mit-av-web Reporte del escaneo

Nombre del proyecto	mit-av-web
Iniciar Escaneo	miércoles, 18 de mayo de 2022 15:03:41
Conjunto de Consultas	OWASP TOP 10 - 2017
Tiempo de escaneo	00h:12m:24s
Líneas de código escaneadas	135247
Archivos escaneados	1034
Hora de creación del reporte	miércoles, 18 de mayo de 2022 15:16:18
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733
Equipo	DEVOPS
Versión de Checkmarx	9.2.0.41015 HF28
Tipo de escaneo	Completo
Origen de la Fuente	GIT
Rama	/refs/heads/FTR-RITM0051065
Densidad	5/10000 (Vulnerabilidades/LOC)
Visibilidad	Público

Configuración de filtro

Severidad

Incluido: Altas, Medias, Bajas, Información

Excluido: Ninguna

Estado del resultado

Incluido: Confirmado, No explotable, Para verificar, Urgente, Propuesto no explotable

Excluido: Ninguna

Asignado a

Incluido: Todas

Categorías

Incluido:

Sin categoría	Todas
Custom	Todas
PCI DSS v3.2.1	Todas
OWASP Top 10 2013	Todas
FISMA 2014	Todas
NIST SP 800-53	Todas
OWASP Top 10 2017	Todas
OWASP Mobile Top 10 2016	Todas
OWASP Top 10 API	Todas
OWASP Top 10 2021	Todas

Excluido:

Sin categoría	Ninguna

Custom	Ninguna
PCI DSS v3.2.1	Ninguna
OWASP Top 10 2013	Ninguna
FISMA 2014	Ninguna
NIST SP 800-53	Ninguna
OWASP Top 10 2017	Ninguna
OWASP Mobile Top 10 2016	Ninguna
OWASP Top 10 API	Ninguna
OWASP Top 10 2021	Ninguna

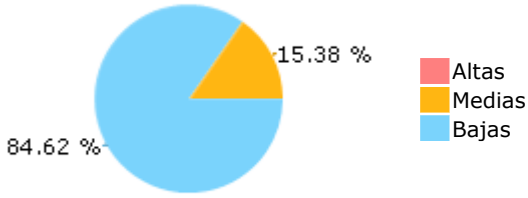
Límite de resultados

El límite de resultados por consulta se estableció en 50

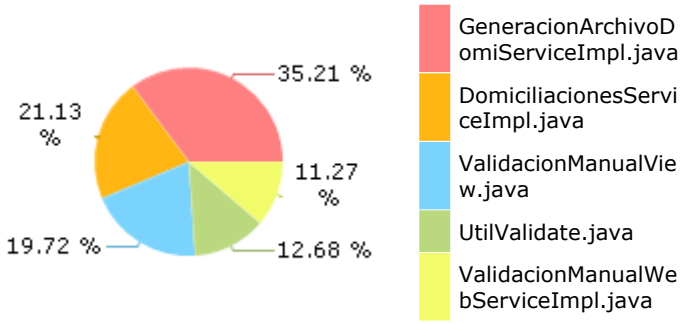
Consultas seleccionadas

Las consultas seleccionadas estan listadas en Resumen de los resultados

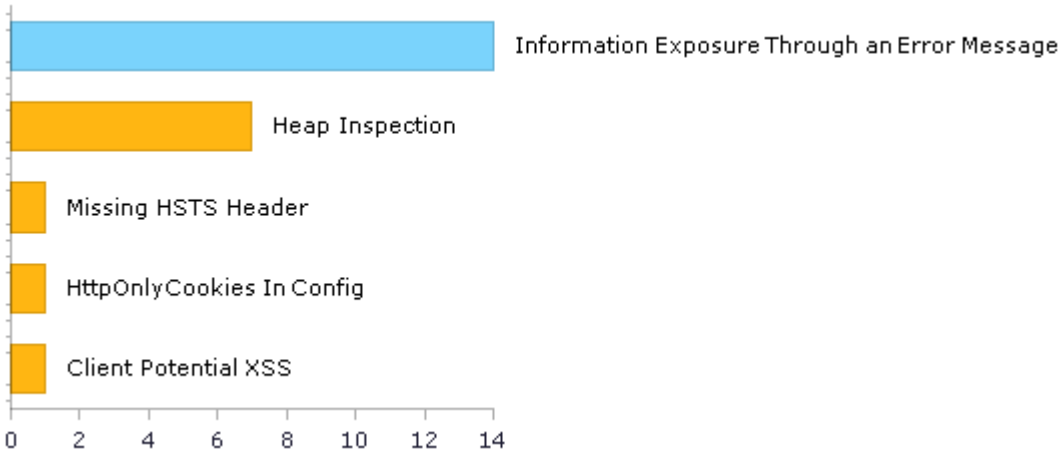
Resumen de los resultados



Archivos más vulnerables



Las 5 Vulnerabilidades Principales



Resumen de escaneo - OWASP Top 10 2017

Información adicional sobre vulnerabilidades y riesgos puede ser encontrada en: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	4	4
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	13	12
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	188	188
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	49	43
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	2
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	14	14
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

Resumen de escaneo - OWASP Top 10 2021

Category	Issues Found	Best Fix Locations
A1-Broken Access Control*	188	188
A2-Cryptographic Failures*	0	0
A3-Injection*	3	4
A4-Insecure Design*	67	60
A5-Security Misconfiguration*	0	1
A6-Vulnerable and Outdated Components	14	14
A7-Identification and Authentication Failures*	2	3
A8-Software and Data Integrity Failures*	0	0
A9-Security Logging and Monitoring Failures*	65	65
A10-Server-Side Request Forgery	0	0

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

Resumen de escaneo - OWASP Top 10 2013

Información adicional sobre vulnerabilidades y riesgos puede ser encontrada en: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	2	2
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)*	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	2
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	34	28
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	13	12
A7-Missing Function Level Access Control	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	188	188
A8-Cross-Site Request Forgery (CSRF)*	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	14	14
A10-Unvalidated Redirects and Forwards*	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

Resumen de escaneo - PCI DSS v3.2.1

Category	Issues Found	Best Fix Locations
PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection*	1	1
PCI DSS (3.2.1) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage	9	9
PCI DSS (3.2.1) - 6.5.4 - Insecure communications*	0	0
PCI DSS (3.2.1) - 6.5.5 - Improper error handling*	34	28
PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)	0	2
PCI DSS (3.2.1) - 6.5.8 - Improper access control*	188	188
PCI DSS (3.2.1) - 6.5.9 - Cross-site request forgery*	0	0
PCI DSS (3.2.1) - 6.5.10 - Broken authentication and session management*	0	0

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

Resumen de escaneo - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control*	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	12	13
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management*	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	14	8
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	2	2
Media Protection*	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection*	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity*	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	9	9

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados

para incluir todas las consultas estandard

Resumen de escaneo - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)*	18	18
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)*	1	1
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)*	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)*	1	1
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)*	1	1
SC-4 Information in Shared Resources (P1)*	0	0
SC-5 Denial of Service Protection (P1)*	1	1
SC-8 Transmission Confidentiality and Integrity (P1)*	0	0
SI-10 Information Input Validation (P1)*	2	2
SI-11 Error Handling (P2)*	14	8
SI-15 Information Output Filtering (P0)*	0	1
SI-16 Memory Protection (P1)*	0	0

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

Resumen de escaneo - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage*	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage*	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication*	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication*	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography*	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization*	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality*	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	1	1
M8-Code Tampering*	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering*	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality*	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

* Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

Resumen de escaneo - OWASP Top 10 API

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization*	0	0
API2-Broken Authentication*	0	0
API3-Excessive Data Exposure*	14	8
API4-Lack of Resources and Rate Limiting*	0	0
API5-Broken Function Level Authorization*	0	0
API6-Mass Assignment	0	0
API7-Security Misconfiguration*	0	0
API8-Injection*	2	2
API9-Improper Assets Management*	0	0
API10-Insufficient Logging and Monitoring	64	64

***** Los resultados del escaneo del proyecto no incluyen todas las consultas relevantes. El grupo de consultas y/o los filtros deben ser cambiados para incluir todas las consultas estandard

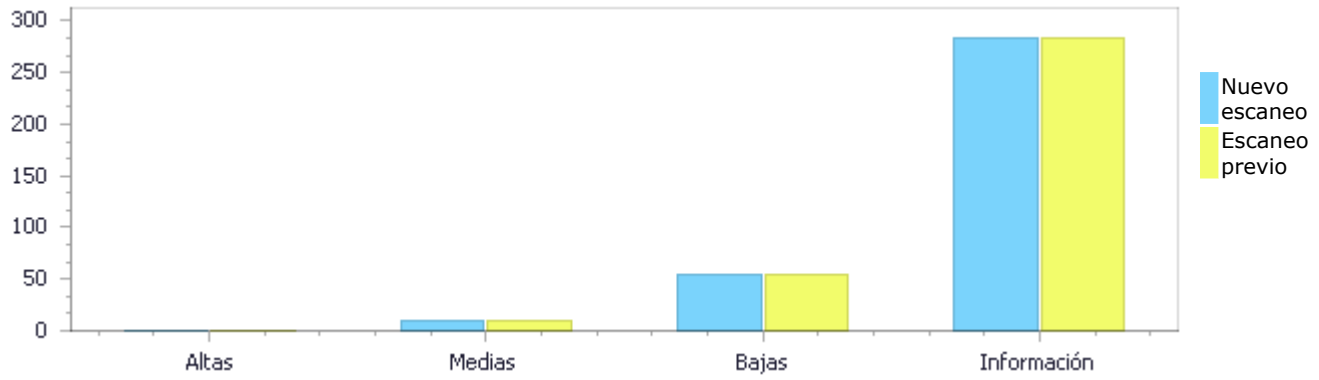
Resumen de escaneo - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Distribución de resultados por estatus

Comparado con el escaneo del proyecto de 04/04/2022 19:25

	Altas	Medias	Bajas	Información	Total
Nuevas vulnerabilidades	0	0	0	0	0
Vulnerabilidades recurrentes	0	0	55	284	339
Total	0	0	55	284	339
Vulnerabilidades solucionadas	0	0	0	0	0



Distribución de resultados por estado

	Altas	Medias	Bajas	Información	Total
Confirmado	0	0	0	0	0
No explotable	0	10	0	0	10
Para verificar	0	0	55	284	339
Urgente	0	0	0	0	0
Propuesto no explotable	0	0	0	0	0
Total	0	10	55	284	349

Resumen de los resultados

Tipo de vulnerabilidad	Ocurrencias	Severidad
Heap Inspection	7	Medias

Client Potential XSS	1	Medias
HttpOnlyCookies In Config	1	Medias
Missing HSTS Header	1	Medias
Information Exposure Through an Error Message	14	Bajas
Client JQuery Deprecated Symbols	13	Bajas
Incorrect Permission Assignment For Critical Resources	12	Bajas
Race Condition Format Flaw	6	Bajas
Serializable Class Containing Sensitive Data	3	Bajas
Client Password In Comment	1	Bajas
Log Forging	1	Bajas
Missing Content Security Policy	1	Bajas
Missing CSP Header	1	Bajas
Missing X Frame Options	1	Bajas
Potential ReDoS	1	Bajas
Spring defaultHtmlEscape Not True	1	Bajas
Exposure of Resource to Wrong Sphere	188	Información
Insufficient Logging of Exceptions	43	Información
Insufficient Logging of Database Actions	21	Información
Pages Without Global Error Handler	20	Información
Potentially Serializable Class With Sensitive Data	9	Información
Dynamic SQL Queries	2	Información
Use of Obsolete Functions	1	Información

Los 10 archivos más vulnerables

Vulnerabilidades altas y medias

Nombre del archivo	Problemas encontrados
source/mit-av-web/src/main/webapp/core/static/tema/js/biblioteca.js	1
source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java	1
source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.java	1
source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java	1
source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java	1
source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java	1
source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java	1
source/mit-av-business/src/main/wsc/java/profuturo/mx/nci/modelo/Parametro.java	1
source/mit-av-web/src/main/webapp/WEB-INF/web.xml	1
source/mit-av-web/src/main/java/mx/profuturo/nci/web/security/RedirectInvocationStrategy.java	1

Detalles de los Resultados del escaneo

Heap Inspection

Ruta de consulta:
Java\Cx\Java Medium Threat\Heap Inspection Versión:2

Categorías

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A2-Cryptographic Failures

Descripción

Heap Inspection\Ruta 1:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=2
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java
Línea	13	13
Objeto	password	password

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java
Método	private String password;

```
....
13.      private String password;
```

Heap Inspection\Ruta 2:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=3
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.j	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.j

	ava	ava
Línea	9	9
Objeto	clave	clave

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.java

Método: private String clave;

```
....
9.    private String clave;
```

Heap Inspection\Ruta 3:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=4
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java
Línea	40	40
Objeto	contrasena	contrasena

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java

Método: protected String contrasena;

```
....
40.      protected String contrasena;
```

Heap Inspection\Ruta 4:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=5
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-	source/mit-av-

	business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java	business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java
Línea	42	42
Objeto	contrasena	contrasena

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java
Método: protected String contrasena;

```
....
42.      protected String contrasena;
```

Heap Inspection\Ruta 5:

Severidad: Medias
Estado del resultado: No explotable
Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=6
Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java
Línea	38	38
Objeto	clave	clave

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java
Método: protected String clave;

```
....
38.      protected String clave;
```

Heap Inspection\Ruta 6:

Severidad: Medias
Estado del resultado: No explotable
Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=7
Estatus: Recurrente

	Origen	Destino

Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java
Línea	41	41
Objeto	clave	clave

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java

Método: protected String clave;

```
....
41.      protected String clave;
```

Heap Inspection\Ruta 7:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=8
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/nci/modelo/Parametro.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/nci/modelo/Parametro.java
Línea	37	37
Objeto	clave	clave

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/nci/modelo/Parametro.java

Método: protected int clave;

```
....
37.      protected int clave;
```

Client Potential XSS

Ruta de consulta:
JavaScript\Cx\JavaScript Medium Threat\Client Potential XSS Versión:3

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: Access Control
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)

OWASP Top 10 2021: A3-Injection

Descripción

Client Potential XSS\Ruta 1:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=1
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/biblioteca.js	source/mit-av-web/src/main/webapp/core/static/tema/js/biblioteca.js
Línea	22	37
Objeto	attr	outerHTML

Fragmento de código

Nombre del archivo source/mit-av-web/src/main/webapp/core/static/tema/js/biblioteca.js

Método $(".link-ejemplo").click(function () {

```
....
22.          div = ($(this).attr("href")).substr(1) + "-ejemplo";
```

Nombre del archivo source/mit-av-web/src/main/webapp/core/static/tema/js/biblioteca.js

Método function getChildNodes(cont) {

```
....
37.
$(codigo).append(quitarEtiquetas(child.outerHTML.toString()) + "<br>");
```

HttpOnlyCookies In Config

Ruta de consulta:
Java\Cx\Java Medium Threat\HttpOnlyCookies In Config Versión:1

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A5-Security Misconfiguration

Descripción

HttpOnlyCookies In Config\Ruta 1:

Severidad	Medias
Estado del resultado	No explotable
Resultados en	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid

línea	=2733&pathid=9
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/WEB-INF/web.xml	source/mit-av-web/src/main/webapp/WEB-INF/web.xml
Línea	1	1
Objeto	CxXmlConfigClass1190789717	CxXmlConfigClass1190789717

Fragmento de código

Nombre del archivo source/mit-av-web/src/main/webapp/WEB-INF/web.xml

Método <?xml version="1.0" encoding="UTF-8"?>

```
....
1.  <?xml version="1.0" encoding="UTF-8"?>
```

Missing HSTS Header

Ruta de consulta:
Java\Cx\Java Medium Threat\Missing HSTS Header Versión:1

Categorías

OWASP Top 10 2021: A7-Identification and Authentication Failures

Descripción

Missing HSTS Header\Ruta 1:

Severidad	Medias
Estado del resultado	No explotable
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=10
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/security/RedirectInvocationStrategy.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/security/RedirectInvocationStrategy.java
Línea	34	34
Objeto	write	write

Fragmento de código

Nombre del archivo source/mit-av-web/src/main/java/mx/profuturo/nci/web/security/RedirectInvocationStrategy.java

Método public void onInvalidSessionDetected(HttpServletRequest req, HttpServletResponse res) throws IOException, ServletException {

```
....
34.              res.getWriter().write(ajaxRedirectXml);
```

Information Exposure Through an Error Message

Ruta de consulta:
Java\Cx\Java Low Visibility\Information Exposure Through an Error Message Versión:3

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
OWASP Top 10 2013: A5-Security Misconfiguration
FISMA 2014: Configuration Management
NIST SP 800-53: SI-11 Error Handling (P2)
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 API: API3-Excessive Data Exposure
OWASP Top 10 2021: A4-Insecure Design

Descripción

Information Exposure Through an Error Message\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=25
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	1770	1783
Objeto	ex	printStackTrace

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	private void updateEstatusSolicitud(List<SolicitudVO> domis, String usuario) throws MitBusinessException {

```
....
1770.             }catch(Exception ex){
....
1783.                   ex.printStackTrace();
```

Information Exposure Through an Error Message\Ruta 2:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=26

Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	1770	1782
Objeto	ex	println

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java

Método: private void updateEstatusSolicitud(List<SolicitudVO> domis, String usuario) throws MitBusinessException {

```
....
1770.             }catch(Exception ex){
....
1782.                   System.out.println("ERROR UPDATE ESTATUS
SOLICITUD F4 :: " + ex.getMessage());
```

Information Exposure Through an Error Message\Ruta 3:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=27
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	495	497
Objeto	e	printStackTrace

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método: private void generarArchivoDomiF4(SolicitudFilter solicitudFilter,Date fecha,String archivo,Integer consecutivo, Short origenDomi) throws MitBusinessException{

```
....
495.                          } catch (Exception e) {
....
497.                                e.printStackTrace();
```

Information Exposure Through an Error Message\Ruta 4:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=28
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	495	496
Objeto	e	println

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	private void generarArchivoDomiF4(SolicitudFilter solicitudFilter,Date fecha,String archivo,Integer consecutivo, Short origenDomi) throws MitBusinessException{

```
....
495.                            } catch (Exception e) {
496.                                  System.out.println("OCURRIO UNA
EXCEPCIÓN DESPUES DE INSERTAR :" + e.getMessage());
```

Information Exposure Through an Error Message\Ruta 5:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=29
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	506	510
Objeto	ex	printStackTrace

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método	private void generarArchivoDomiF4(SolicitudFilter solicitudFilter,Date fecha,String archivo,Integer consecutivo, Short origenDomi) throws MitBusinessException{

```
....
506.                }catch(Exception ex){
....
510.                      ex.printStackTrace();
```

Information Exposure Through an Error Message\Ruta 6:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=30
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	506	509
Objeto	ex	println

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	private void generarArchivoDomiF4(SolicitudFilter solicitudFilter,Date fecha,String archivo,Integer consecutivo, Short origenDomi) throws MitBusinessException{

```
....
506.                }catch(Exception ex){
....
509.                      System.out.println( "ERROR MENSAJE      :" +
ex.getMessage());
```

Information Exposure Through an Error Message\Ruta 7:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=31
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Línea	864	866
Objeto	e	println

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método: private Boolean insertCargosF3(List<SolicitudVO> domis, Long idArchivo, String usuario, List<CatPrioridadesDiversificacionesVO> catDivPrioridades) {

```
....
864.                          } catch (Exception e) {
....
866.                                  System.out.println("ERROR AL
INSERTAR CARGO :: DETALLE  " + e.getMessage());
```

Information Exposure Through an Error Message\Ruta 8:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=32
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	938	943
Objeto	e	printStackTrace

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método: private String getFolioIdArchivo() {

```
....
938.              } catch (BusinessException e) {
....
943.                    e.printStackTrace();
```

Information Exposure Through an Error Message\Ruta 9:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=33
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	938	942
Objeto	e	println

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método: private String getFolioIdArchivo() {

```
....
938.              } catch (BusinessException e) {
....
942.                    System.out.println("ERROR MENSAJE    :" +
e.getMessage());
```

Information Exposure Through an Error Message\Ruta 10:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=34
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	1230	1238
Objeto	ex	printStackTrace

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método: private void updateEstatusSolicitud(List<SolicitudVO> domis, String usuario) throws MitBusinessException {

```
....
1230.             }catch(Exception ex){
....
1238.                   ex.printStackTrace();
```

Information Exposure Through an Error Message\Ruta 11:

