

Seguridad de aplicaciones Java/JakartaEE con OWASP Top 10

Víctor Orozco - @tuxtor

17 de mayo de 2020

Academik



ACADEMIK

Principios básicos

- No existe un framework generico para hacer "seguridad 360"
- Seguridad = Balance entre necesidad de negocio/tecnología
- En Java hay n formas de hacer lo mismo
- Requerimientos -> Cifrado, firmas digitales, autenticación, autorización
- Herramientas

¿Java?

- Lenguaje
- VM
- Bibliotecas/API

El conjunto es la plataforma Java

¿Java?

- Lenguaje
- VM
- Bibliotecas/API

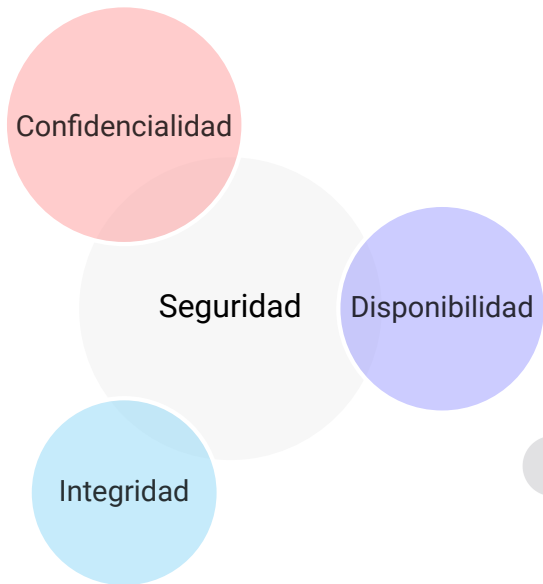
El conjunto es la plataforma Java (TM)

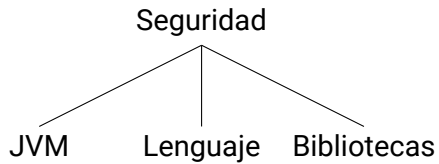


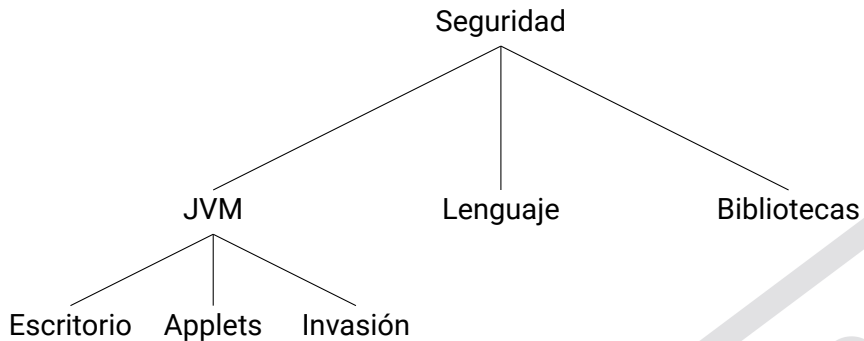
ACADEMIK

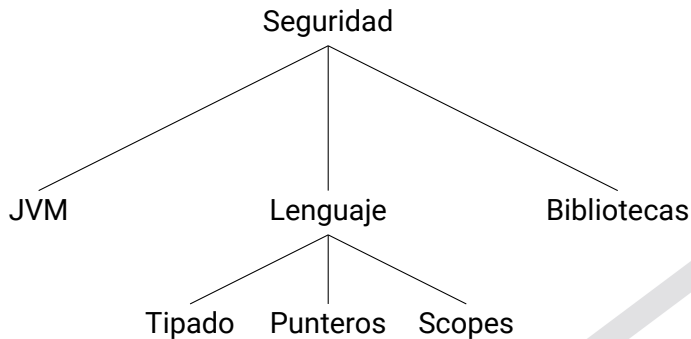
Seguridad en Java

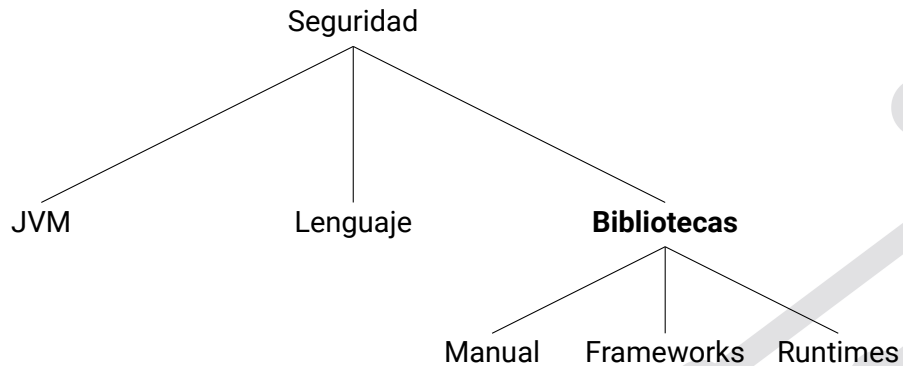












Bibliotecas

¿Cual?

