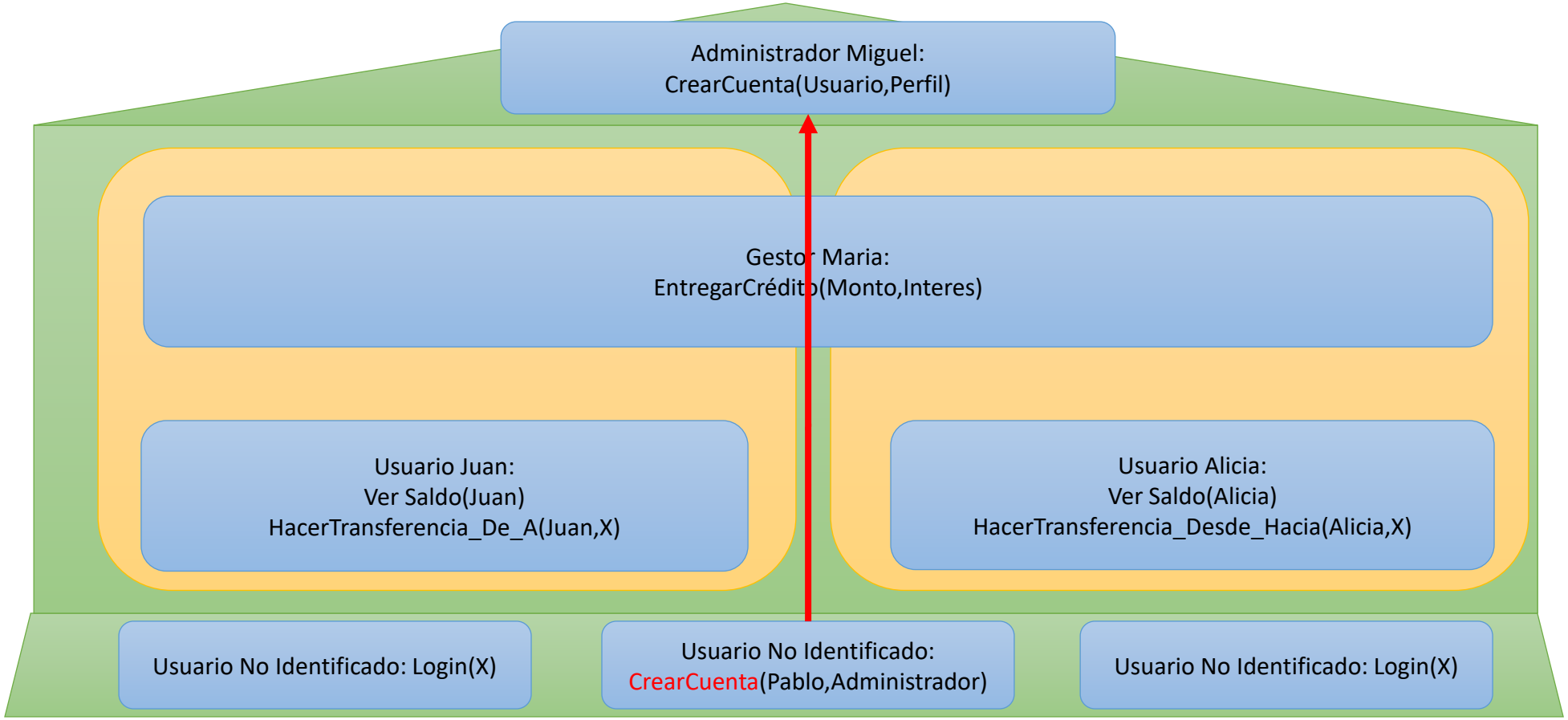
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



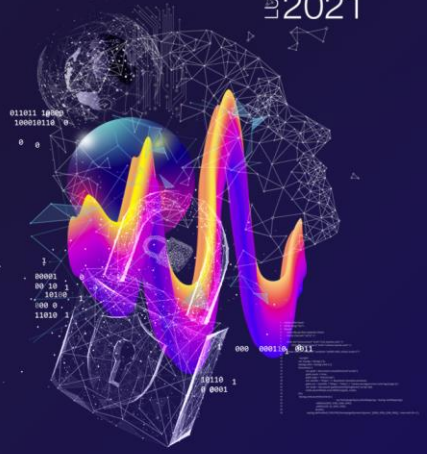
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidad en Autenticación