Severidad	Bajas

Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=35
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	1230	1237
Objeto	ex	println

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	private void updateEstatusSolicitud(List<SolicitudVO> domis, String usuario) throws MitBusinessException {

```
....
1230.             }catch(Exception ex){
....
1237.                   System.out.println("ERROR UPDATE ESTATUS
SOLICITUD F4 :: " + ex.getMessage());
```

Information Exposure Through an Error Message\Ruta 12:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=36
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java
Línea	166	174
Objeto	e	printStackTrace

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java
Método	public void run() {

```
....
166.                    }catch( Exception e ) {
....
174.                            e.printStackTrace();
```

Information Exposure Through an Error Message\Ruta 13:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=37
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java
Línea	166	173
Objeto	e	println

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java

Método: public void run() {

```
....
166.                    }catch( Exception e ) {
....
173.                            System.out.println( "ERROR MENSAJE    :" +
e.getMessage());
```

Information Exposure Through an Error Message\Ruta 14:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=38
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/login.xhtml	source/mit-av-web/src/main/webapp/views/login.xhtml
Línea	44	44
Objeto	SPRING_SECURITY_LAST_EXCEPTION	CxJsfOutput

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/webapp/views/login.xhtml

Método: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

```
....
44.
      #{sessionScope.SPRING_SECURITY_LAST_EXCEPTION.message}
```

Client JQuery Deprecated Symbols

Ruta de consulta:
JavaScript\Cx\JavaScript Low Visibility\Client JQuery Deprecated Symbols Versión:3

Categorías

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A6-Vulnerable and Outdated Components

Descripción

Client JQuery Deprecated Symbols\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=11
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Línea	509	509
Objeto	bind	bind

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Método	function bind(b, el, opts) {

```
....
509.                          $(document).bind(events, opts, handler);
```

Client JQuery Deprecated Symbols\Ruta 2:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=12
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js

Línea	511	511
Objeto	unbind	unbind

Fragmento de código
Nombre del archivo source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Método function bind(b, el, opts) {

```
....
511.                            $(document).unbind(events, handler);
```

Client JQuery Deprecated Symbols\Ruta 3:

Severidad Bajas
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=13
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js
Línea	509	509
Objeto	bind	bind

Fragmento de código
Nombre del archivo source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js
Método function bind(b, el, opts) {

```
....
509.                            $(document).bind(events, opts, handler);
```

Client JQuery Deprecated Symbols\Ruta 4:

Severidad Bajas
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=14
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js
Línea	511	511
Objeto	unbind	unbind

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js
Método	function bind(b, el, opts) {

```
....
511.                            $(document).unbind(events, handler);
```

Client JQuery Deprecated Symbols\Ruta 5:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=15
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Línea	29	29
Objeto	isFunction	isFunction

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Método	function setup($) {

```
....
29.         var setExpr = $.isFunction(
document.createElement('div').style.setExpression );
```

Client JQuery Deprecated Symbols\Ruta 6:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=16
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js
Línea	29	29
Objeto	isFunction	isFunction

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/mensajeEmergente.js
Método	function setup($) {

```
....
29.         var setExpr = $.isFunction(
document.createElement('div').style.setExpression );
```

Client JQuery Deprecated Symbols\Ruta 7:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=17
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Línea	369	369
Objeto	bind	bind

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Método	}).bind("loaded", function (e,result) {

```
....
369.  }).bind("loaded", function (e,result) {
```

Client JQuery Deprecated Symbols\Ruta 8:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=18
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Línea	482	482
Objeto	delegate	delegate

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js

Método	$(document).ready(function () {

```
....
482.      $('body').delegate("a, button", 'click', function(event) {
```

Client JQuery Deprecated Symbols\Ruta 9:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=19
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Línea	139	139
Objeto	".azul-blanco tbody tr:even"	".azul-blanco tbody tr:even"

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Método	$(document).ready(function() {

```
....
139.      $(".azul-blanco tbody tr:even").css("background-color",
"#cfe8f7");
```

Client JQuery Deprecated Symbols\Ruta 10:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=20
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/componentes/menus.js	source/mit-av-web/src/main/webapp/core/static/tema/js/componentes/menus.js
Línea	21	21
Objeto	"ul.options-tabs li:first"	"ul.options-tabs li:first"

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/componentes/menus.js
Método	$(document).ready(function() {

```
....
21.      $("ul.options-tabs li:first").addClass("active").show();
```

Client JQuery Deprecated Symbols\Ruta 11:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=21
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/componentes/menus.js	source/mit-av-web/src/main/webapp/core/static/tema/js/componentes/menus.js
Línea	22	22
Objeto	".options-content li:first"	".options-content li:first"

Fragmento de código

Nombre del archivo source/mit-av-web/src/main/webapp/core/static/tema/js/componentes/menus.js

Método $(document).ready(function() {

```
....
22.      $(".options-content li:first").addClass("that-tab").show();
```

Client JQuery Deprecated Symbols\Ruta 12:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=22
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Línea	124	124
Objeto	"ul.options-tabs li:first"	"ul.options-tabs li:first"

Fragmento de código

Nombre del archivo source/mit-av-web/src/main/webapp/core/static/tema/js/script.js

Método $(document).ready(function() {

```
....
124.      $("ul.options-tabs li:first").addClass("active").show();
```

Client JQuery Deprecated Symbols\Ruta 13:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=23
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js	source/mit-av-web/src/main/webapp/core/static/tema/js/script.js
Línea	125	125
Objeto	".options-content li:first"	".options-content li:first"

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/webapp/core/static/tema/js/script.js

Método: $(document).ready(function() {

```
....
125.      $(".options-content li:first").addClass("that-tab").show();
```

Incorrect Permission Assignment For Critical Resources

Ruta de consulta:
Java\Cx\Java Low Visibility\Incorrect Permission Assignment For Critical Resources Versión:2

Categorías

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design

Descripción

Incorrect Permission Assignment For Critical Resources\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=39
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/Loc	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/Loc

	aFileTransferServiceImpl.java	aFileTransferServiceImpl.java
Línea	17	17
Objeto	f	f

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java
Método: public Boolean sendFile(StringBuffer sb, String path) throws IOException {

```
....
17.         File f = new File(path);
```

Incorrect Permission Assignment For Critical Resources\Ruta 2:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=40
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java
Línea	68	68
Objeto	archivo	archivo

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java
Método: public ReporteVO generarArchivoCifrasGenerales(List cifrasControlReporteVO) throws BusinessException {

```
....
68.         File archivo = new File(CIFRAS_CONTROL_REPORT_JRXML);
```

Incorrect Permission Assignment For Critical Resources\Ruta 3:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=41
Estatus	Recurrente

	Origen	Destino

Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java
Línea	74	74
Objeto	archivoSalida	archivoSalida

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java

Método: public ReporteVO generarArchivoCifrasGenerales(List cifrasControlReporteVO) throws BusinessException {

```
....
74.         File archivoSalida = new
File(CIFRAS_CONTROL_REPORT_FILE_NAME_PREFIX+""+CIFRAS_CONTROL_REPORT_FIL
E_NAME_EXTENSION);
```

Incorrect Permission Assignment For Critical Resources\Ruta 4:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=42
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/CifrasGeneralesServiceIT.java	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/CifrasGeneralesServiceIT.java
Línea	32	32
Objeto	archivo	archivo

Fragmento de código

Nombre del archivo: source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/CifrasGeneralesServiceIT.java

Método: public void consultarIT() throws BusinessException {

```
....
32.                 File archivo = new
File("/main/resources/reports/cifrasControl.jrxml");
```

Incorrect Permission Assignment For Critical Resources\Ruta 5:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid

línea	=2733&pathid=43
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/FileNetServiceIT.java	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/FileNetServiceIT.java
Línea	69	69
Objeto	file	file

Fragmento de código

Nombre del archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/FileNetServiceIT.java
Método	private static byte[] readBytesFromFile(String filePath) {

```
....
69.               File file = new File(filePath);
```

Incorrect Permission Assignment For Critical Resources\Ruta 6:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=44
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Línea	492	492
Objeto	rutaOut	rutaOut

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Método	private void copiarArchivo(DepositoArchivoBean depositoArchivoBean)

```
....
492.                    File rutaOut=new File(ruta);
```

Incorrect Permission Assignment For Critical Resources\Ruta 7:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=45

Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Línea	500	500
Objeto	fileOut	fileOut

Fragmento de código
Nombre del archivo source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Método private void copiarArchivo(DepositoArchivoBean depositoArchivoBean)

```
....
500.                                    File fileOut=new
File(ruta,fileName);
```

Incorrect Permission Assignment For Critical Resources\Ruta 8:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=46
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	436	436
Objeto	fileWriter	fileWriter

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método public static Boolean generaArchivoCsv(String texto, String nombreCsv, String ruta) throws Exception {

```
....
436.                    fileWriter = new FileWriter(ruta+nombreCsv);
```

Incorrect Permission Assignment For Critical Resources\Ruta 9:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=47
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	447	447
Objeto	fileWriter	fileWriter

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método public static Boolean generaArchivoCsv(String texto, String nombreCsv, String ruta) throws Exception {

```
....
447.                        fileWriter.flush();
```

Incorrect Permission Assignment For Critical Resources\Ruta 10:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=48
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	448	448
Objeto	fileWriter	fileWriter

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método public static Boolean generaArchivoCsv(String texto, String nombreCsv, String ruta) throws Exception {

```
....
448.                        fileWriter.close();
```

Incorrect Permission Assignment For Critical Resources\Ruta 11:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=49
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java
Línea	33	33
Objeto	fos	fos

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java

Método: public Boolean sendFile(DataFileBean dfb) throws IOException {

```
....
33.                     FileOutputStream fos = new
FileOutputStream(dfb.getFile());
```

Incorrect Permission Assignment For Critical Resources\Ruta 12:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=50
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	433	433
Objeto	fileWriter	fileWriter

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java

Método: public static Boolean generaArchivoCsv(String texto, String nombreCsv, String ruta) throws Exception {

```
....
433.              FileWriter fileWriter = null;
```

Race Condition Format Flaw

Ruta de consulta:
Java\Cx\Java Low Visibility\Race Condition Format Flaw Versión:1

Categorías

FISMA 2014: System And Information Integrity
NIST SP 800-53: AC-3 Access Enforcement (P1)

OWASP Top 10 2021: A4-Insecure Design

Descripción

Race Condition Format Flaw\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=60
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	347	347
Objeto	format	format

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java

Método: public static String parseString(String pattern, Object object) {

```
....
347.                return new SimpleDateFormat(pattern).format((Date)
object);
```

Race Condition Format Flaw\Ruta 2:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=61
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	307	307
Objeto	parse	parse

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java

Método: public DomiParameterMapFilter getDomiParameterMapFilter(PeticionesDomiFilter petDomiFilter) throws Exception {

```
....
307.                    map.setFechaFin( new
SimpleDateFormat("dd/MM/yyyy").parse(petDomiFilter.getFechaFin()) );
```

Race Condition Format Flaw\Ruta 3:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=62
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	308	308
Objeto	parse	parse

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	public DomiParameterMapFilter getDomiParameterMapFilter(PeticionesDomiFilter petDomiFilter) throws Exception {

```
....
308.                    map.setFechaInicio( new
SimpleDateFormat("dd/MM/yyyy").parse(petDomiFilter.getFechaInicio()) );
```

Race Condition Format Flaw\Ruta 4:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=63
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	350	350
Objeto	format	format

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método	public static String parseString(String pattern, Object object) {

```
....
350.                return new DecimalFormat(pattern).format((Number)
object);
```

Race Condition Format Flaw\Ruta 5:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=64
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/OrdenSpeiController.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/OrdenSpeiController.java
Línea	104	104
Objeto	format	format

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/OrdenSpeiController.java
Método	public Boolean guardarOrdenSpei(ClienteOrdenSpeiBean clienteSpei, boolean monto) {

```
....
104.                                    div.setPorcentaje(new Short(new
DecimalFormat("#").format(new
Double(fondo.getValor().replaceAll("\\$","").replaceAll("\\%","").replac
eAll("\\,", ""))))));
```

Race Condition Format Flaw\Ruta 6:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=65
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	353	353
Objeto	format	format

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método	public static String parseString(String pattern, Object object) {

```
....
353.            return MessageFormat.format(pattern, object);
```

Serializable Class Containing Sensitive Data

Ruta de consulta:
Java\Cx\Java Low Visibility\Serializable Class Containing Sensitive Data Versión:2

Categorías

OWASP Top 10 2013: A6-Sensitive Data Exposure
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A4-Insecure Design

Descripción

Serializable Class Containing Sensitive Data\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=56
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/traspasos/DetalleMesDetalleBean.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/traspasos/DetalleMesDetalleBean.java
Línea	18	6
Objeto	recursosAcreditados	DetalleMesDetalleBean

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/traspasos/DetalleMesDetalleBean.java
Método	private BigDecimal recursosAcreditados;

```
....
18.   private BigDecimal recursosAcreditados;
```

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/traspasos/DetalleMesDetalleBean.java
Método	public class DetalleMesDetalleBean implements Serializable

```
....
6.  public class DetalleMesDetalleBean  implements Serializable
```

Serializable Class Containing Sensitive Data\Ruta 2:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=57
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/traspasos/InversionDomiciliacionView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/traspasos/InversionDomiciliacionView.java
Línea	37	23
Objeto	porAcreditar	InversionDomiciliacionView

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/traspasos/InversionDomiciliacionView.java
Método	private InversionDomiTraspasosBean porAcreditar;

```
....
37.   private InversionDomiTraspasosBean porAcreditar;
```

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/traspasos/InversionDomiciliacionView.java
Método	@ManagedBean(name = "inversionDomiciliacionView")

```
....
23.  @ManagedBean(name = "inversionDomiciliacionView")
```

Serializable Class Containing Sensitive Data\Ruta 3:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=58
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/we	source/mit-av-web/src/main/java/mx/profuturo/nci/we

	b/views/traspasos/InversionDomiciliacionView.java	b/views/traspasos/InversionDomiciliacionView.java
Línea	40	23
Objeto	acreditados	InversionDomiciliacionView

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/traspasos/InversionDomiciliacionView.java

Método: private InversionDomiTraspasosBean acreditados;

```
....
40.   private InversionDomiTraspasosBean acreditados;
```

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/traspasos/InversionDomiciliacionView.java

Método: @ManagedBean(name = "inversionDomiciliacionView")

```
....
23.  @ManagedBean(name = "inversionDomiciliacionView")
```

Client Password In Comment

Ruta de consulta:
JavaScript\Cx\JavaScript Low Visibility\Client Password In Comment Versión:2

Categorías

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A4-Insecure Design

Descripción

Client Password In Comment\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=24
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/traspasos.js	source/mit-av-web/src/main/webapp/core/static/tema/js/traspasos.js
Línea	77	77
Objeto	pass"	pass"

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/traspasos.js
Método	validator2.showErrors({"login-pass": "La contraseña proporcionada no coincide con el correo electrónico, favor de revisar la información e intentarlo de nuevo."});

```
....
77.            validator2.showErrors({"login-pass": "La
contrase&ntilde;a proporcionada no coincide con el correo
electr&oacute;nico, favor de revisar la informaci&oacute;n e intentarlo
de nuevo."});
```

Missing CSP Header

Ruta de consulta:
JavaScript\Cx\JavaScript Server Side Vulnerabilities\Missing CSP Header Versión:2

Categorías

OWASP Top 10 2021: A7-Identification and Authentication Failures

Descripción

Missing CSP Header\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=51
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Línea	475	475
Objeto	appendChild	appendChild

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/static/tema/js/BlockUI.js
Método	function reset(els,data,opts,el) {

```
....
475.                                  data.parent.appendChild(data.el);
```

Log Forging

Ruta de consulta:
Java\Cx\Java Low Visibility\Log Forging Versión:1

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
FISMA 2014: System And Information Integrity

NIST SP 800-53: AU-9 Protection of Audit Information (P1)
OWASP Top 10 2017: A1-Injection
OWASP Mobile Top 10 2016: M7-Client Code Quality
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures

Descripción

Log Forging\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=52
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/WebServiceAuthenticationManagerImpl.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/WebServiceAuthenticationManagerImpl.java
Línea	48	61
Objeto	getName	debug

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/WebServiceAuthenticationManagerImpl.java
Método	public Authentication authenticate(Authentication authentication)

```
....
48.         String username = authentication.getName();
....
61.                     LOGGER.debug("El usuario " + username + " entro
a la aplicacion");
```

Missing Content Security Policy

Ruta de consulta:
Java\Cx\Java Low Visibility\Missing Content Security Policy Versión:1

Categorías

OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A7-Identification and Authentication Failures

Descripción

Missing Content Security Policy\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=53
Estatus	Recurrente

	Origen	Destino

Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java
Línea	45	45
Objeto	printStackTrace	printStackTrace

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/LocaFileTransferServiceImpl.java
Método public Boolean sendFile(DataFileBean dfb) throws IOException {

```
....
45.                 e.printStackTrace();
```

Missing X Frame Options

Ruta de consulta:
Java\Cx\Java Low Visibility\Missing X Frame Options Versión:3

Categorías

NIST SP 800-53: SC-18 Mobile Code (P2)
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design

Descripción

Missing X Frame Options\Ruta 1:

Severidad Bajas
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=54
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/WEB-INF/web.xml	source/mit-av-web/src/main/webapp/WEB-INF/web.xml
Línea	1	1
Objeto	CxXmlConfigClass1190789717	CxXmlConfigClass1190789717

Fragmento de código
Nombre del archivo source/mit-av-web/src/main/webapp/WEB-INF/web.xml
Método <?xml version="1.0" encoding="UTF-8"?>

```
....
1.  <?xml version="1.0" encoding="UTF-8"?>
```

Potential ReDoS

Ruta de consulta:
Java\Cx\Java Low Visibility\Potential ReDoS Versión:1

Categorías

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

Descripción

Potential ReDoS\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=55
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/IdentificarClienteView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/IdentificarClienteView.java
Línea	706	706
Objeto	"""([0-9]*[.]?[0-9]*)"""	"""([0-9]*[.]?[0-9]*)"""

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/IdentificarClienteView.java
Método	public void cleanDiversificacionValues(){

```
....
706.                    this.regexMontoPorcentaje = "'([0-9]*[.]?[0-9]*)'";
```

Spring defaultHtmlEscape Not True

Ruta de consulta:
Java\Cx\Java Low Visibility\Spring defaultHtmlEscape Not True Versión:0

Categorías

OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design

Descripción

Spring defaultHtmlEscape Not True\Ruta 1:

Severidad	Bajas
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=59
Estatus	Recurrente

	Origen	Destino

Archivo	source/mit-av-web/src/main/webapp/WEB-INF/web.xml	source/mit-av-web/src/main/webapp/WEB-INF/web.xml
Línea	1	1
Objeto	CxXmlConfigClass1190789717	CxXmlConfigClass1190789717

Fragmento de código
Nombre del archivo source/mit-av-web/src/main/webapp/WEB-INF/web.xml
Método <?xml version="1.0" encoding="UTF-8"?>

```
....
1.  <?xml version="1.0" encoding="UTF-8"?>
```

Exposure of Resource to Wrong Sphere

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Exposure of Resource to Wrong Sphere Versión:2

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.8 - Improper access control
OWASP Top 10 2013: A7-Missing Function Level Access Control
OWASP Top 10 2017: A5-Broken Access Control
OWASP Top 10 2021: A1-Broken Access Control

Descripción

Exposure of Resource to Wrong Sphere\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=66
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/test/java/CatalogoServiceIT.java	source/mit-av-web/src/test/java/CatalogoServiceIT.java
Línea	26	26
Objeto	bancosService	bancosService

Fragmento de código
Nombre del archivo source/mit-av-web/src/test/java/CatalogoServiceIT.java
Método @Autowired

```
....
26.   @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 2:

Severidad	Información

Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=67
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/bean/RespGeneracionArchivosDomi.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/bean/RespGeneracionArchivosDomi.java
Línea	4	4
Objeto	idArchivo	idArchivo

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/bean/RespGeneracionArchivosDomi.java
Método	public String idArchivo;

```
....
4.    public String idArchivo;
```

Exposure of Resource to Wrong Sphere\Ruta 3:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=68
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/bean/RespGeneracionArchivosDomi.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/bean/RespGeneracionArchivosDomi.java
Línea	5	5
Objeto	nombreArchivo	nombreArchivo

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/bean/RespGeneracionArchivosDomi.java
Método	public String nombreArchivo;