- Apache Shiro
- Spring Security
- OACC
- Keycloak
- JGuard
- JACC
- SoteriaRI
- MicroProfile JWT

...

@tuxtor



Render en servidor

- JSF (Icefaces, Primefaces)
- GWT
- JSP
- Servlets
- Vaadin
- Struts
- Spring MVC

Render en servidor

- JSF (Icefaces, Primefaces)
- GWT
- JSP
- Servlets
- Vaadin
- Struts
- Spring MVC

Render en cliente

- Angular
- React
- Knockout (Oracle JET)
- Vue

Render en servidor

- JSF (Icefaces, Primefaces)
- GWT
- JSP
- Servlets
- Vaadin
- Struts
- Spring MVC

Render en cliente

- Angular
- React
- Knockout (Oracle JET)
- Vue

Servicios

- SOAP
- Rest
- RMI

ORACLE®



PostgreSQL



MySQL®



mongoDB®

@tuxto



ORACLE®
LINUX



Java®
ENTERPRISE
EDITION



- Mejor integración de JSF con CDI
- Mejor integración de JMS con CDI
- HTTP/2
- JSON-B
- Security
- JAX-RS Reactivo

Java EE 8



Batch	Dependency Injection	JACC	JAXR	JSTL	Management
Bean Validation	Deployment	JASPIC	JMS	JTA	Servlet
CDI	EJB	JAX-RPC	JSF	JPA	Web Services
Common Annotations	EL	JAX-RS	JSON-P	JavaMail	Web Services Metadata
Concurrency EE	Interceptors	JAX-WS	JSP	Managed Beans	WebSocket
Connector	JSP Debugging	JAXB			
JSON-B	Security				

EE vs OWASP Top 10

- Visto en N desarrollos
- Un punto de inicio
- Informar

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Sensitive Data Exposure
- A4-XML External Entities
- A5-Broken Access Control
- A6-Security Misconfiguration
- A7-Cross-Site Scripting (XSS)
- A8-Insecure deserialization
- A9-Using Components with Known Vulnerabilities
- A10-Insufficient Logging y Monitoring

<https://owasp.org/www-project-top-ten/>

- **A1-Injection**
- **A2-Broken Authentication and Session Management**
- **A3-Sensitive Data Exposure**
- A4-XML External Entities
- **A5-Broken Access Control**
- **A6-Security Misconfiguration**
- A7-Cross-Site Scripting (XSS)
- **A8-Insecure deserialization**
- **A9-Using Components with Known Vulnerabilities**
- A10-Insufficient Logging y Monitoring

https://www.owasp.org/index.php/Top_10_2017-Top_10

Problemas y causas comunes

- Concatenación de Strings en SQL
- Datos mal intencionados a aplicaciones
- Manipulación data stores
- Escalar privilegios

Sugerencias

- JAMAS y NUNCA concatenar parametros
- Siempre utilizar mecanismos de sanitizing
- Parchar con OWASP ESAPI
- JDBC y JPA soportan de serie sanitizing si no se concatena
- Bean Validation en parametros

Peligro

```
1 String query = "SELECT p FROM AdmPhrase p " +  
2 "where p.author LIKE " + autor +  
3 "and p.phrase LIKE " + phrase;
```

Mejor

```
1 String query = "SELECT p FROM AdmPhrase p " +  
2 "where p.author LIKE :author " +  
3 "and p.phrase LIKE :phrase";  
4  
5 return em.createQuery(query, AdmPhrase.class)  
6     .setParameter("author", autor)  
7     .setParameter("phrase", phrase)  
8     .getResultList();
```

Problemas y causas comunes

- Implementación de solución manual vs frameworks
- Falta de políticas
- Entrenamiento en la plataforma
- Comunicación y/o autenticación via http

Sugerencias

- Forzar https
- Utilizar adecuadamente los ciclos de vida de la plataforma (singleton != stateless != statefull) y cache
- No implementar en base a interceptores unicamente

JavaEE - A2-Broken Authentication and Session Management

App rest normal

```
1 public class DemoinfosecRestApplication extends Application {}
```

Activar mecanismo de autenticación (MicroProfile JWT)

```
1 @LoginConfig(authMethod = "MP-JWT")
2 @DeclareRoles({RolesEnum.Constants.MOBILE_VALUE, RolesEnum.
   Constants.WEB_VALUE})
3 public class DemoinfosecRestApplication extends Application {}
```