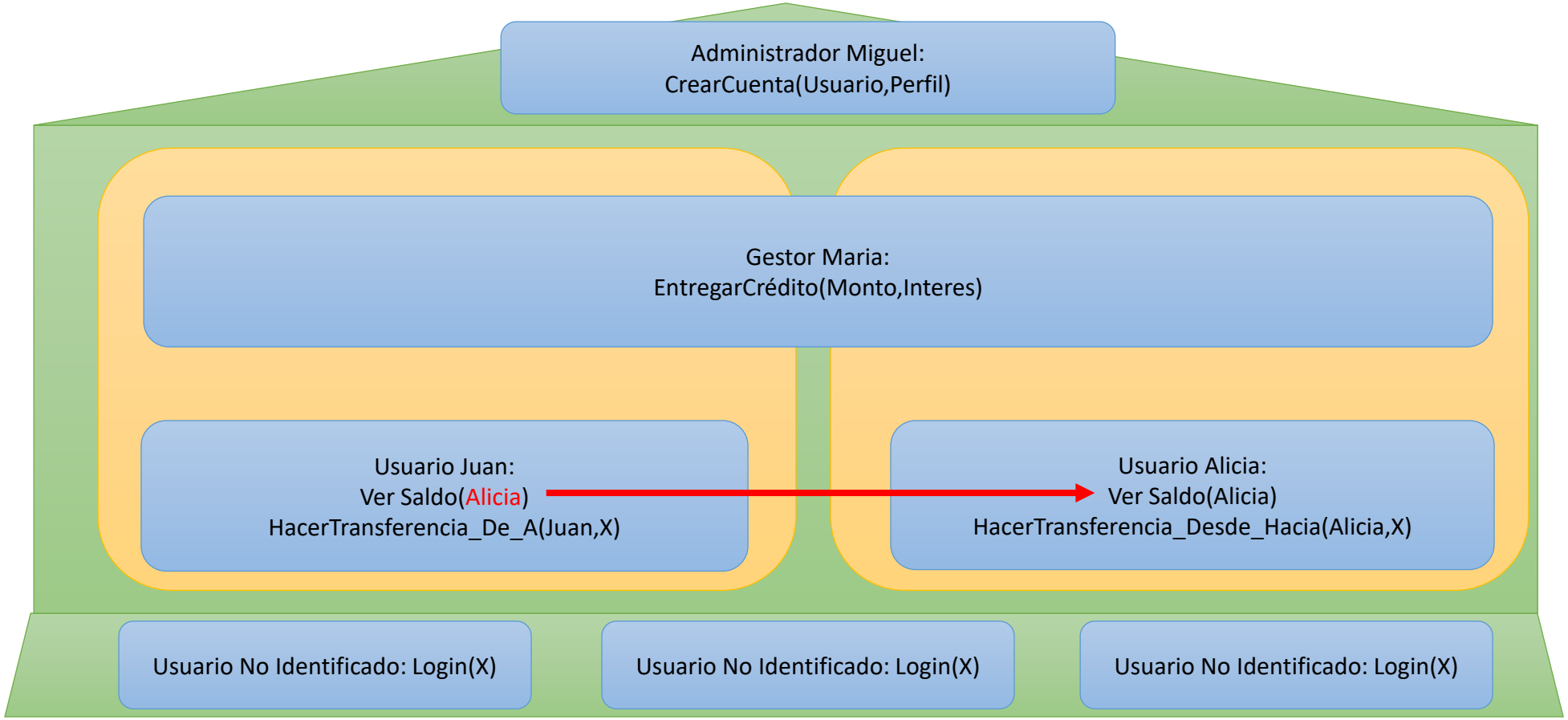
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