```
....
5.    public String nombreArchivo;
```

Exposure of Resource to Wrong Sphere\Ruta 4:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=69
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/cliente/service/impl/WSCOperacionesLdapServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/cliente/service/impl/WSCOperacionesLdapServiceImpl.java
Línea	24	24
Objeto	wsPortTypeFactory	wsPortTypeFactory

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/cliente/service/impl/WSCOperacionesLdapServiceImpl.java
Método	@Autowired WSPortTypeFactory wsPortTypeFactory;

```
....
24.    @Autowired WSPortTypeFactory wsPortTypeFactory;
```

Exposure of Resource to Wrong Sphere\Ruta 5:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=70
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/handler/CurrencyTypeHandler.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/handler/CurrencyTypeHandler.java
Línea	12	12
Objeto	df	df

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/handler/CurrencyTypeHandler.java
Método	DecimalFormat df = new DecimalFormat();

```
....
12.    DecimalFormat df = new DecimalFormat();
```

Exposure of Resource to Wrong Sphere\Ruta 6:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=71
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java
Línea	60	60
Objeto	basicReportService	basicReportService

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/CifrasControlReportServiceImpl.java
Método	@Autowired

```
....
60.      @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 7:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=72
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Línea	40	40
Objeto	reportService	reportService

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Método	@Autowired IBasicReportService reportService;

```
....
40.   @Autowired IBasicReportService reportService;
```

Exposure of Resource to Wrong Sphere\Ruta 8:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=73
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/AforeMovilServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/AforeMovilServiceImpl.java
Línea	21	21
Objeto	aforeMovilPersistence	aforeMovilPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/AforeMovilServiceImpl.java
Método	@Autowired

```
....
21.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 9:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=74
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ArchivoGeneradoServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ArchivoGeneradoServiceImpl.java
Línea	16	16
Objeto	archivoDomiPersistence	archivoDomiPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ArchivoGeneradoServiceImpl.java
Método	@Autowired

```
....
16.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 10:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=75
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ArchivoServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ArchivoServiceImpl.java
Línea	27	27
Objeto	archivoPersistence	archivoPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ArchivoServiceImpl.java
Método	@Autowired

```
....
27.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 11:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=76
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BancosServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BancosServiceImpl.java
Línea	32	32
Objeto	bancoPersistence	bancoPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BancosServiceImpl.java

Método	@Autowired

```
....
32.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 12:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=77
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BancosServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BancosServiceImpl.java
Línea	35	35
Objeto	catalogosService	catalogosService

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BancosServiceImpl.java
Método	@Autowired

```
....
35.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 13:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=78
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BitacoraServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BitacoraServiceImpl.java
Línea	24	24
Objeto	bitacoraPersistence	bitacoraPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/BitacoraServiceImpl.java
Método	@Autowired BitacoraProcesoPersistence bitacoraPersistence;

```
....
24.   @Autowired BitacoraProcesoPersistence bitacoraPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 14:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=79
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CalendarioServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CalendarioServiceImpl.java
Línea	17	17
Objeto	calendarioPersistence	calendarioPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CalendarioServiceImpl.java
Método	@Autowired CalendarioPersistence calendarioPersistence;

```
....
17.   @Autowired CalendarioPersistence calendarioPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 15:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=80
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosConfiguracionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosConfiguracionServiceImpl.java
Línea	22	22
Objeto	catalogoConfiguracionPersistence	catalogoConfiguracionPersistence

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosConfiguracionServiceImpl.java
Método	@Autowired

```
....
22.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 16:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=81
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosServiceImpl.java
Línea	31	31
Objeto	catalogoPersistence	catalogoPersistence

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosServiceImpl.java
Método	@Autowired

```
....
31.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 17:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=82
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosServiceImpl.java
Línea	34	34
Objeto	wsPortTypeFactory	wsPortTypeFactory

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CatalogosServiceImpl.java
Método	@Autowired

```
....
34.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 18:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=83
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasControlClienteImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasControlClienteImpl.java
Línea	30	30
Objeto	cifrasControlClientePersistence	cifrasControlClientePersistence

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasControlClienteImpl.java
Método	@Autowired

```
....
30.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 19:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=84
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasGeneralesImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasGeneralesImpl.java
Línea	32	32

Objeto	cifrasGeneralesPersistence	cifrasGeneralesPersistence

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasGeneralesImpl.java
Método @Autowired

```
....
32.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 20:

Severidad Información
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=85
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasGeneralesImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasGeneralesImpl.java
Línea	35	35
Objeto	cifrasControlReportService	cifrasControlReportService

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasGeneralesImpl.java
Método @Autowired

```
....
35.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 21:

Severidad Información
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=86
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasLiquidacionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasLiquidacionServiceImpl.java

Línea	27	27
Objeto	cifrasLiquidacionPersistence	cifrasLiquidacionPersistence

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasLiquidacionServiceImpl.java
Método: @Autowired

```
....
27.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 22:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=87
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Línea	64	64
Objeto	conciliacionPersistence	conciliacionPersistence

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Método: @Autowired

```
....
64.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 23:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=88
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServic	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServic

	eImpl.java	eImpl.java
Línea	67	67
Objeto	sequencesManagerPersistence	sequencesManagerPersistence

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java

Método: @Autowired

```
....
67.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 24:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=89
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Línea	70	70
Objeto	diversificacionConciliacionPersistence	diversificacionConciliacionPersistence

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java

Método: @Autowired

```
....
70.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 25:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=90
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-	source/mit-av-

	business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java	business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Línea	73	73
Objeto	BancosService	BancosService

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java

Método: @Autowired

```
....
73.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 26:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=91

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Línea	76	76
Objeto	sumConciliacionService	sumConciliacionService

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java

Método: @Autowired

```
....
76.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 27:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=92

Estatus: Recurrente

	Origen	Destino

Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Línea	79	79
Objeto	ordenesService	ordenesService

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConciliacionServiceImpl.java
Método: @Autowired

```
....
79.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 28:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=93
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfigIntentosCargaApoVolImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfigIntentosCargaApoVolImpl.java
Línea	19	19
Objeto	configIntentosCargaApoVolPersistence	configIntentosCargaApoVolPersistence

Fragmento de código
Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfigIntentosCargaApoVolImpl.java
Método: @Autowired

```
....
19.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 29:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=94
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfiguracionPermisoSeccionServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfiguracionPermisoSeccionServiceImpl.java
Línea	17	17
Objeto	tfafogralConfigPermSeccionRepository	tfafogralConfigPermSeccionRepository

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfiguracionPermisoSeccionServiceImpl.java

Método: @Autowired ConfPermisoSeccionPersistence tfafogralConfigPermSeccionRepository;

```
....
17.   @Autowired ConfPermisoSeccionPersistence
tfafogralConfigPermSeccionRepository;
```

Exposure of Resource to Wrong Sphere\Ruta 30:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=95

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfiguracionSubprocesoOrigenServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfiguracionSubprocesoOrigenServiceImpl.java
Línea	23	23
Objeto	configSubprocesoOrigenPersistence	configSubprocesoOrigenPersistence

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConfiguracionSubprocesoOrigenServiceImpl.java

Método: @Autowired

```
....
23.   @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 31:

Severidad: Información

Estado del resultado: Para verificar

Resultados en: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid

línea	=2733&pathid=96
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConsultasBaseServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConsultasBaseServiceImpl.java
Línea	14	14
Objeto	generaFolioPersistence	generaFolioPersistence

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/ConsultasBaseServiceImpl.java
Método	@Autowired

```
....
14.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 32:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=97
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	122	122
Objeto	domisBitacoraPersistence	domisBitacoraPersistence

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
122.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 33:

Severidad	Información
Estado del resultado	Para verificar

Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=98
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	125	125
Objeto	domiciliacionesPersistence	domiciliacionesPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
125.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 34:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=99
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	128	128
Objeto	archivoDomiPersistence	archivoDomiPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
128.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 35:

Severidad	Información
Estado del	Para verificar

resultado	
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=100
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	131	131
Objeto	solicitudPersistence	solicitudPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
131.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 36:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=101
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	134	134
Objeto	catalogosService	catalogosService

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
134.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 37:

Severidad	Información

Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=102
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	137	137
Objeto	catalogoPersistence	catalogoPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
137.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 38:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=103
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	140	140
Objeto	detalleArchivoDomiPersistence	detalleArchivoDomiPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
140.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 39:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=104
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	143	143
Objeto	fileGeneratorService	fileGeneratorService

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
143.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 40:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=105
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	146	146
Objeto	fileTransferService	fileTransferService

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	@Autowired

```
....
146.        @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 41:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=106
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiTraspasosServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiTraspasosServiceImpl.java
Línea	34	34
Objeto	solicitudPersistence	solicitudPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiTraspasosServiceImpl.java
Método	@Autowired

```
....
34.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 42:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=107
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiTraspasosServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiTraspasosServiceImpl.java
Línea	37	37
Objeto	solicitudService	solicitudService

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiTraspasosServiceImpl.java
Método	@Autowired ISolicitudService solicitudService;

```
....
37.    @Autowired ISolicitudService solicitudService;
```

Exposure of Resource to Wrong Sphere\Ruta 43:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=108
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/FilenetServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/FilenetServiceImpl.java
Línea	21	21
Objeto	wsPortTypeFactory	wsPortTypeFactory

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/FilenetServiceImpl.java
Método	@Autowired

```
....
21.    @Autowired
```

Exposure of Resource to Wrong Sphere\Ruta 44:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=109
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	119	119
Objeto	solicitudPersistence	solicitudPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	@Autowired SolicitudPersistence solicitudPersistence;

```
....
119.        @Autowired SolicitudPersistence solicitudPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 45:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=110
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	120	120
Objeto	archivoDomiPersistence	archivoDomiPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	@Autowired ArchivoDomiPersistence archivoDomiPersistence;

```
....
120.        @Autowired ArchivoDomiPersistence archivoDomiPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 46:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=111
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	121	121
Objeto	detalleArchivoDomiPersistence	detalleArchivoDomiPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método	@Autowired DetalleArchivoDomiPersistence detalleArchivoDomiPersistence;

```
....
121.        @Autowired DetalleArchivoDomiPersistence
detalleArchivoDomiPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 47:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=112
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	122	122
Objeto	catalogoPersistence	catalogoPersistence

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	@Autowired CatalogoPersistence catalogoPersistence;

```
....
122.        @Autowired CatalogoPersistence catalogoPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 48:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=113
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	123	123
Objeto	cargoPersistence	cargoPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	@Autowired CargoPersistence cargoPersistence;

```
....
123.        @Autowired CargoPersistence cargoPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 49:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=114
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	124	124
Objeto	diversificacionPersistence	diversificacionPersistence

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	@Autowired DiversificacionPersistence diversificacionPersistence;

```
....
124.        @Autowired DiversificacionPersistence
diversificacionPersistence;
```

Exposure of Resource to Wrong Sphere\Ruta 50:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=115
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	126	126
Objeto	catalogosService	catalogosService

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	@Autowired ICatalogosService catalogosService;

```
....
126.        @Autowired ICatalogosService catalogosService;
```

Insufficient Logging of Exceptions

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Insufficient Logging of Exceptions Versión:1

Categorías

OWASP Top 10 API: API10-Insufficient Logging and Monitoring
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures

Descripción

Insufficient Logging of Exceptions\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=307
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/FilesGeneratorServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/FilesGeneratorServiceImpl.java
Línea	70	70
Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/file/generator/service/impl/FilesGeneratorServiceImpl.java
Método	public <T> StringWriter generateFileF4(T record) {

```
....
70.         }catch( Exception e ) {
```

Insufficient Logging of Exceptions\Ruta 2:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=308
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Línea	99	99
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java

Método: public ReporteVO generaReporteDetalleDomiliacion(List<DiversificacionesDataReportBean> diverReportBean,

```
....
99.         }catch (JRException e){
```

Insufficient Logging of Exceptions\Ruta 3:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=309
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Línea	101	101
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java

Método: public ReporteVO generaReporteDetalleDomiliacion(List<DiversificacionesDataReportBean> diverReportBean,

```
....
101.             }catch (Exception e){
```

Insufficient Logging of Exceptions\Ruta 4:

Severidad	Información

Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=310
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Línea	138	138
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Método	public ReporteVO generaReporteDepositosAforeMovil(List<ConsultaAforeMovilDataReportBean> aforeMovilReportBean)

```
....
138.                }catch (JRException e){
```

Insufficient Logging of Exceptions\Ruta 5:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=311
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Línea	140	140
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/report/impl/ReportesServiceImpl.java
Método	public ReporteVO generaReporteDepositosAforeMovil(List<ConsultaAforeMovilDataReportBean> aforeMovilReportBean)

```
....
140.              }catch (Exception e){
```

Insufficient Logging of Exceptions\Ruta 6:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=312
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasControlClienteImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasControlClienteImpl.java
Línea	74	74
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/CifrasControlClienteImpl.java
Método	public boolean actializarEstatus(String clave, int estatus) throws MitBusinessException {

```
....
74.          }catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 7:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=313
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	650	650
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	public String generarArchivoDomiF4Mant (SolicitudFilter solicitudFilter

```
....
650.                    } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 8:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=314
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Línea	1134	1134
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/DomiciliacionesServiceImpl.java
Método	public Boolean isNumber(String str) {

```
....
1134.             } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 9:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=315
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	178	178
Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	public List<GeneracionArchivoDomiVO> generarArchivosDomi(DomiParameterMapFilter filters) throws MitBusinessException {

```
....
178.                            }catch(Exception e){
```

Insufficient Logging of Exceptions\Ruta 10:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=316
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Línea	381	381
Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java
Método	private void generarArchivoDomi(SolicitudFilter solicitudFilter,Date fecha,String archivo,Integer consecutivo, Short origenDomi) throws MitBusinessException{

```
....
381.                            } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 11:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=317
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Línea	1011	1011
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/GeneracionArchivoDomiServiceImpl.java

Método: private CargoVO convertSolicitudToCargoF4(SolicitudVO s, String idCargo, Long idArchivo, String usuario) {

```
....
1011.             }catch( Exception e ) {
```

Insufficient Logging of Exceptions\Ruta 12:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=318

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/SolicitudServiceImpl.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/SolicitudServiceImpl.java
Línea	195	195
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/service/impl/SolicitudServiceImpl.java

Método: public Date getProximaFechaDeCargo(SolicitudVO solVO) throws MitBusinessException {

```
....
195.              }catch(Exception e){
```

Insufficient Logging of Exceptions\Ruta 13:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=319

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-	source/mit-av-

	business/src/main/java/mx/profuturo/nci/business/util/Constantes.java	business/src/main/java/mx/profuturo/nci/business/util/Constantes.java
Línea	135	135
Objeto	catch	catch

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Constantes.java
Método private static String getServerValue(WebSphereNamespace key){

```
....
135.              } catch (BusinessException e) {
```

Insufficient Logging of Exceptions\Ruta 14:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=320
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/ConsumeWS.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/ConsumeWS.java
Línea	147	147
Objeto	catch	catch

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/ConsumeWS.java
Método private CloseableHttpClient generarHtppCliet( ){

```
....
147.              }catch( Exception e ) {
```

Insufficient Logging of Exceptions\Ruta 15:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=321
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java

Línea	276	276
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/Hilo.java

Método: private CargoVO convertSolicitudToCargoF4(SolicitudVO s, String idCargo, Long idArchivo, String usuario) {

```
....
276.                    }catch( Exception e ) {
```

Insufficient Logging of Exceptions\Ruta 16:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=322
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/NameSpaceBindingProvider.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/NameSpaceBindingProvider.java
Línea	23	23
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/NameSpaceBindingProvider.java

Método: public static String getValue(WebSphereNamespace nameSpace)throws BusinessException

```
....
23.                catch(Exception e)
```

Insufficient Logging of Exceptions\Ruta 17:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=323
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci	source/mit-av-business/src/main/java/mx/profuturo/nci

	/business/util/UtilMethod.java	/business/util/UtilMethod.java
Línea	147	147
Objeto	catch	catch

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilMethod.java
Método public static Long extractNumber(String number) {

```
....
147.              }catch(Exception e) {
```

Insufficient Logging of Exceptions\Ruta 18:

Severidad Información
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=324
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	383	383
Objeto	catch	catch

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método public static boolean validarFechaPorFormato(String fecha, String formato) {

```
....
383.                } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 19:

Severidad Información
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=325
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Línea	417	417

Objeto	catch	catch

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/java/mx/profuturo/nci/business/util/UtilValidate.java
Método public static boolean validarFechaPorFormatoF4(String fecha, String formato) {

```
....
417.              } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 20:

Severidad Información
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=326
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/comun/catalogo/CatalogoComunService.java	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/comun/catalogo/CatalogoComunService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código
Nombre del archivo source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/comun/catalogo/CatalogoComunService.java
Método static {

```
....
35.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 21:

Severidad Información
Estado del resultado Para verificar
Resultados en línea http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=327
Estatus Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ControlAccesoSSOService.java	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ControlAccesoSSOService.java
Línea	35	35

Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ControlAccesoSSOService.java
Método	static {

```
....
35.          } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 22:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=328
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/profuturo/ldap/operacionesldap/OperacionesLdapService.java	source/mit-av-business/src/main/wsc/java/mx/profuturo/ldap/operacionesldap/OperacionesLdapService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/wsc/java/mx/profuturo/ldap/operacionesldap/OperacionesLdapService.java
Método	static {

```
....
35.          } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 23:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=329
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/profuturo/nci/ws/webservice/catalogo/impl/ICatalogoSoapWSService.java	source/mit-av-business/src/main/wsc/java/mx/profuturo/nci/ws/webservice/catalogo/impl/ICatalogoSoapWSService.java

Línea	36	36
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/mx/profuturo/nci/ws/webservice/catalogo/impl/ICatalogoSoapWSService.java

Método: static {

```
....
36.          } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 24:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=330
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/profuturo/nci/ws/webservice/indicadores/impl/IIndicadoresSoapWSService.java	source/mit-av-business/src/main/wsc/java/mx/profuturo/nci/ws/webservice/indicadores/impl/IIndicadoresSoapWSService.java
Línea	37	37
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/mx/profuturo/nci/ws/webservice/indicadores/impl/IIndicadoresSoapWSService.java

Método: static {

```
....
37.          } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 25:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=331
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/conciliacion/conciliacionservi	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/conciliacion/conciliacionservi

	ce/v1/ConciliacionService.java	ce/v1/ConciliacionService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/conciliacion/conciliacionservice/v1/ConciliacionService.java

Método: static {

```
....
35.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 26:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=332
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/domiciliaciones/domiciliacionservice/v1/DomiciliacionService.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/domiciliaciones/domiciliacionservice/v1/DomiciliacionService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/domiciliaciones/domiciliacionservice/v1/DomiciliacionService.java

Método: static {

```
....
35.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 27:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=333
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-	source/mit-av-

	business/src/main/wsc/java/profuturo/mx/iib/apovol/filenet/filenetservice/v1/FileNetService.java	business/src/main/wsc/java/profuturo/mx/iib/apovol/filenet/filenetservice/v1/FileNetService.java
Línea	37	37
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/apovol/filenet/filenetservice/v1/FileNetService.java

Método: static {

```
....
37.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 28:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=334
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/certif/certificaciones/cuentascertificadasservice/v1/CuentasCertificadasService.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/certif/certificaciones/cuentascertificadasservice/v1/CuentasCertificadasService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/certif/certificaciones/cuentascertificadasservice/v1/CuentasCertificadasService.java

Método: static {

```
....
35.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 29:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=335
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/bitacoraprocesos/folioservice/v1/FolioService.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/bitacoraprocesos/folioservice/v1/FolioService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/bitacoraprocesos/folioservice/v1/FolioService.java

Método: static {

```
....
35.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 30:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=336

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/ClienteService.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/ClienteService.java
Línea	38	38
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/ClienteService.java

Método: static {

```
....
38.           }  catch (Exception ex) {
```

Insufficient Logging of Exceptions\Ruta 31:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=337

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/matrizconvivencia/matrizconvivenciaservice/v1/MatrizConvivenciaService.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/matrizconvivencia/matrizconvivenciaservice/v1/MatrizConvivenciaService.java
Línea	35	35
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/matrizconvivencia/matrizconvivenciaservice/v1/MatrizConvivenciaService.java

Método: static {

```
....
35.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 32:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=338

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/EnvioCorreoService.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/EnvioCorreoService.java
Línea	37	37
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/EnvioCorreoService.java

Método: static {