Problemas y causas comunes

- Guardar datos sin cifrar
- Datos con cifrado "debil", AKA cifrado propio
- Transmitir credenciales via http
- Transmisión de excepciones completas a front-end

Sugerencias

- Identificar con un checklist los datos sensitivos
- Evitar cifrado de dos vías a menos que sea necesario
- Evitar transmisión de llaves
- Verificar código auto generado (excepciones)

Problemas y causas comunes

- Implementación de solución manual vs frameworks
- Falta de políticas
- Escalar privilegios
- Comunicación y/o autenticación via http

Sugerencias

- Forzar https
- Implementación RBAC de application server
- Implementación RBAC de framework
- Entender el modelo de JAAS, SoteriaRI y MicroProfile security

JavaEE - A5-Broken Access Control

Endpoint normal

```
1 @GET
2 @Path("/{id:[0-9][0-9]*}")
3 public AdmPhrase findById(@PathParam("id") Long id) {
4     return admPhraseRepository.findById(id);
5 }
```

Endpoint con RBAC

```
1 @GET
2 @Path("/{id:[0-9][0-9]*}")
3 @RolesAllowed({RolesEnum.Constants.MOBILE_VALUE, RolesEnum.
4     Constants.WEB_VALUE})
5 public AdmPhrase findById(@PathParam("id") Long id) {
6     return admPhraseRepository.findById(id);
7 }
```

Problemas y causas comunes

- Configuración por defecto de application server
- Configuración por defecto de SO
- Configuración relajada de capa de transporte

Sugerencias

- Configurar siempre el SO destino
- Proteger y actualizar runtime
- Firewall
- RBAC
- Evitar certificados autofirmados en entornos no controlados
- JVM tipo server

Problemas y causas comunes

- Self made frameworks
- No validation

Sugerencias

- Evaluar si no vale la pena utilizar un software listo
- Bean validation
- Sanitización

Problemas y causas comunes

- Difícil dar seguimiento a los lanzamientos
- Frameworks muy nuevos o muy viejos
- No seguir las notas del lanzamiento

Sugerencias

- Actualizar el app server con el calendario de lanzamiento
- Suscripción a mailing list/foros
- Servicios tipo Bintray, GitHub Security
- Servicios de análisis estático (Sonar)

JavaEE - A9-Using components with known vulnerabilities

Bump nimbus-jose-jwt from 5.7 to 7.9 #1

[Edit](#)

tuxtort merged 1 commit into `master` from `dependabot/maven/com.nimbusds-nimbus-jose-jwt-7.9` on Oct 16, 2019

🛡️ This automated pull request fixes a security vulnerability

Only users with access to security alerts can see this message. [Learn more about automated security updates](#), [opt out](#), or [give us feedback](#).

💬 Conversation 1

🔗 Commits 1

🔍 Checks 0

📄 Files changed 1

+1 -1 🇩🇪 🇬🇧 🇮🇹



dependabot bot commented on behalf of `github` on Oct 16, 2019

Contributor



Bumps `nimbus-jose-jwt` from 5.7 to 7.9.

► Changelog

► Commits

🔗 compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

► Dependabot commands and options

Reviewers



No reviews

Assignees



No one—assign yourself

Labels



dependencies

Projects



None yet

Milestone



No milestone

@tuxto

3.0 GT) 27

Problemas y causas comunes

- Combinación de broken auth, broken access control o security misconfiguration
- No hay nada
- Especialmente grave en rich clients

Sugerencias

- Verificar código auto generado
- Programar en modo deny all



ACADEMIK

Demo



File Users

Back

Manage user accounts for the currently selected security realm.

Configuration Name: server-config

Realm Name: burgerland

File Users (2)

New...Delete

Select	User ID	Group List:
<input type="checkbox"/>	ronald	web
<input type="checkbox"/>	king	mobile

- Proveedor de tokens <https://github.com/tuxtor/microjwt-provider/>
- API protegida <https://github.com/tuxtor/demoinfosec-service-b/>



Oracle
Groundbreakers



ORACLE®
Certified Professional
Java SE 8 Programmer

ORACLE®
Certified Associate
Java SE 8 Programmer

- vorozco@nabenik.com
- @tuxtor
- <http://voroazco.com>
- <http://tuxtor.shekalug.org>



This work is licensed under
Creative Commons Attribution-
NonCommercial-ShareAlike 3.0
Guatemala (CC BY-NC-SA 3.0 GT).



ACADEMIK

Esríbenos a cursos@academik.io

www.academik.io

(CC BY-NC-SA3.0 GT)