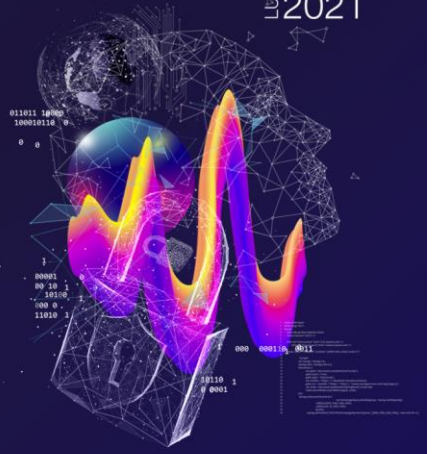
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidad en Autorización



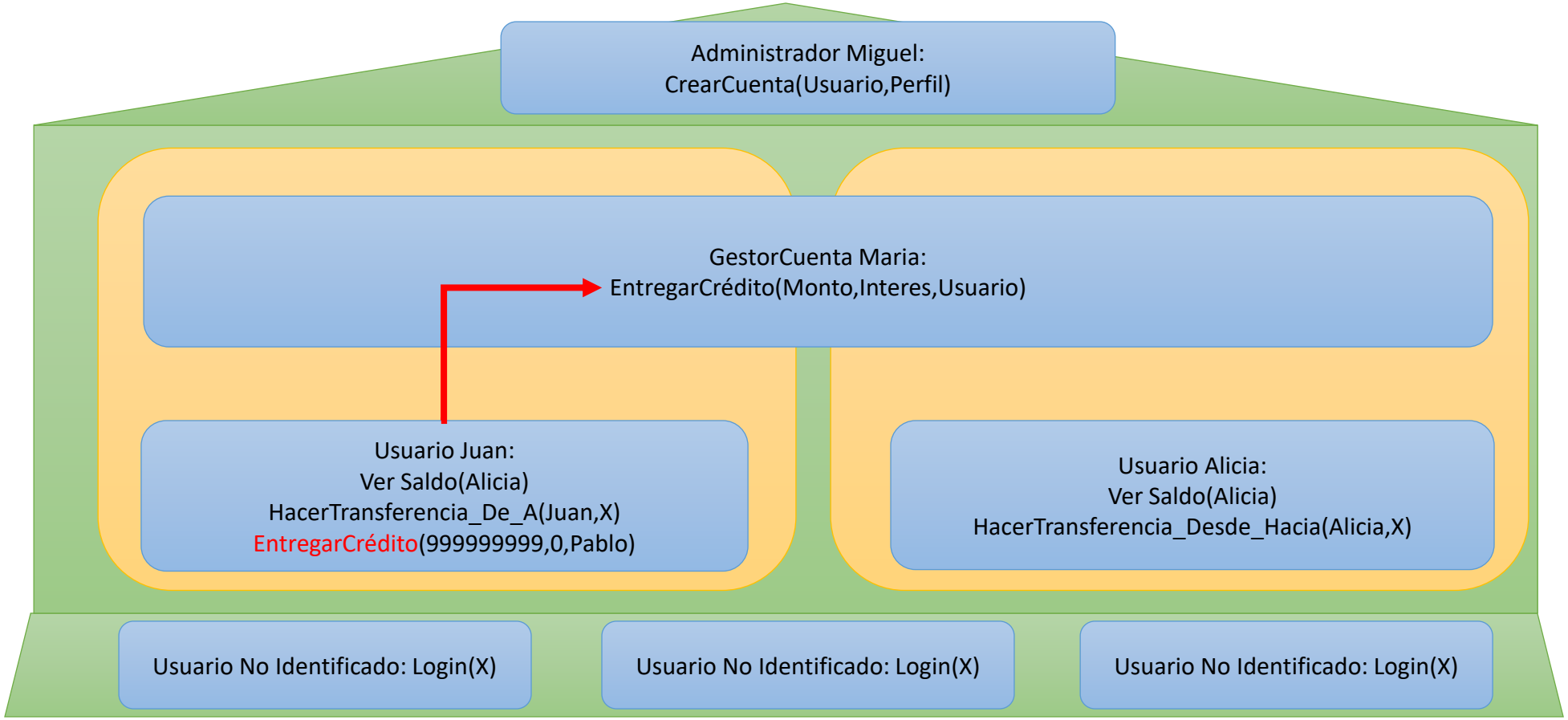
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidad en Autorización y Autenticación