```
....
37.           } catch (Exception e) {
```

Insufficient Logging of Exceptions\Ruta 33:

Severidad: Información

Estado del resultado: Para verificar

Resultados en: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid

línea	=2733&pathid=339
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/AltaSolicitudServiceIT.java	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/AltaSolicitudServiceIT.java
Línea	71	71
Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/AltaSolicitudServiceIT.java
Método	public void consultarIT()

```
....
71.         catch (MitBusinessException ex)
```

Insufficient Logging of Exceptions\Ruta 34:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=340
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/CifrasGeneralesServiceIT.java	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/CifrasGeneralesServiceIT.java
Línea	37	37
Objeto	catch	catch

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/CifrasGeneralesServiceIT.java
Método	public void consultarIT() throws BusinessException {

```
....
37.         } catch (MitBusinessException ex) {
```

Insufficient Logging of Exceptions\Ruta 35:

Severidad	Información
Estado del resultado	Para verificar

Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=341
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/SumConciliacionServiceIT.java	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/SumConciliacionServiceIT.java
Línea	46	46
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-business/src/test/java/mx/profuturo/nci/business/service/test/SumConciliacionServiceIT.java
Método	public void actualizarIT() throws BusinessException {

```
....
46.         } catch (MitBusinessException ex) {
```

Insufficient Logging of Exceptions\Ruta 36:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=342
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Línea	109	109
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Método	public void inicializar()

```
....
109.             catch(MitBusinessException ex)
```

Insufficient Logging of Exceptions\Ruta 37:

Severidad	Información
Estado del resultado	Para verificar
Resultados en	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid

línea	=2733&pathid=343
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Línea	381	381
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/controller/DepositoArchivoView.java
Método	private void validaNombreByExpresioRegular(DepositoArchivoBean depositoArchivoBean, ConfigSubprocesoOrigenBean configSubprocesoOrigenBean)

```
....
381.                                catch (ParseException e)
```

Insufficient Logging of Exceptions\Ruta 38:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=344
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java
Línea	112	112
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java
Método	public List<Profuturo_CIFVo> send2CIF(List<Profuturo_CIFVo> vos,String usuario) throws MitBusinessException {

```
....
112.                    } catch(Exception ex){
```

Insufficient Logging of Exceptions\Ruta 39:

Severidad	Información
Estado del	Para verificar

resultado	
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=345
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java
Línea	223	223
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java

Método: public void generaIdItem(NCI_CIFDataBean bean) {

```
....
223.                    } catch (MitBusinessException e) {
```

Insufficient Logging of Exceptions\Ruta 40:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=346
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java
Línea	118	118
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java

Método: public void editMov() {

```
....
118.                } catch (MitBusinessException e) {
```

Insufficient Logging of Exceptions\Ruta 41:

Severidad	Información
Estado del resultado	Para verificar

Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=347
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java
Línea	130	130
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java
Método	public void send2CIF() {

```
....
130.              } catch (MitBusinessException e) {
```

Insufficient Logging of Exceptions\Ruta 42:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=348
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java
Línea	147	147
Objeto	catch	catch

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/MovimeintosCIFView.java
Método	public void delete2CIF() {

```
....
147.                    } catch (MitBusinessException e) {
```

Insufficient Logging of Exceptions\Ruta 43:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=349
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/ValidacionManualView.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/ValidacionManualView.java
Línea	186	186
Objeto	catch	catch

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/views/ValidacionManualView.java

Método: public void clickValidarCuenta() throws MitBusinessException {

```
....
186.                    }catch(Exception e) {
```

Insufficient Logging of Database Actions

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Insufficient Logging of Database Actions Versión:1

Categorías

OWASP Top 10 API: API10-Insufficient Logging and Monitoring
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures

Descripción

Insufficient Logging of Database Actions\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=274
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/cif/persistence/ProfuturoCIFPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/cif/persistence/ProfuturoCIFPersistence.xml
Línea	164	164
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/cif/persistence/ProfuturoCIFPersistence.xml

Método: <insert id="insert" parameterType="mx.profuturo.nci.business.vo.cif.Profuturo_CIFVo"

```
....
164.        </insert>
```

Insufficient Logging of Database Actions\Ruta 2:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=275
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/AforeMovilPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/AforeMovilPersistence.xml
Línea	83	83
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/AforeMovilPersistence.xml
Método	<update id="rechazarAforeMovil" parameterType="mx.profuturo.nci.business.wrapped.AforeMovilFilter">

```
....
83.         </update>
```

Insufficient Logging of Database Actions\Ruta 3:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=276
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/BitacoraProcesoPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/BitacoraProcesoPersistence.xml
Línea	68	68
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/BitacoraProcesoPersistence.xml
Método	<insert id="insert" parameterType="mx.profuturo.nci.business.vo.BitacoraProcesoVO">

```
....
68.         </insert>
```

Insufficient Logging of Database Actions\Ruta 4:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=277
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/CatalogoConfiguracionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/CatalogoConfiguracionPersistence.xml
Línea	50	50
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/CatalogoConfiguracionPersistence.xml
Método	<update id="updateByIdCatalogo"

```
....
50.    </update>
```

Insufficient Logging of Database Actions\Ruta 5:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=278
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigIntentosCargaApoVolPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigIntentosCargaApoVolPersistence.xml
Línea	102	102
Objeto	executeUpdate	executeUpdate

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigIntentosCargaApoVolPersistence.xml
Método	<insert id="insertConfIntentosCarga"

```
....
102.        </insert>
```

Insufficient Logging of Database Actions\Ruta 6:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=279
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigIntentosCargaApoVolPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigIntentosCargaApoVolPersistence.xml
Línea	112	112
Objeto	executeUpdate	executeUpdate

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigIntentosCargaApoVolPersistence.xml
Método	<update id="editaConfIntentosCarga"

```
....
112.        </update>
```

Insufficient Logging of Database Actions\Ruta 7:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=280
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DetalleArchivoDomiPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DetalleArchivoDomiPersistence.xml
Línea	38	38

Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DetalleArchivoDomiPersistence.xml

Método: <insert id="insertDetalle" parameterType="mx.profuturo.nci.business.vo.DetalleArchivoDomiVO">

```
....
38.   </insert>
```

Insufficient Logging of Database Actions\Ruta 8:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=281
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DetalleArchivoDomiPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DetalleArchivoDomiPersistence.xml
Línea	62	62
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DetalleArchivoDomiPersistence.xml

Método: <insert id="insertDetallePar" parameterType="mx.profuturo.nci.business.vo.DetalleArchivoDomiVO">

```
....
62.   </insert>
```

Insufficient Logging of Database Actions\Ruta 9:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=282
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profutu	source/mit-av-business/src/main/resources/mx/profutu

	ro/nci/persistence/DiversificacionConciliacionPersistence.xml	ro/nci/persistence/DiversificacionConciliacionPersistence.xml
Línea	50	50
Objeto	executeUpdate	executeUpdate

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml
Método	<insert id="insert" parameterType="mx.profuturo.nci.business.vo.DiversificacionConciliacionVO">

```
....
50.    </insert>
```

Insufficient Logging of Database Actions\Ruta 10:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=283
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml
Línea	125	125
Objeto	executeUpdate	executeUpdate

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml
Método	<insert id="insertAll" parameterType="java.util.List">

```
....
125.    </insert>
```

Insufficient Logging of Database Actions\Ruta 11:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=284
Estatus	Recurrente

	Origen	Destino

Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml
Línea	151	151
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionConciliacionPersistence.xml

Método: <update id="update"

```
....
151.        </update>
```

Insufficient Logging of Database Actions\Ruta 12:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=285
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionOrdenesPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionOrdenesPersistence.xml
Línea	96	96
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionOrdenesPersistence.xml

Método: <insert id="insertAll" parameterType="java.util.List">

```
....
96.    </insert>
```

Insufficient Logging of Database Actions\Ruta 13:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=286
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionOrdenesPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionOrdenesPersistence.xml
Línea	124	124
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionOrdenesPersistence.xml

Método: <update id="update" parameterType="mx.profuturo.nci.business.vo.DiversificacionOrdenesVO">

```
....
124.    </update>
```

Insufficient Logging of Database Actions\Ruta 14:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=287
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Línea	156	156
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml

Método: <insert id="insertDiversificacionPreSolicitud"

```
....
156.        </insert>
```

Insufficient Logging of Database Actions\Ruta 15:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=288

Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Línea	208	208
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml

Método: <insert id="insertarDiversificacionSolicitudDomiciliacion"

```
....
208.        </insert>
```

Insufficient Logging of Database Actions\Ruta 16:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=289
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Línea	273	273
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml

Método: <insert id="insertarDiversificacionSolicitudDomiciliacionPar"

```
....
273.        </insert>
```

Insufficient Logging of Database Actions\Ruta 17:

Severidad	Información
Estado del resultado	Para verificar
Resultados en	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid

línea	=2733&pathid=290
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Línea	309	309
Objeto	executeUpdate	executeUpdate

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Método	<update id="actualizarDiversificacionSolicitudDomiciliacion"

```
....
309.      </update>
```

Insufficient Logging of Database Actions\Ruta 18:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=291
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Línea	327	327
Objeto	executeUpdate	executeUpdate

Fragmento de código	
Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Método	<update id="logicDeleteDiversificacionSolicitudDomiciliacion" parameterType="mx.profuturo.nci.business.vo.DiversificacionVO">

```
....
327.      </update>
```

Insufficient Logging of Database Actions\Ruta 19:

Severidad	Información
Estado del	Para verificar

resultado	
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=292
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Línea	357	357
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/DiversificacionPersistence.xml
Método	<update id="actualizarDiversificacionPreSolicitudDomiciliacion"

```
....
357.        </update>
```

Insufficient Logging of Database Actions\Ruta 20:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=293
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/FolioPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/FolioPersistence.xml
Línea	62	62
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/FolioPersistence.xml
Método	<insert id="insert" parameterType="mx.profuturo.nci.business.wrapped.FolioFilter">

```
....
62.    </insert>
```

Insufficient Logging of Database Actions\Ruta 21:

Severidad	Información
Estado del	Para verificar

resultado	
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=294
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/MatrizConvivenciaPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/MatrizConvivenciaPersistence.xml
Línea	44	44
Objeto	executeUpdate	executeUpdate

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/MatrizConvivenciaPersistence.xml
Método	<insert id="insert"

```
....
44.    </insert>
```

Pages Without Global Error Handler

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Pages Without Global Error Handler Versión:0

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
OWASP Top 10 2013: A5-Security Misconfiguration
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design

Descripción

Pages Without Global Error Handler\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=254
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/desktop/desktop.xhtml	source/mit-av-web/src/main/webapp/core/desktop/desktop.xhtml
Línea	1	1
Objeto	CxWrapper1362850320	CxWrapper1362850320

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/core/desktop/desktop.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 2:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=255
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/desktop/footer.xhtml	source/mit-av-web/src/main/webapp/core/desktop/footer.xhtml
Línea	1	1
Objeto	CxWrapper2016165217	CxWrapper2016165217

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/core/desktop/footer.xhtml
Método	<ui:component

```
....
1.  <ui:component
```

Pages Without Global Error Handler\Ruta 3:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=256
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/desktop/header.xhtml	source/mit-av-web/src/main/webapp/core/desktop/header.xhtml
Línea	1	1
Objeto	CxWrapper1185195935	CxWrapper1185195935

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/core/desktop/header.xhtml
Método	<ui:component xmlns="http://www.w3.org/1999/xhtml"

```
....
1.  <ui:component xmlns="http://www.w3.org/1999/xhtml"
```

Pages Without Global Error Handler\Ruta 4:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=257
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/desktop/languages.xhtml	source/mit-av-web/src/main/webapp/core/desktop/languages.xhtml
Línea	1	1
Objeto	CxWrapper2119409253	CxWrapper2119409253

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/desktop/languages.xhtml
Método	<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>

```
....
1.  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
```

Pages Without Global Error Handler\Ruta 5:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=258
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/core/desktop/menu.xhtml	source/mit-av-web/src/main/webapp/core/desktop/menu.xhtml
Línea	1	1
Objeto	CxWrapper420489415	CxWrapper420489415

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/core/desktop/menu.xhtml
Método	<ui:component

```
....
1.  <ui:component
```

Pages Without Global Error Handler\Ruta 6:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=259
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/access-denied.xhtml	source/mit-av-web/src/main/webapp/views/access-denied.xhtml
Línea	1	1
Objeto	CxWrapper965877413	CxWrapper965877413

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/webapp/views/access-denied.xhtml

Método: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 7:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=260
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/aforeMovil/configMinimosAfiliadoIndependiente.xhtml	source/mit-av-web/src/main/webapp/views/aforeMovil/configMinimosAfiliadoIndependiente.xhtml
Línea	1	1
Objeto	CxWrapper2146459624	CxWrapper2146459624

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/webapp/views/aforeMovil/configMinimosAfiliadoIndependiente.xhtml

Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 8:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=261
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/aforeMovil/consultaMontosAforeMovil.xhtml	source/mit-av-web/src/main/webapp/views/aforeMovil/consultaMontosAforeMovil.xhtml
Línea	1	1
Objeto	CxWrapper1929583730	CxWrapper1929583730

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/aforeMovil/consultaMontosAforeMovil.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 9:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=262
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/apovol-spei/ordenespei.xhtml	source/mit-av-web/src/main/webapp/views/apovol-spei/ordenespei.xhtml
Línea	1	1
Objeto	CxWrapper2006476018	CxWrapper2006476018

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/views/apovol-spei/ordenespei.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 10:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=263
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/apovol-spei/relacionarorden.xhtml	source/mit-av-web/src/main/webapp/views/apovol-spei/relacionarorden.xhtml
Línea	1	1
Objeto	CxWrapper737954286	CxWrapper737954286

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/views/apovol-spei/relacionarorden.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 11:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=264
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/depositoArchivo/depositoArchivo.xhtml	source/mit-av-web/src/main/webapp/views/depositoArchivo/depositoArchivo.xhtml
Línea	1	1
Objeto	CxWrapper220651811	CxWrapper220651811

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/depositoArchivo/depositoArchivo.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 12:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=265
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/domiciliacion/consultaDomiciliacion.xhtml	source/mit-av-web/src/main/webapp/views/domiciliacion/consultaDomiciliacion.xhtml
Línea	1	1
Objeto	CxWrapper1270619336	CxWrapper1270619336

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/domiciliacion/consultaDomiciliacion.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 13:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=266
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/domiciliacion/parametrizacionIntentosCarga.xhtml	source/mit-av-web/src/main/webapp/views/domiciliacion/parametrizacionIntentosCarga.xhtml
Línea	1	1
Objeto	CxWrapper877516474	CxWrapper877516474

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/domiciliacion/parametrizacionIntentosCarga.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 14:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=267
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/errorPage.xhtml	source/mit-av-web/src/main/webapp/views/errorPage.xhtml
Línea	1	1
Objeto	CxWrapper624501620	CxWrapper624501620

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/errorPage.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 15:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=268
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/index.xhtml	source/mit-av-web/src/main/webapp/views/index.xhtml
Línea	1	1
Objeto	CxWrapper1260685553	CxWrapper1260685553

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/index.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 16:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=269
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/login.xhtml	source/mit-av-web/src/main/webapp/views/login.xhtml
Línea	1	1
Objeto	CxWrapper1468689796	CxWrapper1468689796

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/login.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
```

Pages Without Global Error Handler\Ruta 17:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=270
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/traspasos/detalleMes.xhtml	source/mit-av-web/src/main/webapp/views/traspasos/detalleMes.xhtml
Línea	1	1
Objeto	CxWrapper1629652827	CxWrapper1629652827

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/views/traspasos/detalleMes.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 18:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=271
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/traspasos/inversionDomiciliacion.xhtml	source/mit-av-web/src/main/webapp/views/traspasos/inversionDomiciliacion.xhtml
Línea	1	1
Objeto	CxWrapper1219027744	CxWrapper1219027744

Fragmento de código

Nombre del archivo	source/mit-av-web/src/main/webapp/views/traspasos/inversionDomiciliacion.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 19:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=272
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/traspasos/monitoreoCargos.xhtml	source/mit-av-web/src/main/webapp/views/traspasos/monitoreoCargos.xhtml
Línea	1	1
Objeto	CxWrapper227046990	CxWrapper227046990

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/traspasos/monitoreoCargos.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Pages Without Global Error Handler\Ruta 20:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=273
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/webapp/views/traspasos/monitoreoSolicitudes.xhtml	source/mit-av-web/src/main/webapp/views/traspasos/monitoreoSolicitudes.xhtml
Línea	1	1
Objeto	CxWrapper1071449027	CxWrapper1071449027

Fragmento de código	
Nombre del archivo	source/mit-av-web/src/main/webapp/views/traspasos/monitoreoSolicitudes.xhtml
Método	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

```
....
1.  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Potentially Serializable Class With Sensitive Data

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Potentially Serializable Class With Sensitive Data Versión:1

Categorías

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A6-Sensitive Data Exposure
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A4-Insecure Design

Descripción

Potentially Serializable Class With Sensitive Data\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=297

Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/CatalogoConfigVO.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/CatalogoConfigVO.java
Línea	38	6
Objeto	regAcreditado	CatalogoConfigVO

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/CatalogoConfigVO.java

Método: private Short regAcreditado;

```
....
38.   private Short regAcreditado;
```

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/CatalogoConfigVO.java

Método: public class CatalogoConfigVO extends AbstractAuditoriaVO

```
....
6.  public class CatalogoConfigVO extends AbstractAuditoriaVO
```

Potentially Serializable Class With Sensitive Data\Ruta 2:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=298
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/PrincipalVO.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/PrincipalVO.java
Línea	38	6
Objeto	regAcreditado	PrincipalVO

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/PrincipalVO.java

Método: private Short regAcreditado;

```
....
38.   private Short regAcreditado;
```

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/PrincipalVO.java
Método	public class PrincipalVO extends AbstractAuditoriaVO

```
....
6.  public class PrincipalVO extends AbstractAuditoriaVO
```

Potentially Serializable Class With Sensitive Data\Ruta 3:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=299
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/Indicadores.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/Indicadores.java
Línea	56	36
Objeto	creditoInfonavit	Indicadores

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/Indicadores.java
Método	protected String creditoInfonavit;

```
....
56.      protected String creditoInfonavit;
```

Nombre del archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/Indicadores.java
Método	@XmlAccessorType(XmlAccessType.FIELD)

```
....
36.  @XmlAccessorType(XmlAccessType.FIELD)
```

Potentially Serializable Class With Sensitive Data\Ruta 4:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=300
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java
Línea	13	9
Objeto	password	AppUserBean

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java

Método: private String password;

```
....
13.      private String password;
```

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/beans/AppUserBean.java

Método: public class AppUserBean implements UserDetails {

```
....
9.  public class AppUserBean implements UserDetails {
```

Potentially Serializable Class With Sensitive Data\Ruta 5:

Severidad: Información

Estado del resultado: Para verificar

Resultados en línea: http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=301

Estatus: Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.java	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.java
Línea	9	6
Objeto	clave	SolicitudReclasificacionVO

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.java

Método: private String clave;

```
....
9.    private String clave;
```

Nombre del archivo	source/mit-av-business/src/main/java/mx/profuturo/nci/business/vo/SolicitudReclasificacionVO.java
Método	public class SolicitudReclasificacionVO {

```
....
6.  public class SolicitudReclasificacionVO {
```

Potentially Serializable Class With Sensitive Data\Ruta 6:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=302
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java
Línea	39	30
Objeto	contrasena	AutenticacionRequest

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java
Método	@XmlElement(required = true)

```
....
39.      @XmlElement(required = true)
```

Nombre del archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/AutenticacionRequest.java
Método	@XmlAccessorType(XmlAccessType.FIELD)

```
....
30.  @XmlAccessorType(XmlAccessType.FIELD)
```

Potentially Serializable Class With Sensitive Data\Ruta 7:

Severidad	Información

Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=303
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java
Línea	41	31
Objeto	contrasena	ConfirmarAccesoRequest

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java
Método	@XmlElement(required = true)

```
....
41.      @XmlElement(required = true)
```

Nombre del archivo	source/mit-av-business/src/main/wsc/java/mx/com/profuturo_gnp/ws/sso/controlacceso/ConfirmarAccesoRequest.java
Método	@XmlAccessorType(XmlAccessType.FIELD)

```
....
31.  @XmlAccessorType(XmlAccessType.FIELD)
```

Potentially Serializable Class With Sensitive Data\Ruta 8:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=304
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java
Línea	37	30
Objeto	clave	TipoContacto

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java
Método	@XmlElement(required = true)

```
....
37.       @XmlElement(required = true)
```

Nombre del archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/identificacioncliente/clienteservice/v1/types/TipoContacto.java
Método	@XmlAccessorType(XmlAccessType.FIELD)

```
....
30.   @XmlAccessorType(XmlAccessType.FIELD)
```

Potentially Serializable Class With Sensitive Data\Ruta 9:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=305
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java
Línea	40	32
Objeto	clave	ParametroCorreo

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java
Método	@XmlElement(required = true)

```
....
40.       @XmlElement(required = true)
```

Nombre del archivo	source/mit-av-business/src/main/wsc/java/profuturo/mx/iib/nci/notificaciones/enviocorreoservice/v1/types/ParametroCorreo.java
Método	@XmlAccessorType(XmlAccessType.FIELD)

```
....
32.  @XmlAccessorType(XmlAccessType.FIELD)
```

Dynamic SQL Queries

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Dynamic SQL Queries Versión:3

Categorías

OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 API: API8-Injection
OWASP Top 10 2021: A3-Injection

Descripción

Dynamic SQL Queries\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=295
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigSubprocesoOrigenPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigSubprocesoOrigenPersistence.xml
Línea	91	108
Objeto	Base_Column_List	executeQuery

Fragmento de código

Nombre del archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/ConfigSubprocesoOrigenPersistence.xml
Método	<select id="selectAll"

```
....
91.         <include refid="Base_Column_List" />
....
108.      </select>
```

Dynamic SQL Queries\Ruta 2:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=296
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/GeneraFolioPersistence.xml	source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/GeneraFolioPersistence.xml
Línea	7	7
Objeto	sql	executeQuery

Fragmento de código

Nombre del archivo: source/mit-av-business/src/main/resources/mx/profuturo/nci/persistence/GeneraFolioPersistence.xml

Método: <select id="generaFolio" parameterType="mx.profuturo.nci.business.wrapped.GeneraFolioFilter" statementType="CALLABLE">

```
....
7.  </select>
```

Use of Obsolete Functions

Ruta de consulta:
Java\Cx\Java Best Coding Practice\Use of Obsolete Functions Versión:4

Categorías

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A6-Vulnerable and Outdated Components

Descripción

Use of Obsolete Functions\Ruta 1:

Severidad	Información
Estado del resultado	Para verificar
Resultados en línea	http://172.21.17.5/CxWebClient/ViewerMain.aspx?scanid=1028003&projectid=2733&pathid=306
Estatus	Recurrente

	Origen	Destino
Archivo	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java	source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java
Línea	124	124
Objeto	getDummyCIFDataBean	getDummyCIFDataBean

Fragmento de código

Nombre del archivo: source/mit-av-web/src/main/java/mx/profuturo/nci/web/service/impl/MovimientosCifWebServiceImpl.java

Método: private List<NCI_CIFDataBean> getDummyData(int size) {

```
....
124.                    dataBeans.add(getDummyCIFDataBean());
```

Failure to Preserve Web Page Structure ('Cross-site Scripting')

Weakness ID: 79 *(Weakness Base)* **Status:** Usable

Description

Description Summary

The software does not sufficiently validate, filter, escape, and/or encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.

2. The web application dynamically generates a web page that contains this untrusted data.

3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.

4. A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.

5. Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.

6. This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

There are three main kinds of XSS:

Type 1: Reflected XSS (or Non-Persistent)

The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.

Type 2: Stored XSS (or Persistent)

The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. For example, the attacker might inject XSS into a log message, which might not be handled properly when an administrator views the logs.

Type 0: DOM-Based XSS

In DOM-based XSS, the client performs the injection of XSS into the page; in the other types, the server performs the injection. DOM-based XSS generally involves server-controlled, trusted script that is sent to the client, such as Javascript that performs sanity checks on a form before the user submits it. If the server-supplied script processes user-supplied data and then injects it back into the web page (such as with dynamic HTML), then DOM-based XSS is possible.

Once the malicious script is injected, the attacker can perform a variety of malicious activities. The attacker could transfer private information, such as cookies that may include session information, from the victim's machine to the attacker. The attacker could send malicious requests to a web site on behalf of the victim, which could be especially dangerous to the site if the victim has administrator privileges to manage that site. Phishing attacks could be used to emulate trusted web sites and trick the victim into entering a password, allowing the attacker to compromise the victim's account on that web site. Finally, the script could exploit a vulnerability in the web browser itself possibly taking over the victim's machine, sometimes referred to as "drive-by hacking."

In many cases, the attack can be launched without the victim even being aware of it. Even with careful users, attackers frequently use a variety of methods to encode the malicious portion of the attack, such as URL encoding or Unicode, so the request looks less suspicious.

Alternate Terms

XSS	
CSS:	"CSS" was once used as the acronym for this problem, but this could cause confusion with "Cascading Style Sheets," so usage of this acronym has declined significantly.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

Language-independent

Architectural Paradigms

Web-based: *(Often)*

Technology Classes

Web-Server: *(Often)*

Platform Notes

XSS flaws are very common in web applications since they require a great deal of developer discipline to avoid them.

Common Consequences

Scope	Effect
Confidentiality	The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Typically, a malicious user will craft a client-side script, which -- when parsed by a web browser -- performs some activity (such as sending all site cookies to a given E-mail address). This script will be loaded and run by each user visiting the web site. Since the site requesting to run the script has access to the cookies in question, the malicious script does also.
Access Control	In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined

	with other flaws.
Confidentiality Integrity Availability	The consequence of an XSS attack is the same regardless of whether it is stored or reflected. The difference is in how the payload arrives at the server. XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. Some cross-site scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on the end user systems for a variety of nefarious purposes. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirecting the user to some other page or site, running "Active X" controls (under Microsoft Internet Explorer) from sites that a user perceives as trustworthy, and modifying presentation of content.

Likelihood of Exploit

High to Very High

Enabling Factors for Exploitation

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted web site for the consumption of other valid users, commonly on places such as bulletin-board web sites which provide web based mailing list-style functionality.

Stored XSS got its start with web sites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook entries, and all subsequent visitors to the guestbook page would execute the malicious code. As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response.

Detection Methods

Automated Static Analysis

Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible, especially when multiple components are involved.

Effectiveness: Moderate

Black Box

Use the XSS Cheat Sheet [REF-14] or automated test-generation tools to help launch a wide variety of attacks against your web application. The Cheat Sheet contains many subtle XSS variations that are specifically targeted against weak XSS defenses.

Effectiveness: Moderate

With Stored XSS, the indirection caused by the data store can make it more difficult to find the problem. The tester must first inject the XSS string into the data store, then find the appropriate application functionality in which the XSS string is sent to other users of the application. These are two distinct steps in which the activation of the XSS can take place minutes, hours, or days after the XSS was originally injected into the data store.

Demonstrative Examples

Example 1

This example covers a Reflected XSS (Type 1) scenario.

The following JSP code segment reads an employee ID, eid, from an HTTP request and displays it to the user.

(Bad Code)

Example Language: **JSP**

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

The following ASP.NET code segment reads an employee ID number from an HTTP request and displays it to the user.

(Bad Code)

Example Language: **ASP.NET**

```
...
protected System.Web.UI.WebControls.TextBox Login;
protected System.Web.UI.WebControls.Label EmployeeID;
...
EmployeeID.Text = Login.Text;
```

```
... (HTML follows) ...
<p><asp:label id="EmployeeID" runat="server" /></p>
...
```

The code in this example operates correctly if the Employee ID variable contains only standard alphanumeric text. If it has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response. Initially this might not appear to be much of a vulnerability. After all, why would someone enter a URL that causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use e-mail or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers.

Example 2

This example covers a Stored XSS (Type 2) scenario.

The following JSP code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

(Bad Code)

Example Language: **JSP**

```
<%
...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
rs.next();
String name = rs.getString("name");
%>

Employee Name: <%= name %>
```

The following ASP.NET code segment queries a database for an employee with a given employee ID and prints the name corresponding with the ID.

(Bad Code)

Example Language: **ASP.NET**

```
protected System.Web.UI.WebControls.Label EmployeeName;
...
string query = "select * from emp where id=" + eid;
sda = new SqlDataAdapter(query, conn);
sda.Fill(dt);
string name = dt.Rows[0]["Name"];
...
EmployeeName.Text = name;
```

This code can appear less dangerous because the value of name is read from a database, whose contents are apparently managed by the application. However, if the value of name originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker can execute malicious commands in the user's web browser.

Observed Examples

Reference	Description
CVE-2008-5080	Chain: protection mechanism failure allows XSS
CVE-2006-4308	Chain: only checks "javascript:" tag
CVE-2007-5727	Chain: only removes SCRIPT tags, enabling XSS
CVE-2008-5770	Reflected XSS using the PATH INFO in a URL
CVE-2008-4730	Reflected XSS not properly handled when generating an error message
CVE-2008-5734	Reflected XSS sent through email message.

CVE-2008-0971	Stored XSS in a security product.
CVE-2008-5249	Stored XSS using a wiki page.
CVE-2006-3568	Stored XSS in a guestbook application.
CVE-2006-3211	Stored XSS in a guestbook application using a javascript: URI in a bbcode img tag.
CVE-2006-3295	Chain: library file is not protected against a direct request (CWE-425), leading to reflected XSS.

Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Phases: Implementation; Architecture and Design

Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:

- HTML body
- Element attributes (such as src="XYZ")
- URIs
- JavaScript sections
- Cascading Style Sheets and style property

etc. Note that HTML Entity Encoding is only appropriate for the HTML body.

Consult the XSS Prevention Cheat Sheet [REF-16] for more details on the types of encoding and escaping that are needed.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phase: Implementation

Use and specify a strong character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can open you up to subtle XSS attacks related to that encoding. See CWE-116 for more mitigations related to encoding/escaping.

Phase: Implementation

With Struts, you should write all data from form beans with the bean's filter attribute set to true.

Phase: Implementation

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an

example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed, not just parameters that the user is supposed to specify, but all data in the request, including hidden fields, cookies, headers, the URL itself, and so forth. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.

Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.

Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

Phase: Operation

Use an application firewall that can detect attacks against this weakness. This might not catch all attacks, and it might require some effort for customization. However, it can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

Background Details

Same Origin Policy

The same origin policy states that browsers should limit the resources accessible to scripts running on a given web site , or "origin", to the resources associated with that web site on the client-side, and not the client-side resources of any other sites or "origins". The goal is to prevent one site from being able to modify or read the contents of an unrelated site. Since the World Wide Web involves interactions between many sites, this policy is important for browsers to enforce.

Domain

The Domain of a website when referring to XSS is roughly equivalent to the resources associated with that website on the client-side of the connection. That is, the domain can be thought of as all resources the browser is storing for the user's interactions with this particular site.

Weakness Ordinalities

Ordinality	Description
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to	Named Chain(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**	
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ChildOf	Category	442	Web Problems	Development Concepts699	
ChildOf	Category	712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	**Weaknesses in OWASP Top Ten (2007) (primary)629**	
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711	
ChildOf	Category	725	OWASP Top Ten 2004 Category A4 -	**Weaknesses in OWASP Top Ten**	

			Cross-Site Scripting (XSS) Flaws	**(2004) (primary)711**	
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**	
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**	
CanPrecede	Weakness Base	494	Download of Code Without Integrity Check	Research Concepts1000	
PeerOf	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000	
ParentOf	Weakness Variant	80	Improper Sanitization of Script-Related HTML Tags in a Web Page (Basic XSS)	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ParentOf	Weakness Variant	81	Improper Sanitization of Script in an Error Message Web Page	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ParentOf	Weakness Variant	83	Improper Neutralization of Script in Attributes in a Web Page	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ParentOf	Weakness Variant	84	Failure to Resolve Encoded URI Schemes in a Web Page	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ParentOf	Weakness Variant	85	Doubled Character XSS Manipulations	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ParentOf	Weakness Variant	86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	**Development Concepts (primary)699 Research Concepts (primary)1000**	
ParentOf	Weakness Variant	87	Failure to Sanitize Alternate XSS Syntax	**Development Concepts (primary)699 Research Concepts (primary)1000**	
MemberOf	View	635	Weaknesses Used by NVD	**Weaknesses Used by NVD (primary)635**	
CanFollow	Weakness Base	113	Failure to Sanitize CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	Research Concepts1000	
CanFollow	Weakness Base	184	Incomplete Blacklist	Research Concepts1000	Incomplete Blacklist to Cross-Site Scripting692

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Cross-site scripting (XSS)
7 Pernicious Kingdoms			Cross-site Scripting
CLASP			Cross-site scripting
OWASP Top Ten 2007	A1	Exact	Cross Site Scripting (XSS)
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A4	Exact	Cross-Site Scripting (XSS) Flaws
WASC	8		Cross-site Scripting

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
85	Client Network Footprinting (using AJAX/XSS)	
86	Embedding Script (XSS) in HTTP Headers	
32	Embedding Scripts in HTTP Query Strings	
18	Embedding Scripts in Nonscript Elements	
19	Embedding Scripts within Scripts	
63	Simple Script Injection	
91	XSS in IMG Tags	
106	Cross Site Scripting through Log Files	
198	Cross-Site Scripting in Error Pages	
199	Cross-Site Scripting Using Alternate Syntax	
209	Cross-Site Scripting Using MIME Type Mismatch	
243	Cross-Site Scripting in Attributes	
244	Cross-Site Scripting via Encoded URI Schemes	
245	Cross-Site Scripting Using Doubled Characters, e.g. %3C%3Cscript	
246	Cross-Site Scripting Using Flash	
247	Cross-Site Scripting with Masking through Invalid Characters in Identifiers	

References

[REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Syngress. 2007.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 2: Web-Server Related Vulnerabilities (XSS, XSRF, and Response Splitting)." Page 31. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 3: Web-Client Related Vulnerabilities (XSS)." Page 63. McGraw-Hill. 2010.

"Cross-site scripting". Wikipedia. 2008-08-26. <http://en.wikipedia.org/wiki/Cross-site_scripting>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 13, "Web-Specific Input Issues" Page 413. 2nd Edition. Microsoft. 2002.

[REF-14] RSnake. "XSS (Cross Site Scripting) Cheat Sheet". <http://ha.ckers.org/xss.html>.

Microsoft. "Mitigating Cross-site Scripting With HTTP-only Cookies". <http://msdn.microsoft.com/en-us/library/ms533046.aspx>.

Mark Curphey, Microsoft. "Anti-XSS 3.0 Beta and CAT.NET Community Technology Preview now Live!". <http://blogs.msdn.com/cisg/archive/2008/12/15/anti-xss-3-0-beta-and-cat-net-community-technology-preview-now-live.aspx>.

"OWASP Enterprise Security API (ESAPI) Project". <http://www.owasp.org/index.php/ESAPI>.

Ivan Ristic. "XSS Defense HOWTO". <http://blog.modsecurity.org/2008/07/do-you-know-how.html>.

OWASP. "Web Application Firewall". <http://www.owasp.org/index.php/Web_Application_Firewall>.

Web Application Security Consortium. "Web Application Firewall Evaluation Criteria". <http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html>.

RSnake. "Firefox Implements httpOnly And is Vulnerable to XMLHTTPRequest". 2007-07-19.

"XMLHttpRequest allows reading HTTPOnly cookies". Mozilla. <https://bugzilla.mozilla.org/show_bug.cgi?id=380418>.

"Apache Wicket". <http://wicket.apache.org/>.

[REF-16] OWASP. "XSS (Cross Site Scripting) Prevention Cheat Sheet". <http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Description, Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Observed Examples, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Observed Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Description, Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Cross-site Scripting (XSS)
2009-01-12	Failure to Sanitize Directives in a Web Page (aka 'Cross-site scripting' (XSS))
2009-05-27	Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')

BACK TO TOP

Failure to Clear Heap Memory Before Release ('Heap Inspection')

Weakness ID: 244 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

Using realloc() to resize buffers that store sensitive information can leave the sensitive information exposed to attack, because it is not removed from memory.

Extended Description

When sensitive data such as a password or an encryption key is not removed from memory, it could be exposed to an attacker using a "heap inspection" attack that reads the sensitive data using memory dumps or other methods. The realloc() function is commonly used to increase the size of a block of allocated memory. This operation often requires copying the contents of the old memory block into a new and larger block. This operation leaves the contents of the original block intact but inaccessible to the program, preventing the program from being able to scrub sensitive data from memory. If an attacker can later examine the contents of a memory dump, the sensitive data could be exposed.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Confidentiality	Be careful using vfork() and fork() in security sensitive code. The process state will not be cleaned up and will contain traces of data from past use.

Demonstrative Examples

Example 1

The following code calls realloc() on a buffer containing sensitive data:

(Bad Code)

Example Language: **C**

```
cleartext_buffer = get_secret();...
cleartext_buffer = realloc(cleartext_buffer, 1024);
...
scrub_memory(cleartext_buffer, 1024);
```

There is an attempt to scrub the sensitive data from memory, but realloc() is used, so a copy of the data can still be exposed in the memory originally allocated for cleartext_buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	226	Sensitive Information Uncleared Before Release	**Research Concepts (primary)1000**
ChildOf	Weakness Class	227	Failure to Fulfill API Contract ('API Abuse')	**Development Concepts (primary)699 Seven Pernicious Kingdoms**

				(primary)700
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
CanPrecede	Weakness Class	669	Incorrect Resource Transfer Between Spheres	Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Heap Inspection
CERT C Secure Coding	MEM03-C		Clear sensitive information stored in reusable resources returned for reuse

White Box Definitions

A weakness where code path has:

1. start statement that stores information in a buffer
2. end statement that resize the buffer and
3. path does not contain statement that performs cleaning of the buffer

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Name, Relationships, Other Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Relationships		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Other Notes		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Heap Inspection		
2008-09-09	Failure to Clear Heap Memory Before Release		
2009-05-27	Failure to Clear Heap Memory Before Release (aka 'Heap Inspection')		

BACK TO TOP

Origin Validation Error

Weakness ID: 346 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not properly verify that the source of data or communication is valid.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Observed Examples

Reference	Description
CVE-2000-1218	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2005-0877	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2001-1452	DNS server caches glue records received from non-delegated name servers
CVE-2005-2188	user ID obtained from untrusted source (URL)
CVE-2003-0174	LDAP service does not verify if a particular attribute was set by the LDAP server
CVE-1999-1549	product does not sufficiently distinguish external HTML from internal, potentially dangerous HTML, allowing bypass using special strings in the page title. Overlaps special elements.
CVE-2003-0981	product records the reverse DNS name of a visitor in the logs, allowing spoofing and resultant XSS.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	345	Insufficient Verification of Data Authenticity	**Development Concepts (primary)699 Research Concepts (primary)1000**
RequiredBy	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000
RequiredBy	Compound Element: Composite	384	Session Fixation	Research Concepts1000
PeerOf	Weakness Base	451	UI Misrepresentation of Critical Information	Research Concepts1000

Relationship Notes

This is a factor in many weaknesses, both primary and resultant. The problem could be due to design or implementation. This is a fairly general class.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

PLOVER			Origin Validation Error

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
21	Exploitation of Session Variables, Resource IDs and other Trusted Credentials	
89	Pharming	
59	Session Credential Falsification through Prediction	
60	Reusing Session IDs (aka Session Replay)	
75	Manipulating Writeable Configuration Files	
76	Manipulating Input to File System Calls	
111	JSON Hijacking (aka JavaScript Hijacking)	

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Relationship Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

BACK TO TOP

Use of Obsolete Functions

Weakness ID: 477 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses deprecated or obsolete functions, which suggests that the code has not been actively reviewed or maintained.

Time of Introduction

- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses the deprecated function getpw() to verify that a plaintext password matches a user's encrypted password. If the password is valid, the function sets result to 1; otherwise it is set to 0.

(Bad Code)

Example Language: **C**

```
...
getpw(uid, pwdline);
for (i=0; i<3; i++){
cryptpw=strtok(pwdline, ":");
pwdline=0;
}
result = strcmp(crypt(plainpw,cryptpw), cryptpw) == 0;
...
```

Although the code often behaves correctly, using the getpw() function can be problematic from a security standpoint, because it can overflow the buffer passed to its second parameter. Because of this vulnerability, getpw() has been supplanted by getpwuid(), which performs the same lookup as getpw() but returns a pointer to a statically-allocated structure to mitigate the risk. Not all functions are deprecated or replaced because they pose a security risk. However, the presence of an obsolete function often indicates that the surrounding code has been neglected and may be in a state of disrepair. Software security has not been a priority, or even a consideration, for very long. If the program uses deprecated or obsolete functions, it raises the probability that there are security problems lurking nearby.

Example 2

In the following code, the programmer assumes that the system always has a property named "cmd" defined. If an attacker can control the program's environment so that "cmd" is not defined, the program throws a null pointer exception when it attempts to call the "Trim()" method.

(Bad Code)

Example Language: **Java**

```
String cmd = null;
...
cmd = Environment.GetEnvironmentVariable("cmd");
cmd = cmd.Trim();
```

Example 3

The following code constructs a string object from an array of bytes and a value that

specifies the top 8 bits of each 16-bit Unicode character.

(Bad Code)

Example Language: **Java**

```
...
String name = new String(nameBytes, highByte);
...
```

In this example, the constructor may fail to correctly convert bytes to characters depending upon which charset is used to encode the string represented by nameBytes. Due to the evolution of the charsets used to encode strings, this constructor was deprecated and replaced by a constructor that accepts as one of its parameters the name of the charset used to encode the bytes for conversion.

Potential Mitigations

Consider seriously the security implication of using an obsolete function. Consider using alternate functions.

The system should warn the user from using an obsolete function.

Other Notes

As programming languages evolve, functions occasionally become obsolete due to:

- Advances in the language
- Improved understanding of how operations should be performed effectively and securely
- Changes in the conventions that govern certain operations

Functions that are removed are usually replaced by newer counterparts that perform the same task in some different and hopefully improved way. Refer to the documentation for this function in order to determine why it is deprecated or obsolete and to learn about alternative ways to achieve the same functionality. The remainder of this text discusses general problems that stem from the use of deprecated or obsolete functions.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Obsolete

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-01-30	Obsolete		

BACK TO TOP

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699 Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

Information Exposure Through an Error Message

Weakness ID: 209 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software generates an error message that includes sensitive information about its environment, users, or associated data.

Extended Description

The sensitive information may be valuable information on its own (such as a password), or it may be useful for launching other, more deadly attacks. If an attack fails, an attacker may use error information provided by the server to launch another more focused attack. For example, an attempt to exploit a path traversal weakness (CWE-22) might yield the full pathname of the installed application. In turn, this could be used to select the proper number of ".." sequences to navigate to the targeted file. An attack using SQL injection (CWE-89) might not initially succeed, but an error message could reveal the malformed query, which would expose query logic and possibly even passwords or other sensitive information used within the query.

Time of Introduction

- Architecture and Design
- Implementation
- System Configuration
- Operation

Applicable Platforms

Languages

PHP: *(Often)*

All

Common Consequences

Scope	Effect
Confidentiality	Often this will either reveal sensitive information which may be used for a later attack or private information stored in the server.

Likelihood of Exploit

High

Detection Methods

Manual Analysis

This weakness generally requires domain-specific interpretation using manual analysis. However, the number of potential error conditions may be too large to cover completely within limited time constraints.

Effectiveness: High

Automated Analysis

Automated methods may be able to detect certain idioms automatically, such as exposed stack traces or pathnames, but violation of business rules or privacy requirements is not typically feasible.

Effectiveness: Moderate

Demonstrative Examples

Example 1

In the following example, sensitive information might be printed depending on the exception that occurs.

(Bad Code)

Example Language: **Java**

```
try {
/.../
}
catch (Exception e) {
System.out.println(e);
}
```

If an exception related to SQL is handled by the catch, then the output might contain sensitive information such as SQL query structure or private information. If this output is redirected to a web user, this may represent a security problem.

Example 2

The following code generates an error message that leaks the full pathname of the configuration file.

(Bad Code)

Example Language: **Perl**

```
$ConfigDir = "/home/myprog/config";
$uname = GetUserInput("username");
# avoid CWE-22, CWE-78, others.
ExitError("Bad hacker!") if ($uname !~ /^\w+$/);
$file = "$ConfigDir/$uname.txt";
if (! (-e $file)) {
ExitError("Error: $file does not exist");
}
...
```

If this code is running on a server, such as a web application, then the person making the request should not know what the full pathname of the configuration directory is. By submitting a username that does not produce a $file that exists, an attacker could get this pathname. It could then be used to exploit path traversal or symbolic link following problems that may exist elsewhere in the application.

Observed Examples

Reference	Description
CVE-2008-2049	POP3 server reveals a password in an error message after multiple APOP commands are sent. Might be resultant from another weakness.
CVE-2007-5172	Program reveals password in error message if attacker can trigger certain database errors.
CVE-2008-4638	Composite: application running with high privileges allows user to specify a restricted file to process, which generates a parsing error that leaks the contents of the file.
CVE-2008-1579	Existence of user names can be determined by requesting a nonexistent blog and reading the error message.
CVE-2007-1409	Direct request to library file in web application triggers pathname leak in error message.
CVE-2008-3060	Malformed input to login page causes leak of full path when IMAP call fails.

Potential Mitigations

Phase: Implementation

Ensure that error messages only contain minimal details that are useful to the intended audience, and nobody else. The messages need to strike the balance between being too cryptic and not being cryptic enough. They should not necessarily reveal the methods that were used to determine the error. Such detailed information can help an attacker craft another attack that now will pass through the validation filters.

If errors must be tracked in some detail, capture them in log messages - but consider what could occur if the log messages can be viewed by attackers. Avoid recording highly sensitive information such as passwords in any form. Avoid inconsistent messaging that might accidentally tip off an attacker about internal state, such as whether a username is valid or not.

Phase: Implementation

Handle exceptions internally and do not display errors containing potentially sensitive information to a user.

Phase: Build and Compilation

Debugging information should not make its way into a production release.

Phase: Testing

Identify error conditions that are not likely to occur during normal usage and trigger them. For example, run the program under low memory conditions, run with insufficient privileges or permissions, interrupt a transaction before it is completed, or disable connectivity to basic network services such as DNS. Monitor the software for any unexpected behavior. If you trigger an unhandled exception or similar error that was discovered and handled by the application's environment, it may still indicate unexpected conditions that were not handled by the application itself.

Phase: Testing

Stress-test the software by calling it simultaneously from a large number of threads or processes, and look for evidence of any unexpected behavior. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Phase: System Configuration

Where available, configure the environment to use less verbose error messages. For example, in PHP, disable the display_errors setting during configuration, or at runtime using the error_reporting() function.

Phase: System Configuration

Create default error pages or messages that do not leak any information.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	200	Information Exposure	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	717	OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	728	OWASP Top Ten 2004 Category A7 - Improper Error Handling	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	731	OWASP Top Ten 2004 Category A10 - Insecure Configuration Management	Weaknesses in OWASP Top Ten (2004)711
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Weakness Class	755	Improper Handling of Exceptional Conditions	Research Concepts1000
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Base	210	Product-Generated Error Message Information Leak	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	211	Product-External Error Message Information Leak	**Development Concepts (primary)699 Research Concepts (primary)1000**
CanFollow	Weakness Base	600	Failure to Catch All Exceptions in Servlet	Research Concepts1000
CanFollow	Weakness Class	756	Missing Custom Error Page	Research Concepts1000
CanAlsoBe	Weakness Variant	81	Improper Sanitization of	Research Concepts1000

			Script in an Error Message Web Page	
CanAlsoBe	Weakness Variant	201	Information Leak Through Sent Data	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Accidental leaking of sensitive information through error messages
OWASP Top Ten 2007	A6	CWE More Specific	Information Leakage and Improper Error Handling
OWASP Top Ten 2004	A7	CWE More Specific	Improper Error Handling
OWASP Top Ten 2004	A10	CWE More Specific	Insecure Configuration Management

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
7	Blind SQL Injection	
54	Probing an Application Through Targeting its Error Reporting	
214	Fuzzing for garnering J2EE/.NET-based stack traces, for application mapping	
215	Fuzzing and observing application log data/errors for application mapping	

References

Web Application Security Consortium. "Information Leakage". <http://www.webappsec.org/projects/threat/classes/information_leakage.shtml>.

Brian Chess and Jacob West. "Secure Programming with Static Analysis". Section 9.2, page 326.. Addison-Wesley. 2007.

M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 16, "General Good Practices." Page 415. 1st Edition. Microsoft. 2002.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 11: Failure to Handle Errors Correctly." Page 185. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 12: Information Leakage." Page 194. McGraw-Hill. 2010.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Name, Observed Examples, Other Notes, Potential Mitigations, Relationships, Time of Introduction		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Potential Mitigations, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name, Potential Mitigations, References, Time of Introduction		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Detection Factors, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names	
Change Date	**Previous Entry Name**
2009-01-12	Error Message Information Leaks
2009-12-28	Error Message Information Leak

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Origin Validation Error

Weakness ID: 346 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not properly verify that the source of data or communication is valid.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Observed Examples

Reference	Description
CVE-2000-1218	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2005-0877	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2001-1452	DNS server caches glue records received from non-delegated name servers
CVE-2005-2188	user ID obtained from untrusted source (URL)
CVE-2003-0174	LDAP service does not verify if a particular attribute was set by the LDAP server
CVE-1999-1549	product does not sufficiently distinguish external HTML from internal, potentially dangerous HTML, allowing bypass using special strings in the page title. Overlaps special elements.
CVE-2003-0981	product records the reverse DNS name of a visitor in the logs, allowing spoofing and resultant XSS.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	345	Insufficient Verification of Data Authenticity	**Development Concepts (primary)699 Research Concepts (primary)1000**
RequiredBy	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000
RequiredBy	Compound Element: Composite	384	Session Fixation	Research Concepts1000
PeerOf	Weakness Base	451	UI Misrepresentation of Critical Information	Research Concepts1000

Relationship Notes

This is a factor in many weaknesses, both primary and resultant. The problem could be due to design or implementation. This is a fairly general class.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

PLOVER			Origin Validation Error

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
21	Exploitation of Session Variables, Resource IDs and other Trusted Credentials	
89	Pharming	
59	Session Credential Falsification through Prediction	
60	Reusing Session IDs (aka Session Replay)	
75	Manipulating Writeable Configuration Files	
76	Manipulating Input to File System Calls	
111	JSON Hijacking (aka JavaScript Hijacking)	

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Relationship Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

BACK TO TOP

Improper Output Sanitization for Logs

Weakness ID: 117 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not properly sanitize or incorrectly sanitizes output that is written to logs.

Extended Description

This can allow an attacker to forge log entries or inject malicious content into logs.

Log forging vulnerabilities occur when:

1. Data enters an application from an untrusted source.
2. The data is written to an application or system log file.

Time of Introduction

- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Integrity	Interpretation of the log files may be hindered or misdirected if an attacker can supply data to the application that is subsequently logged verbatim. In the most benign case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. Forged or otherwise corrupted log files can be used to cover an attacker's tracks, possibly by skewing statistics, or even to implicate another party in the commission of a malicious act. If the log file is processed automatically, the attacker can render the file unusable by corrupting the format of the file or injecting unexpected characters. An attacker may inject code or other commands into the log file and take advantage of a vulnerability in the log processing utility.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following web application code attempts to read an integer value from a request object. If the value fails to parse as an integer, then the input is logged with an error message indicating what happened.

(Bad Code)

Example Language: **Java**

```
String val = request.getParameter("val");
try {

int value = Integer.parseInt(val);
}
catch (NumberFormatException) {
log.info("Failed to parse val = " + val);
}
...
```

If a user submits the string "twenty-one" for val, the following entry is logged: INFO: Failed to parse val=twenty-one However, if an attacker submits the string "twenty-one%0a%0aINFO:+User+logged+out%3dbadguy", the following entry is logged: INFO:

Failed to parse val=twenty-one INFO: User logged out=badguy Clearly, attackers can use this same mechanism to insert arbitrary log entries.

Observed Examples

Reference	Description
CVE-2006-4624	Chain: inject fake log entries with fake timestamps using CRLF injection

Potential Mitigations

Phase: Architecture and Design

Assume all input is malicious. Use a standard input validation mechanism to validate all input for length, type, syntax, and business rules before accepting the data to be displayed or stored. Use an "accept known good" validation strategy.

Use and specify a strong output encoding (such as ISO 8859-1 or UTF 8).

Do not rely exclusively on blacklist validation to detect malicious input or to encode output. There are too many variants to encode a character; you're likely to miss some variants.

Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass whitelist schemes by introducing dangerous inputs after they have been checked.

Background Details

Applications typically use log files to store a history of events or transactions for later review, statistics gathering, or debugging. Depending on the nature of the application, the task of reviewing log files may be performed manually on an as-needed basis or automated with a tool that automatically culls logs for important events or trending information.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	116	Improper Encoding or Escaping of Output	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**Weaknesses in OWASP Top Ten (2004) (primary)711**
CanFollow	Weakness Base	93	Failure to Sanitize CRLF Sequences ('CRLF Injection')	Research Concepts1000

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Log Forging

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
93	Log Injection-Tampering-Forging	
81	Web Logs Tampering	
106	Cross Site Scripting through Log Files	

References

G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. February 2004.

A. Muffet. "The night the log was forged". <http://doc.novsu.ac.ru/oreilly/tcpip/puis/ch10_05.htm>.

OWASP. "OWASP TOP 10". <http://www.owasp.org/index.php/Top_10_2007>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated References, Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Background Details, Common Consequences, Description, Other Notes, References		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Name, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Other Notes, Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Log Forging		
2009-05-27	Incorrect Output Sanitization for Logs		

BACK TO TOP

Origin Validation Error

Weakness ID: 346 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not properly verify that the source of data or communication is valid.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Observed Examples

Reference	Description
CVE-2000-1218	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2005-0877	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2001-1452	DNS server caches glue records received from non-delegated name servers
CVE-2005-2188	user ID obtained from untrusted source (URL)
CVE-2003-0174	LDAP service does not verify if a particular attribute was set by the LDAP server
CVE-1999-1549	product does not sufficiently distinguish external HTML from internal, potentially dangerous HTML, allowing bypass using special strings in the page title. Overlaps special elements.
CVE-2003-0981	product records the reverse DNS name of a visitor in the logs, allowing spoofing and resultant XSS.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	345	Insufficient Verification of Data Authenticity	**Development Concepts (primary)699 Research Concepts (primary)1000**
RequiredBy	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000
RequiredBy	Compound Element: Composite	384	Session Fixation	Research Concepts1000
PeerOf	Weakness Base	451	UI Misrepresentation of Critical Information	Research Concepts1000

Relationship Notes

This is a factor in many weaknesses, both primary and resultant. The problem could be due to design or implementation. This is a fairly general class.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

PLOVER			Origin Validation Error

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
21	Exploitation of Session Variables, Resource IDs and other Trusted Credentials	
89	Pharming	
59	Session Credential Falsification through Prediction	
60	Reusing Session IDs (aka Session Replay)	
75	Manipulating Writeable Configuration Files	
76	Manipulating Input to File System Calls	
111	JSON Hijacking (aka JavaScript Hijacking)	

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Relationship Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

BACK TO TOP

Uncontrolled Resource Consumption ('Resource Exhaustion')

Weakness ID: 400 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

The software does not properly restrict the size or amount of resources that are requested or influenced by an actor, which can be used to consume more resources than intended.

Extended Description

Limited resources include memory, file system storage, database connection pool entries, or CPU. If an attacker can trigger the allocation of these limited resources, but the number or size of the resources is not controlled, then the attacker could cause a denial of service that consumes all available resources. This would prevent valid users from accessing the software, and it could potentially have an impact on the surrounding environment. For example, a memory exhaustion attack against an application could slow down the application as well as its host operating system.

Resource exhaustion problems have at least two common causes:

- (1) Error conditions and other exceptional circumstances
- (2) Confusion over which part of the program is responsible for releasing the resource

Time of Introduction

- Operation
- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	The most common result of resource exhaustion is denial of service. The software may slow down, crash due to unhandled errors, or lock out legitimate users.
Integrity	In some cases it may be possible to force the software to "fail open" in the event of resource exhaustion. The state of the software -- and possibly the security functionality - may then be compromised.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis typically has limited utility in recognizing resource exhaustion problems, except for program-independent system resources such as files, sockets, and processes. For system resources, automated static analysis may be able to detect circumstances in which resources are not released after they have expired. Automated analysis of configuration files may be able to detect settings that do not specify a maximum value.

Automated static analysis tools will not be appropriate for detecting exhaustion of custom resources, such as an intended security policy in which a bulletin board user is only allowed to make a limited number of posts per day.

Effectiveness: Limited

Automated Dynamic Analysis

Certain automated dynamic analysis techniques may be effective in spotting resource exhaustion problems, especially with

resources such as processes, memory, and connections. The technique may involve generating a large number of requests to the software within a short time frame.

Effectiveness: Moderate

Fuzzing

While fuzzing is typically geared toward finding low-level implementation bugs, it can inadvertently find resource exhaustion problems. This can occur when the fuzzer generates a large number of test cases but does not restart the targeted software in between test cases. If an individual test case produces a crash, but it does not do so reliably, then an inability to handle resource exhaustion may be the cause.

Effectiveness: Opportunistic

Demonstrative Examples

Example 1

(Bad Code)

Example Language: **Java**

```
class Worker implements Executor {
...
public void execute(Runnable r) {

try {
...
}
catch (InterruptedException ie) {

// postpone response
Thread.currentThread().interrupt();
}
}
public Worker(Channel ch, int nworkers) {
...
}
protected void activate() {

Runnable loop = new Runnable() {

public void run() {

try {
for (;;) {

Runnable r = ... r.run();
}
}
catch (InterruptedException ie) {
...
}
}
};
new Thread(loop).start();
}
```

There are no limits to runnables. Potentially an attacker could cause resource problems very quickly.

Example 2

This code allocates a socket and forks each time it receives a new connection.

(Bad Code)

Example Languages: **C and C++**

```
sock=socket(AF_INET, SOCK_STREAM, 0);
while (1) {

newsock=accept(sock, ...);
printf("A connection has been accepted\n");
pid = fork();
```