Ministerio del Interior y Seguridad Pública

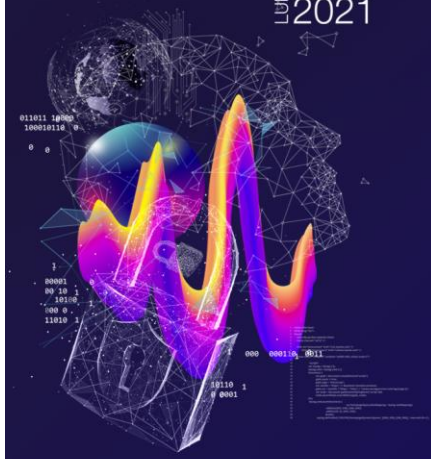
Gobierno de Chile

Formas de Obtener listados

- Enumeracion se puede realizar de varias formas:
  - Listado de Directorio
  - Búsquedas en motores de búsqueda incluyendo caché
  - Repositorios Git
  - Archivos interesantes como robots.txt o Sitemap.xml
  - Crawling/Spidering
  - Inspección de Código fuente y comentarios
  - Archivos .DS_Store y thumbs.db
  - Ataques por diccionario y por fuerza bruta.

2do Seminario de Ciberseguridad para funcionarios públicos

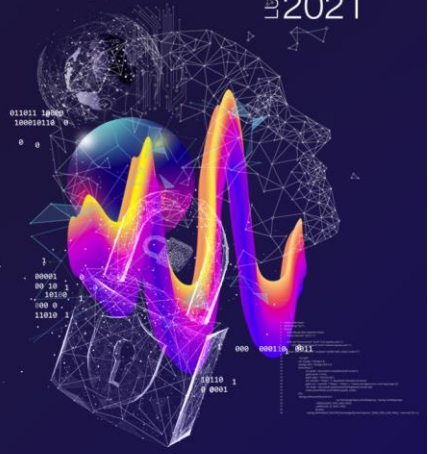
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Consecuencias

El efecto de estas vulnerabilidades depende del aplicativo en sí.

Se debe tener especial cuidado en las funciones relacionadas a la creación de usuarios, a la subida de archivos, a funciones que entreguen información sensible y con los reportes.

Ministerio del Interior y Seguridad Pública

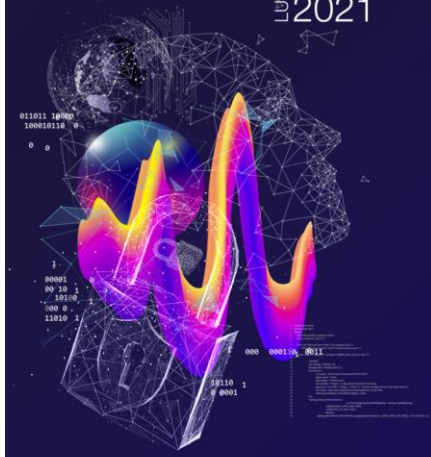
Gobierno de Chile

Vulnerabilidades de Lógica de Negocio: Interceptación

- Para poder realizar la tarea de explotar la lógica de negocio, muchas veces es necesario utilizar un servidor proxy para interceptar solicitudes al servidor y alterarlas.
- Recordar que la comunicación en internet se realiza por lo general por solicitudes y respuestas hacia los servidores. En ocasiones, las validaciones son realizadas por el navegador pero no son revalidadas por el servidor al momento de enviar la solicitud.