```
}
```

The program does not track how many connections have been made, and it does not limit the number of connections. Because forking is a relatively expensive operation, an attacker would be able to cause the system to run out of CPU, processes, or memory by making a large number of connections.

Observed Examples

Reference	Description
CVE-2009-2874	Product allows attackers to cause a crash via a large number of connections.
CVE-2009-1928	Malformed request triggers uncontrolled recursion, leading to stack exhaustion.
CVE-2009-2858	Chain: memory leak (CWE-404) leads to resource exhaustion.
CVE-2009-2726	Driver does not use a maximum width when invoking sscanf style functions, causing stack consumption.
CVE-2009-2540	Large integer value for a length property in an object causes a large amount of memory allocation.
CVE-2009-2299	Web application firewall consumes excessive memory when an HTTP request contains a large Content-Length value but no POST data.
CVE-2009-2054	Product allows exhaustion of file descriptors when processing a large number of TCP packets.
CVE-2008-5180	Communication product allows memory consumption with a large number of SIP requests, which cause many sessions to be created.
CVE-2008-2121	TCP implementation allows attackers to consume CPU and prevent new connections using a TCP SYN flood attack.
CVE-2008-2122	Port scan triggers CPU consumption with processes that attempt to read data from closed sockets.
CVE-2008-1700	Product allows attackers to cause a denial of service via a large number of directives, each of which opens a separate window.
CVE-2007-4103	Product allows resource exhaustion via a large number of calls that do not complete a 3-way handshake.
CVE-2006-1173	Mail server does not properly handle deeply nested multipart MIME messages, leading to stack exhaustion.
CVE-2007-0897	Chain: anti-virus product encounters a malformed file but returns from a function without closing a file descriptor (CWE-775) leading to file descriptor consumption (CWE-400) and failed scans.

Potential Mitigations

Phase: Architecture and Design

Design throttling mechanisms into the system architecture. The best protection is to limit the amount of resources that an unauthorized user can cause to be expended. A strong authentication and access control model will help prevent such attacks from occurring in the first place. The login application should be protected against DoS attacks as much as possible. Limiting the database access, perhaps by caching result sets, can help minimize the resources expended. To further limit the potential for a DoS attack, consider tracking the rate of requests received from users and blocking requests that exceed a defined rate threshold.

Phase: Architecture and Design

Mitigation of resource exhaustion attacks requires that the target system either:

- recognizes the attack and denies that user further access for a given amount of time, or
- uniformly throttles all requests in order to make it more difficult to consume resources more quickly than they can again be freed.

The first of these solutions is an issue in itself though, since it may allow attackers to prevent the use of the system by a particular valid user. If the attacker impersonates the valid user, he may be able to prevent the user from accessing the server in question.

The second solution is simply difficult to effectively institute -- and even when properly done, it does not provide a full solution. It simply makes the attack require more resources on the part of the attacker.

Phase: Architecture and Design

Ensure that protocols have specific limits of scale placed on them.

Phase: Implementation

Ensure that all failures in resource allocation place the system into a safe posture.

Other Notes

Database queries that take a long time to process are good DoS targets. An attacker would have to write a few lines of Perl code to generate enough traffic to exceed the site's ability to keep up. This would effectively prevent authorized users from using the site at all. Resources can be exploited simply by ensuring that the target machine must do much more work and consume more resources in order to service a request than the attacker must do to initiate a request.

A prime example of this can be found in old switches that were vulnerable to "macof" attacks (so named for a tool developed by Dugsong). These attacks flooded a switch with random IP and MAC address combinations, therefore exhausting the switch's cache, which held the information of which port corresponded to which MAC addresses. Once this cache was exhausted, the switch would fail in an insecure way and would begin to act simply as a hub, broadcasting all traffic on all ports and allowing for basic sniffing attacks.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Weakness Class	664	Improper Control of a Resource Through its Lifetime	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ParentOf	Category	769	File Descriptor Exhaustion	**Development Concepts (primary)699**
ParentOf	Weakness Base	770	Allocation of Resources Without Limits or Throttling	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Base	771	Missing Reference to Active Allocated Resource	**Research Concepts (primary)1000**
ParentOf	Weakness Base	772	Missing Release of Resource after Effective Lifetime	Research Concepts1000
ParentOf	Weakness Base	779	Logging of Excessive Data	**Development Concepts (primary)699 Research Concepts (primary)1000**
CanFollow	Weakness Base	410	Insufficient Resource Pool	Development Concepts699 Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Resource exhaustion (file descriptor, disk space, sockets, ...)
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service
WASC	10		Denial of Service
WASC	41		XML Attribute Blowup

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
2	Inducing Account Lockout	
82	Violating Implicit Assumptions Regarding XML Content (aka XML Denial of Service (XDoS))	

147	XML Ping of Death
228	Resource Depletion through DTD Injection in a SOAP Message

References

Joao Antunes, Nuno Ferreira Neves and Paulo Verissimo. "Detection and Prediction of Resource-Exhaustion Vulnerabilities". Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE). November 2008. <http://homepages.di.fc.ul.pt/~nuno/PAPERS/ISSRE08.pdf>.

D.J. Bernstein. "Resource exhaustion". <http://cr.yp.to/docs/resources.html>.

Pascal Meunier. "Resource exhaustion". Secure Programming Educational Material. 2004. <http://homes.cerias.purdue.edu/~pmeunier/secprog/sanitized/class1/6.resource%20exhaustion.ppt>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 17, "Protecting Against Denial of Service Attacks" Page 517. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name, Relationships		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description, Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Observed Examples, Other Notes, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Detection Factors, Potential Mitigations, References, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2008-10-14	Resource Exhaustion
2009-05-27	Uncontrolled Resource Consumption (aka 'Resource Exhaustion')

BACK TO TOP

Serializable Class Containing Sensitive Data

Weakness ID: 499 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code contains a class with sensitive data, but the class does not explicitly deny serialization. The data can be accessed by serializing the class through another class.

Extended Description

Serializable classes are effectively open classes since data cannot be hidden in them. Classes that do not explicitly deny serialization can be serialized by any other class, which can then in turn use the data stored inside it.

Time of Introduction

- Implementation

Applicable Platforms

Languages

Java

Common Consequences

Scope	Effect
Confidentiality	an attacker can write out the class to a byte stream, then extract the important data from it.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

(Bad Code)

Example Language: **Java**

```
class Teacher {
private String name;
private String clas;
public Teacher(String name,String clas) {

//...
//Check the database for the name and address
this.SetName() = name;
this.Setclas() = clas;
}
}
```

Potential Mitigations

Phase: Implementation

In Java, explicitly define final writeObject() to prevent serialization. This is the recommended solution. Define the writeObject() function to throw an exception explicitly denying serialization.

Phase: Implementation

Make sure to prevent serialization of your objects.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	485	Insufficient Encapsulation	**Development Concepts (primary)699 Research Concepts (primary)1000**

CanPrecede	Weakness Class	200	Information Exposure	Development Concepts699 Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Information leak through serialization

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Relationships, Taxonomy Mappings		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Information Leak through Serialization

BACK TO TOP

Spring default Html Escape Not True

Weakness ID: 10711 *(Weakness Base)* **Status:** Draft

Description

Description Summary

If the "defaultHtmlEscape" is set to false, data received as an input may not be escaped and potentialy exposing the application to XSS attacks.

Extended Description

Escaping ensures that charecters are not treated as relevant to the interperter's parser, but rather treated as data, and by this preventing XSS attacks.
If there is a proper escaping, malicious input script will not be executed.

Time of Introduction

- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example:

The following example in HTML shows us a basic mechanism of receiveng an input from a user and submitting it in a form:

(Bad Code)
Example Language: **HTML**

```
<form name="input" action="submitted.jsp" method="get">
Username:
<input type="text" name="user" />
<input type="submit" value="Submit" />
</form>
```

The following line can be submittedd by a malicious user:
<script>window.location.href="www.someMaliciousSite.com"</script>

If no escaping is used, this input might cause XSS .
However, if escaping is used the input will be treated as data and will appear as:

<script>window.location.href="www.someMaliciousSite"</script>

Potential Mitigations

Setting "defaultHtmlEscape" to true.

Race Condition

Weakness ID: 362 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code requires that certain state should not be modified between two operations, but a timing window exists in which the state can be modified by an unexpected actor or process.

Extended Description

This can have security implications when the expected synchronization is in security-critical code, such as recording whether a user is authenticated, or modifying important state information that should not be influenced by an outsider.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Architectural Paradigms

Concurrent Systems Operating on Shared Resources: *(Often)*

Common Consequences

Scope	Effect
Availability	When a race condition makes it possible to bypass a resource cleanup routine or trigger multiple initialization routines, it may lead to resource exhaustion (CWE-400).
Availability	When a race condition allows multiple control flows to access a resource simultaneously, it might lead the program(s) into unexpected states, possibly resulting in a crash.
Confidentiality Integrity	When a race condition is combined with predictable resource names and loose permissions, it may be possible for an attacker to overwrite or access confidential data (CWE-59).

Likelihood of Exploit

Medium

Detection Methods

Black Box

Black box methods may be able to identify evidence of race conditions via methods such as multiple simultaneous connections, which may cause the software to become instable or crash. However, race conditions with very narrow timing windows would not be detectable.

White Box

Common idioms are detectable in white box analysis, such as time-of-check-time-of-use (TOCTOU) file operations (CWE-367), or double-checked locking (CWE-609).

Demonstrative Examples

Example 1

This code could be used in an e-commerce application that supports transfers between accounts. It takes the total amount of the transfer, sends it to the new account, and deducts the amount from the original account.

(Bad Code)

Example Language: **Perl**

```
$transfer_amount = GetTransferAmount();
$balance = GetBalanceFromDatabase();

if ($transfer_amount < 0) {
```

```
FatalError("Bad Transfer Amount");
}
$newbalance = $balance - $transfer_amount;
if (($balance - $transfer_amount) < 0) {
FatalError("Insufficient Funds");
}
SendNewBalanceToDatabase($newbalance);
NotifyUser("Transfer of $transfer_amount succeeded.");
NotifyUser("New balance: $newbalance");
```

A race condition could occur between the calls to GetBalanceFromDatabase() and SendNewBalanceToDatabase().

Suppose the same user can invoke this program multiple times simultaneously, such as by making multiple requests in a web application. An attack could be constructed as follows:

Suppose the balance is initially 100.00.

The attacker makes two simultaneous calls of the program, CALLER-1 and CALLER-2. Both callers are for the same user account.

CALLER-1 (the attacker) is associated with PROGRAM-1 (the instance that handles CALLER-1). CALLER-2 is associated with PROGRAM-2.

CALLER-1 makes a transfer request of 80.00.

PROGRAM-1 calls GetBalanceFromDatabase and sets $balance to 100.00

PROGRAM-1 calculates $newbalance as 20.00, then calls SendNewBalanceToDatabase().

Due to high server load, the PROGRAM-1 call to SendNewBalanceToDatabase() encounters a delay.

CALLER-2 makes a transfer request of 1.00.

PROGRAM-2 calls GetBalanceFromDatabase() and sets $balance to 100.00. This happens because the previous PROGRAM-1 request was not processed yet.

PROGRAM-2 determines the new balance as 99.00.

After the initial delay, PROGRAM-1 commits its balance to the database, setting it to 20.00.

PROGRAM-2 sends a request to update the database, setting the balance to 99.00

At this stage, the attacker should have a balance of 19.00 (due to 81.00 worth of transfers), but the balance is 99.00, as recorded in the database.

To prevent this weakness, the programmer has several options, including using a lock to prevent multiple simultaneous requests to the web application, or using a synchronization mechanism that includes all the code between GetBalanceFromDatabase() and SendNewBalanceToDatabase().

Observed Examples

Reference	Description
CVE-2008-5044	Race condition leading to a crash by calling a hook removal procedure while other activities are occurring at the same time.
CVE-2008-2958	chain: time-of-check time-of-use (TOCTOU) race condition in program allows bypass of protection mechanism that was designed to prevent symlink attacks.
CVE-2008-1570	chain: time-of-check time-of-use (TOCTOU) race condition in program allows bypass of protection mechanism that was designed to prevent symlink attacks.
CVE-2008-0058	Unsynchronized caching operation enables a race condition that causes messages to be sent to a deallocated object.
CVE-2008-0379	Race condition during initialization triggers a buffer overflow.

CVE-2007-6599	Daemon crash by quickly performing operations and undoing them, which eventually leads to an operation that does not acquire a lock.
CVE-2007-6180	chain: race condition triggers NULL pointer dereference
CVE-2007-5794	Race condition in library function could cause data to be sent to the wrong process.
CVE-2007-3970	Race condition in file parser leads to heap corruption.
CVE-2008-5021	chain: race condition allows attacker to access an object while it is still being initialized, causing software to access uninitialized memory.

Potential Mitigations

Phase: Architecture and Design

In languages that support it, use synchronization primitives. Only wrap these around critical code to minimize the impact on performance.

Phase: Architecture and Design

Use thread-safe capabilities such as the data access abstraction in Spring.

Phase: Architecture and Design

Minimize the usage of shared resources in order to remove as much complexity as possible from the control flow and to reduce the likelihood of unexpected conditions occurring.

Additionally, this will minimize the amount of synchronization necessary and may even help to reduce the likelihood of a denial of service where an attacker may be able to repeatedly trigger a critical section (CWE-400).

Phase: Implementation

When using multi-threading, only use thread-safe functions on shared variables.

Phase: Implementation

Use atomic operations on shared variables. Be wary of innocent-looking constructs like "x++". This is actually non-atomic, since it involves a read followed by a write.

Phase: Implementation

Use a mutex if available, but be sure to avoid related weaknesses such as CWE-412.

Phase: Implementation

Avoid double-checked locking (CWE-609) and other implementation errors that arise when trying to avoid the overhead of synchronization.

Phase: Implementation

Disable interrupts or signals over critical parts of the code, but also make sure that the code does not go into a large or infinite loop.

Phase: Implementation

Use the volatile type modifier for critical variables to avoid unexpected compiler optimization or reordering. This does not necessarily solve the synchronization problem, but it can help.

Phase: Testing

Stress-test the software by calling it simultaneously from a large number of threads or processes, and look for evidence of any unexpected behavior. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Insert breakpoints or delays in between relevant code statements to artificially expand the race window so that it will be easier to detect.

Phase: Testing

Identify error conditions that are not likely to occur during normal usage and trigger them. For example, run the program under low memory conditions, run with insufficient privileges or permissions, interrupt a transaction before it is completed, or disable connectivity to basic network services such as DNS. Monitor the software for any unexpected behavior. If you trigger an unhandled exception or similar error that was discovered and handled by the application's environment, it may still indicate unexpected conditions that were not handled by the application itself.

Relationships

Nature	Type	ID	Name	View(s) this

				relationship pertains to
ChildOf	Category	361	Time and State	**Development Concepts (primary)699**
ChildOf	Weakness Class	691	Insufficient Control Flow Management	**Research Concepts (primary)1000**
ChildOf	Category	743	CERT C Secure Coding Section 09 - Input Output (FIO)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	61	UNIX Symbolic Link (Symlink) Following	Research Concepts1000
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Base	364	Signal Handler Race Condition	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	365	Race Condition in Switch	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	366	Race Condition within a Thread	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	367	Time-of-check Time-of-use (TOCTOU) Race Condition	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	368	Context Switching Race Condition	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	421	Race Condition During Access to Alternate Channel	Development Concepts699 Research Concepts1000
MemberOf	View	635	Weaknesses Used by NVD	**Weaknesses Used by NVD (primary)635**
CanFollow	Weakness Base	609	Double-Checked Locking	Development Concepts699 Research Concepts1000
CanFollow	Weakness Base	662	Insufficient Synchronization	Development Concepts699 Research Concepts1000
CanAlsoBe	Category	557	Concurrency Issues	Research Concepts1000

Research Gaps

Race conditions in web applications are under-studied and probably under-reported. However, in 2008 there has been growing interest in this area.

Much of the focus of race condition research has been in Time-of-check Time-of-use (TOCTOU) variants (CWE-367), but many race conditions are related to synchronization problems that do not necessarily require a time-of-check.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

PLOVER			Race Conditions
CERT C Secure Coding	FIO31-C		Do not simultaneously open the same file multiple times

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
26	Leveraging Race Conditions	
29	Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions	

References

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 13: Race Conditions." Page 205. McGraw-Hill. 2010.

Andrei Alexandrescu. "volatile - Multithreaded Programmer's Best Friend". Dr. Dobb's. 2008-02-01. <http://www.ddj.com/cpp/184403766>.

Steven Devijver. "Thread-safe webapps using Spring". <http://www.javalobby.org/articles/thread-safe/index.jsp>.

David Wheeler. "Prevent race conditions". 2007-10-04. <http://www.ibm.com/developerworks/library/l-sprace.html>.

Matt Bishop. "Race Conditions, Files, and Security Flaws; or the Tortoise and the Hare Redux". September 1995. <http://www.cs.ucdavis.edu/research/tech-reports/1995/CSE-95-9.pdf>.

David Wheeler. "Secure Programming for Linux and Unix HOWTO". 2003-03-03. <http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/avoid-race.html>.

Blake Watts. "Discovering and Exploiting Named Pipe Security Flaws for Fun and Profit". April 2002. <http://www.blakewatts.com/namedpipepaper.html>.

Roberto Paleari, Davide Marrone, Danilo Bruschi and Mattia Monga. "On Race Vulnerabilities in Web Applications". <http://security.dico.unimi.it/~roberto/pubs/dimva08-web.pdf>.

"Avoiding Race Conditions and Insecure File Operations". Apple Developer Connection. <http://developer.apple.com/documentation/Security/Conceptual/SecureCodingGuide/Articles/RaceConditions.html>.

Maintenance Notes

The relationship between race conditions and synchronization problems (CWE-662) needs to be further developed. They are not necessarily two perspectives of the same core concept, since synchronization is only one technique for avoiding race conditions, and synchronization can be used for other purposes besides race condition prevention.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Relationships		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Description, Likelihood of Exploit, Maintenance Notes, Observed Examples, Potential Mitigations, References, Relationships, Research Gaps		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Detection Factors, References, Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		

2008-04-11	Race Conditions

BACK TO TOP

Critical Public Variable Without Final Modifier

Weakness ID: 493 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product has a critical public variable that is not final, which allows the variable to be modified to contain unexpected values.

Extended Description

If a field is non-final and public, it can be changed once the value is set by any function that has access to the class which contains the field. This could lead to a vulnerability if other parts of the program make assumptions about the contents of that field.

Time of Introduction

- Implementation

Applicable Platforms

Languages

Java

C++

Common Consequences

Scope	Effect
Integrity	The object could potentially be tampered with.
Confidentiality	The object could potentially allow the object to be read.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Suppose this WidgetData class is used for an e-commerce web site. The programmer attempts to prevent price-tampering attacks by setting the price of the widget using the constructor.

(Bad Code)

Example Language: **Java**

```
public final class WidgetData extends Applet {
public float price;
...
public WidgetData(...) {
this.price = LookupPrice("MyWidgetType");
}
}
```

The price field is not final. Even though the value is set by the constructor, it could be modified by anybody that has access to an instance of WidgetData.

Example 2

Assume the following code is intended to provide the location of a configuration file that controls execution of the application.

(Bad Code)

Example Language: **C++**

```
public string configPath = "/etc/application/config.dat";
```

(Bad Code)

Example Language: **Java**

```
public String configPath = new String("/etc/application/config.dat");
```

While this field is readable from any function, and thus might allow an information leak of a pathname, a more serious problem is that it can be changed by any function.

Potential Mitigations

Phase: Implementation

Declare all public fields as final when possible, especially if it is used to maintain internal state of an Applet or of classes used by an Applet. If a field must be public, then perform all appropriate sanity checks before accessing the field from your code.

Background Details

Mobile code, such as a Java Applet, is code that is transmitted across a network and executed on a remote machine. Because mobile code developers have little if any control of the environment in which their code will execute, special security concerns become relevant. One of the biggest environmental threats results from the risk that the mobile code will run side-by-side with other, potentially malicious, mobile code. Because all of the popular web browsers execute code from multiple sources together in the same JVM, many of the security guidelines for mobile code are focused on preventing manipulation of your objects' state and behavior by adversaries who have access to the same virtual machine where your program is running.

Final provides security by only allowing non-mutable objects to be changed after being set. However, only objects which are not extended can be made final.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	216	Containment Errors (Container Errors)	Research Concepts1000
ChildOf	Weakness Class	485	Insufficient Encapsulation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	490	Mobile Code Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	500	Public Static Field Not Marked Final	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Mobile Code: Non-Final Public Field
CLASP			Failure to provide confidentiality for stored data

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Likelihood of Exploit, Relationships, Other Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Background Details, Demonstrative Examples, Description, Other Notes, Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Background Details, Demonstrative Examples, Description, Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Mobile Code: Non-final Public Field		

BACK TO TOP

Failure to Use a Standardized Error Handling Mechanism

Weakness ID: 544 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not use a standardized method for handling errors throughout the code, which might introduce inconsistent error handling and resultant weaknesses.

Extended Description

If the application handles error messages individually, on a one-by-one basis, this is likely to result in inconsistent error handling. The causes of errors may be lost. Also, detailed information about the causes of an error may be unintentionally returned to the user.

Time of Introduction

- Architecture and Design

Potential Mitigations

Phase: Architecture and Design

define a strategy for handling errors of different severities, such as fatal errors versus basic log events. Use or create built-in language features, or an external package, that provides an easy-to-use API and define coding standards for the detection and handling of errors.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	388	Error Handling	**Development Concepts (primary)699**
ChildOf	Category	746	CERT C Secure Coding Section 12 - Error Handling (ERR)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Weakness Class	755	Improper Handling of Exceptional Conditions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
Anonymous Tool Vendor (under NDA)			
CERT C Secure Coding	ERR00-C		Adopt and implement a consistent and comprehensive error-handling policy

Content History

Submissions

Submission Date	Submitter	Organization	Source
	Anonymous Tool Vendor (under NDA)		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Relationships		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Time of Introduction		

Previous Entry Names	
Change Date	**Previous Entry Name**
2009-03-10	Missing Error Handling Mechanism

BACK TO TOP

Insufficient Logging

Weakness ID: 778 *(Weakness Base)* **Status:** Draft

Description

Description Summary

When a security-critical event occurs, the software either does not record the event or omits important details about the event when logging it.

Extended Description

When security-critical events are not logged properly, such as a failed login attempt, this can make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds.

Time of Introduction

- Operation

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Accountability	If security critical information is not recorded, there will be no trail for forensic analysis and discovering the cause of problems or the source of attacks may become more difficult or impossible.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The example below shows a configuration for the service security audit feature in the Windows Communication Foundation (WCF).

(Bad Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="None"
messageAuthenticationAuditLevel="None" />
...
</system.serviceModel>
```

The previous configuration file has effectively disabled the recording of security-critical events, which would force the administrator to look to other sources during debug or recovery efforts.

Logging failed authentication attempts can warn administrators of potential brute force attacks. Similarly, logging successful authentication events can provide a useful audit trail when a legitimate account is compromised. The following configuration shows appropriate settings, assuming that the site does not have excessive traffic, which could fill the logs if there are a large number of success or failure events (CWE-779).

(Good Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="SuccessAndFailure"
messageAuthenticationAuditLevel="SuccessAndFailure" />
...
</system.serviceModel>
```

Observed Examples

Reference	Description
CVE-2008-4315	server does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2008-1203	admin interface does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2007-3730	default configuration for POP server does not log source IP or username for login attempts
CVE-2007-1225	proxy does not log requests without "http://" in the URL, allowing web surfers to access restricted web content without detection
CVE-2003-1566	web server does not log requests for a non-standard request type

Potential Mitigations

Phase: Architecture and Design

Use a centralized logging mechanism that supports multiple levels of detail. Ensure that all security-related successes and failures can be logged.

Phase: Operation

Be sure to set the level of logging appropriately in a production environment. Sufficient data should be logged to enable system administrators to detect attacks, diagnose errors, and recover from attacks. At the same time, logging too much data (CWE-779) can cause the same problems.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	223	Omission of Security-relevant Information	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	254	Security Features	Development Concepts699
ChildOf	Weakness Class	693	Protection Mechanism Failure	Research Concepts1000

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2009-07-02			Internal CWE Team
Contributions			
Contribution Date	**Contributor**	**Organization**	**Source**
2009-07-02		Fortify Software	Content
	Provided code example and additional information for description and consequences.		

BACK TO TOP

Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')

Weakness ID: 89 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Extended Description

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.

SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

All

Technology Classes

Database-Server

Modes of Introduction

This weakness typically appears in data-rich applications that save user inputs in a database.

Common Consequences

Scope	Effect
Confidentiality	Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL injection vulnerabilities.
Authentication	If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
Authorization	If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL injection vulnerability.
Integrity	Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL injection attack.

Likelihood of Exploit

Very High

Enabling Factors for Exploitation

The application dynamically generates queries that contain user input.

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis might not be able to recognize when proper input validation is being performed, leading to false positives - i.e., warnings that do not have any security consequences or do not require any code changes.

Automated static analysis might not be able to detect the usage of custom API functions or third-party libraries that indirectly invoke SQL commands, leading to false negatives - especially if the API/library code is not available for analysis.

Manual Analysis

Manual analysis can be useful for finding this weakness, but it might not achieve desired code coverage within limited time constraints. This becomes difficult for weaknesses that must be considered for all inputs, since the attack surface can be too large.

Demonstrative Examples

Example 1

In 2008, a large number of web servers were compromised using the same SQL injection attack string. This single string worked against many different programs. The SQL injection was then used to modify the web sites to serve malicious code. [1]

Example 2

The following code dynamically constructs and executes a SQL query that searches for items matching a specified name. The query restricts the items displayed to those where owner matches the user name of the currently-authenticated user.

(Bad Code)

Example Language: **C#**

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '" + userName + "' AND itemname = '" + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

The query that this code intends to execute follows:

```
SELECT * FROM items WHERE owner = <userName> AND itemname = <itemName>;
```

However, because the query is constructed dynamically by concatenating a constant base query string and a user input string, the query only behaves correctly if itemName does not contain a single-quote character. If an attacker with the user name wiley enters the string:

(Attack)

```
name' OR 'a'='a
```

for itemName, then the query becomes the following:

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

The addition of the:

(Attack)

```
OR 'a'='a'
```

condition causes the WHERE clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query:

(Attack)

```
SELECT * FROM items;
```

This simplification of the query allows the attacker to bypass the requirement that the query only return items owned by the authenticated user; the query now returns all entries stored in the items table, regardless of their specified owner.

Example 3

This example examines the effects of a different malicious value passed to the query constructed and executed in the previous example.

If an attacker with the user name wiley enters the string:

(Attack)

```
name'; DELETE FROM items; --
```

for itemName, then the query becomes the following two queries:

(Attack)

Example Language: **SQL**

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
--'
```

Many database servers, including Microsoft(R) SQL Server 2000, allow multiple SQL statements separated by semicolons to be executed at once. While this attack string results in an error on Oracle and other database servers that do not allow the batch-execution of statements separated by semicolons, on databases that do allow batch execution, this type of attack allows the attacker to execute arbitrary commands against the database.

Notice the trailing pair of hyphens (--), which specifies to most database servers that the remainder of the statement is to be treated as a comment and not executed. In this case the comment character serves to remove the trailing single-quote left over from the modified query. On a database where comments are not allowed to be used in this way, the general attack could still be made effective using a trick similar to the one shown in the previous example.

If an attacker enters the string

(Attack)

```
name'; DELETE FROM items; SELECT * FROM items WHERE 'a'='a
```

Then the following three valid statements will be created:

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
SELECT * FROM items WHERE 'a'='a';
```

One traditional approach to preventing SQL injection attacks is to handle them as an input validation problem and either accept only characters from a whitelist of safe values or identify and escape a blacklist of potentially malicious values. Whitelisting can be a very effective means of enforcing strict input validation rules, but parameterized SQL statements require less maintenance and can offer more guarantees with respect to security. As is almost always the case, blacklisting is riddled with loopholes that make it ineffective at preventing SQL injection attacks. For example, attackers can:

- Target fields that are not quoted
- Find ways to bypass the need for certain escaped meta-characters
- Use stored procedures to hide the injected meta-characters.

Manually escaping characters in input to SQL queries can help, but it will not make your application secure from SQL injection attacks.

Another solution commonly proposed for dealing with SQL injection attacks is to use

stored procedures. Although stored procedures prevent some types of SQL injection attacks, they fail to protect against many others. For example, the following PL/SQL procedure is vulnerable to the same SQL injection attack shown in the first example.

(Bad Code)

```
procedure get_item ( itm_cv IN OUT ItmCurTyp, usr in varchar2, itm in varchar2)
is open itm_cv for
' SELECT * FROM items WHERE ' || 'owner = '|| usr || ' AND itemname = ' || itm || ';
end get_item;
```

Stored procedures typically help prevent SQL injection attacks by limiting the types of statements that can be passed to their parameters. However, there are many ways around the limitations and many interesting statements that can still be passed to stored procedures. Again, stored procedures can prevent some exploits, but they will not make your application secure against SQL injection attacks.

Example 4

MS SQL has a built in function that enables shell command execution. An SQL injection in such a context could be disastrous. For example, a query of the form:

(Bad Code)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='$user_input' ORDER BY PRICE
```

Where $user_input is taken from the user and unfiltered.

If the user provides the string:

(Attack)

```
' exec master..xp_cmdshell 'vol' --
```

The query will take the following form: "

(Attack)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='' exec master..xp_cmdshell 'vol' --' ORDER BY PRICE
```

Now, this query can be broken down into:

- [1] a first SQL query: SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY=''
- [2] a second SQL query, which executes a shell command: exec master..xp_cmdshell 'vol'
- [3] an MS SQL comment: --' ORDER BY PRICE

As can be seen, the malicious input changes the semantics of the query into a query, a shell command execution and a comment.

Example 5

This code intends to print a message summary given the message ID.

(Bad Code)

Example Language: **PHP**

```
$id = $_COOKIE["mid"];
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

The programmer may have skipped any input validation on $id under the assumption that attackers cannot modify the cookie. However, this is easy to do with custom client code or even in the web browser.

While $id is wrapped in single quotes in the call to mysql_query(), an attacker could simply change the incoming mid cookie to:

(Attack)

```
1432' or '1' = '1
```

This would produce the resulting query:

(Result)

```
SELECT MessageID, Subject FROM messages WHERE MessageID = '1432' or '1' = '1'
```

Not only will this retrieve message number 1432, it will retrieve all other messages.

In this case, the programmer could apply a simple modification to the code to eliminate the SQL injection:

(Good Code)

Example Language: **PHP**

```
$id = intval($_COOKIE["mid"]);
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

However, if this code is intended to support multiple users with different message boxes, the code might also need an access control check (CWE-285) to ensure that the application user has the permission to see that message.

Example 6

This example attempts to take a last name provided by a user and enter it into a database.

(Bad Code)

Example Language: **Perl**

```
$userKey = getUserID();
$name = getUserInput();
# ensure only letters, hyphens and apostrophe are allowed
$name = whiteList($name, "^a-zA-z'-$");
$query = "INSERT INTO last_names VALUES('$userKey', '$name')";
```

While the programmer applies a whitelist to the user input, it has shortcomings. First of all, the user is still allowed to provide hyphens which are used as comment structures in SQL. If a user specifies -- then the remainder of the statement will be treated as a comment, which may bypass security logic. Furthermore, the whitelist permits the apostrophe which is also a data / command separator in SQL. If a user supplies a name with an apostrophe, they may be able to alter the structure of the whole statement and even change control flow of the program, possibly accessing or modifying confidential information. In this situation, both the hyphen and apostrophe are legitimate characters for a last name and permitting them is required. Instead, a programmer may want to use a prepared statement or apply an encoding routine to the input to prevent any data / directive misinterpretations.

Observed Examples

Reference	Description
CVE-2004-0366	chain: SQL injection in library intended for database authentication allows SQL injection and authentication bypass.
CVE-2008-2790	SQL injection through an ID that was supposed to be numeric.
CVE-2008-2223	SQL injection through an ID that was supposed to be numeric.
CVE-2007-6602	SQL injection via user name.
CVE-2008-5817	SQL injection via user name or password fields.
CVE-2003-0377	SQL injection in security product, using a crafted group name.
CVE-2008-2380	SQL injection in authentication library.

Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using persistence layers such as Hibernate or Enterprise Java Beans, which can provide significant

protection against SQL injection if used properly.

Phase: Architecture and Design

Strategy: Parameterization

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

Process SQL queries using prepared statements, parameterized queries, or stored procedures. These features should accept parameters or variables and support strong typing. Do not dynamically construct and execute query strings within these features using "exec" or similar functionality, since you may re-introduce the possibility of SQL injection.

Phase: Architecture and Design

Follow the principle of least privilege when creating user accounts to a SQL database. The database users should only have the minimum privileges necessary to use their account. If the requirements of the system indicate that a user can read and modify their own data, then limit their privileges so they cannot read/write others' data. Use the strictest permissions possible on all database objects, such as execute-only for stored procedures.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phase: Implementation

If you need to use dynamically-generated query strings in spite of the risk, use proper encoding and escaping of inputs. Instead of building your own implementation, such features may be available in the database or programming language. For example, the Oracle DBMS_ASSERT package can check or enforce that parameters have certain properties that make them less vulnerable to SQL injection. For MySQL, the mysql_real_escape_string() API function is available in both C and PHP.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

When constructing SQL query strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing SQL injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent SQL injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, the name "O'Reilly" would likely pass the validation step, since it is a common last name in the English language. However, it cannot be directly inserted into the database because it contains the "'" apostrophe character, which would need to be escaped or otherwise handled. In this case, stripping the apostrophe might reduce the risk of SQL injection, but it would produce incorrect behavior because the wrong name would be recorded.

When feasible, it may be safest to disallow meta-characters entirely, instead of escaping them. This will provide some defense in depth. After the data is entered into the database, later processes may neglect to escape meta-characters before use, and you may not have control over those processes.

Phases: Testing; Implementation

Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Phase: Testing

Use dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Phase: Operation

Use an application firewall that can detect attacks against this weakness. This might not catch all attacks, and it might require some effort for customization. However, it can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	77	Improper Sanitization of Special Elements used in a Command ('Command Injection')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711
ChildOf	Category	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	564	SQL Injection: Hibernate	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
MemberOf	View	635	Weaknesses Used by NVD	**Weaknesses Used by NVD (primary)635**
CanFollow	Weakness Base	456	Missing Initialization	Research Concepts1000

Relationship Notes

SQL injection can be resultant from special character mismanagement, MAID, or blacklist/whitelist problems. It can be primary to authentication errors.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			SQL injection
7 Pernicious Kingdoms			SQL Injection
CLASP			SQL injection
OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws
WASC	19		SQL Injection

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
7	Blind SQL Injection	
66	SQL Injection	
108	Command Line Execution through SQL Injection	
109	Object Relational Mapping Injection	
110	SQL Injection through SOAP Parameter	

	Tampering

White Box Definitions

A weakness where the code path has:

1. start statement that accepts input and

2. end statement that performs an SQL command where

a. the input is part of the SQL command and

b. input contains SQL syntax (esp. query separator)

References

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 1: SQL Injection." Page 3. McGraw-Hill. 2010.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 12, "Database Input Issues" Page 397. 2nd Edition. Microsoft. 2002.

OWASP. "SQL Injection Prevention Cheat Sheet". <http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>.

Steven Friedl. "SQL Injection Attacks by Example". 2007-10-10. <http://www.unixwiz.net/techtips/sql-injection.html>.

Ferruh Mavituna. "SQL Injection Cheat Sheet". 2007-03-15. <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>.

David Litchfield, Chris Anley, John Heasman and Bill Grindlay. "The Database Hacker's Handbook: Defending Database Servers". Wiley. 2005-07-14.

David Litchfield. "The Oracle Hacker's Handbook: Hacking and Defending Oracle". Wiley. 2007-01-30.

Microsoft. "SQL Injection". December 2008. <http://msdn.microsoft.com/en-us/library/ms161953.aspx>.

Microsoft Security Vulnerability Research & Defense. "SQL Injection Attack". <http://blogs.technet.com/swi/archive/2008/05/29/sql-injection-attack.aspx>.

Michael Howard. "Giving SQL Injection the Respect it Deserves". 2008-05-15. <http://blogs.msdn.com/sdl/archive/2008/05/15/giving-sql-injection-the-respect-it-deserves.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
	7 Pernicious Kingdoms		Externally Mined
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Modes of Introduction, Name, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Observed Examples		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Enabling Factors for Exploitation, Modes of Introduction, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name, Related Attack Patterns		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description, Name, White Box Definitions		
2009-12-28	CWE Content Team	MITRE	Internal

	updated Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	SQL Injection
2008-09-09	Failure to Sanitize Data into SQL Queries (aka 'SQL Injection')
2009-01-12	Failure to Sanitize Data within SQL Queries (aka 'SQL Injection')
2009-05-27	Failure to Preserve SQL Query Structure (aka 'SQL Injection')
2009-07-27	Failure to Preserve SQL Query Structure ('SQL Injection')

BACK TO TOP

Serializable Class Containing Sensitive Data

Weakness ID: 499 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code contains a class with sensitive data, but the class does not explicitly deny serialization. The data can be accessed by serializing the class through another class.

Extended Description

Serializable classes are effectively open classes since data cannot be hidden in them. Classes that do not explicitly deny serialization can be serialized by any other class, which can then in turn use the data stored inside it.

Time of Introduction

- Implementation

Applicable Platforms

Languages

Java

Common Consequences

Scope	Effect
Confidentiality	an attacker can write out the class to a byte stream, then extract the important data from it.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

(Bad Code)

Example Language: **Java**

```
class Teacher {
private String name;
private String clas;
public Teacher(String name,String clas) {

//...
//Check the database for the name and address
this.SetName() = name;
this.Setclas() = clas;
}
}
```

Potential Mitigations

Phase: Implementation

In Java, explicitly define final writeObject() to prevent serialization. This is the recommended solution. Define the writeObject() function to throw an exception explicitly denying serialization.

Phase: Implementation

Make sure to prevent serialization of your objects.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	485	Insufficient Encapsulation	**Development Concepts (primary)699 Research Concepts (primary)1000**

CanPrecede	Weakness Class	200	Information Exposure	Development Concepts699 Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Information leak through serialization

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Relationships, Taxonomy Mappings		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Information Leak through Serialization

BACK TO TOP

Use of Obsolete Functions

Weakness ID: 477 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses deprecated or obsolete functions, which suggests that the code has not been actively reviewed or maintained.

Time of Introduction

- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses the deprecated function getpw() to verify that a plaintext password matches a user's encrypted password. If the password is valid, the function sets result to 1; otherwise it is set to 0.

(Bad Code)

Example Language: **C**

```
...
getpw(uid, pwdline);
for (i=0; i<3; i++){
cryptpw=strtok(pwdline, ":");
pwdline=0;
}
result = strcmp(crypt(plainpw,cryptpw), cryptpw) == 0;
...
```

Although the code often behaves correctly, using the getpw() function can be problematic from a security standpoint, because it can overflow the buffer passed to its second parameter. Because of this vulnerability, getpw() has been supplanted by getpwuid(), which performs the same lookup as getpw() but returns a pointer to a statically-allocated structure to mitigate the risk. Not all functions are deprecated or replaced because they pose a security risk. However, the presence of an obsolete function often indicates that the surrounding code has been neglected and may be in a state of disrepair. Software security has not been a priority, or even a consideration, for very long. If the program uses deprecated or obsolete functions, it raises the probability that there are security problems lurking nearby.

Example 2

In the following code, the programmer assumes that the system always has a property named "cmd" defined. If an attacker can control the program's environment so that "cmd" is not defined, the program throws a null pointer exception when it attempts to call the "Trim()" method.

(Bad Code)

Example Language: **Java**

```
String cmd = null;
...
cmd = Environment.GetEnvironmentVariable("cmd");
cmd = cmd.Trim();
```

Example 3

The following code constructs a string object from an array of bytes and a value that

specifies the top 8 bits of each 16-bit Unicode character.

(Bad Code)

Example Language: **Java**

```
...
String name = new String(nameBytes, highByte);
...
```

In this example, the constructor may fail to correctly convert bytes to characters depending upon which charset is used to encode the string represented by nameBytes. Due to the evolution of the charsets used to encode strings, this constructor was deprecated and replaced by a constructor that accepts as one of its parameters the name of the charset used to encode the bytes for conversion.

Potential Mitigations

Consider seriously the security implication of using an obsolete function. Consider using alternate functions.

The system should warn the user from using an obsolete function.

Other Notes

As programming languages evolve, functions occasionally become obsolete due to:

- Advances in the language
- Improved understanding of how operations should be performed effectively and securely
- Changes in the conventions that govern certain operations

Functions that are removed are usually replaced by newer counterparts that perform the same task in some different and hopefully improved way. Refer to the documentation for this function in order to determine why it is deprecated or obsolete and to learn about alternative ways to achieve the same functionality. The remainder of this text discusses general problems that stem from the use of deprecated or obsolete functions.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Obsolete

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-01-30	Obsolete		

BACK TO TOP

Insufficient Logging

Weakness ID: 778 *(Weakness Base)* **Status:** Draft

Description

Description Summary

When a security-critical event occurs, the software either does not record the event or omits important details about the event when logging it.

Extended Description

When security-critical events are not logged properly, such as a failed login attempt, this can make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds.

Time of Introduction

- Operation

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Accountability	If security critical information is not recorded, there will be no trail for forensic analysis and discovering the cause of problems or the source of attacks may become more difficult or impossible.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The example below shows a configuration for the service security audit feature in the Windows Communication Foundation (WCF).

(Bad Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="None"
messageAuthenticationAuditLevel="None" />
...
</system.serviceModel>
```

The previous configuration file has effectively disabled the recording of security-critical events, which would force the administrator to look to other sources during debug or recovery efforts.

Logging failed authentication attempts can warn administrators of potential brute force attacks. Similarly, logging successful authentication events can provide a useful audit trail when a legitimate account is compromised. The following configuration shows appropriate settings, assuming that the site does not have excessive traffic, which could fill the logs if there are a large number of success or failure events (CWE-779).

(Good Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="SuccessAndFailure"
messageAuthenticationAuditLevel="SuccessAndFailure" />
...
</system.serviceModel>
```

Observed Examples

Reference	Description
CVE-2008-4315	server does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2008-1203	admin interface does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2007-3730	default configuration for POP server does not log source IP or username for login attempts
CVE-2007-1225	proxy does not log requests without "http://" in the URL, allowing web surfers to access restricted web content without detection
CVE-2003-1566	web server does not log requests for a non-standard request type

Potential Mitigations

Phase: Architecture and Design

Use a centralized logging mechanism that supports multiple levels of detail. Ensure that all security-related successes and failures can be logged.

Phase: Operation

Be sure to set the level of logging appropriately in a production environment. Sufficient data should be logged to enable system administrators to detect attacks, diagnose errors, and recover from attacks. At the same time, logging too much data (CWE-779) can cause the same problems.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	223	Omission of Security-relevant Information	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	254	Security Features	Development Concepts699
ChildOf	Weakness Class	693	Protection Mechanism Failure	Research Concepts1000

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2009-07-02			Internal CWE Team
Contributions			
Contribution Date	**Contributor**	**Organization**	**Source**
2009-07-02		Fortify Software	Content
	Provided code example and additional information for description and consequences.		

BACK TO TOP

Lenguajes escaneados

Lenguajes	Número hash	Cambiar fecha
Java	0188428345217368	30/07/2018
JavaScript	0109410431041810	30/07/2018
VbScript	2005446206231574	30/07/2018
Common	0148805192553332	21/01/2022