2do Seminario de Ciberseguridad para funcionarios públicos

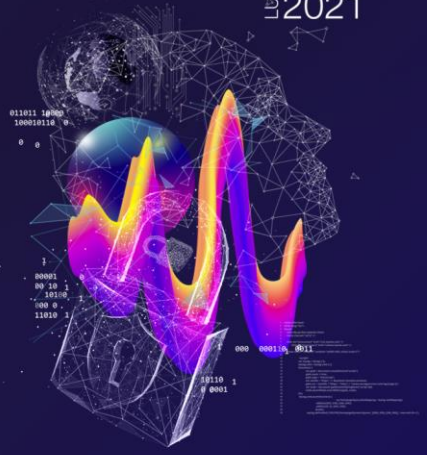
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Vulnerabilidades de Lógica de Negocio: Interceptación

- Generalmente se utiliza Burp Suite para realizar esta tarea, sin embargo OWASP ZAP también trae su propio Servidor Proxy, por lo que se utilizará esta herramienta.
- La configuración del modo guiado de ZAP es suficiente para activar este servidor.
- Una vez capturada la solicitud, también se pueden utilizar herramientas de fuerza bruta para poder obtener credenciales.

Ministerio del Interior y Seguridad Pública

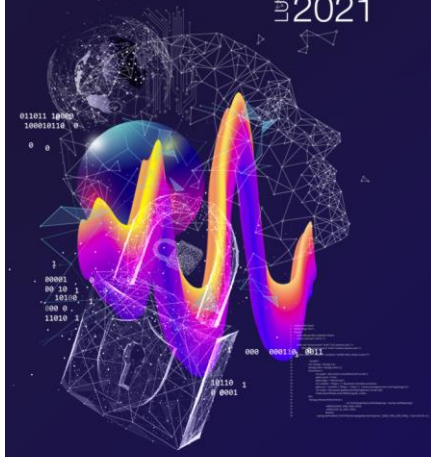
Gobierno de Chile

Propuesta de Clasificación de Vulnerabilidades: Resolución

- Para la resolución correcta de una vulnerabilidad, es crucial entender la causa raíz de ésta.
- En otras palabras, la seguridad de la información no es una tarea de los desarrolladores o de los operadores, sino que es tarea de todos.

2do Seminario de Ciberseguridad para funcionarios públicos

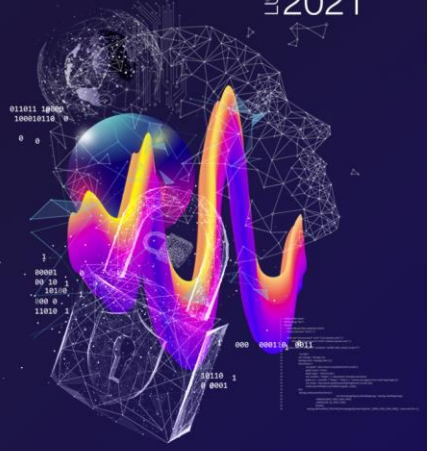
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Propuesta de Clasificacion de Vulnerabilidades: Resolución

- Un defecto en código puede venir de una falta de tiempo para desarrollar o de falta de capacitaciones en desarrollo seguro.
- Un archivo sensible en producción puede significar problemas en el proceso de paso a producción o de falta de prolijidad en el uso de los servidores de operaciones.
- Un error en las autorizaciones puede deberse a una mala toma de requerimientos que no contenga los posibles casos desborde.

Ministerio del Interior y Seguridad Pública

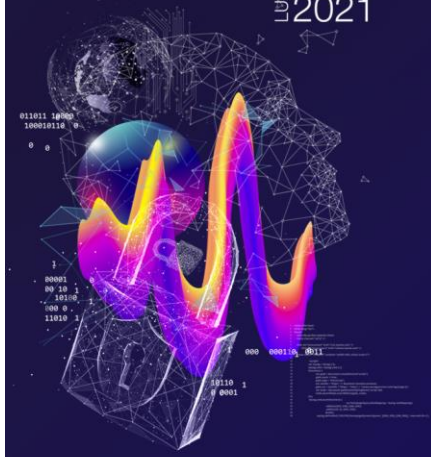
Gobierno de Chile

Propuesta de Clasificacion de Vulnerabilidades: Resolución

- En nuestra experiencia una vulnerabilidad es la punta del iceberg de un problema en el ciclo de vida de un aplicativo web.
- Por lo tanto para finalmente superar una vulnerabilidad detectada, se debe encontrar y solucionar el problema raíz de éste.
- Es crucial entender bien el proceso real de diseño, desarrollo, operación y mantención informática para avanzar hacia una mayor segurización de la organización.

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile