ascentic/

Bloque II

Taller mitigación y pruebas Web con Java

Bloques del curso

Bloque I - Introducción al Desarrollo Seguro

Bloque II - Taller mitigación y Pruebas Web con Java

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Diciembre		1	2	1	2	3	4
	5	6	7	8	9	10	11
	12	13	14	15	16	17	18
	19	20	21	22	23	24	25
	26	27	28	29	30	31	

Horario

- De 8:00 a 11:00
  - 5 minutos de descanso: 9:30 a 9:35

Sobre el profesor

- Más de 25 años de experiencia en el sector y todos estos años compaginando la formación con el desarrollo y el I+D+I
- En formación empecé sobre con asignaturas de programación y los últimos años sobre todo BootCamps así como formación a perfiles de desarrollo seniors.
- Actualmente perfil de arquitecto software, aunque he pasado por casi todos los roles.
- Especialidades:
  - SDLC (CI/CD)
  - Computación en la nube
  - Seguridad en el desarrollo, criptografía
  - Data Science
  - Arquitecturas distribuidas e Integración de sistemas

https://www.linkedin.com/in/juan-antonio-l-373571113/

Repositorio de ficheros

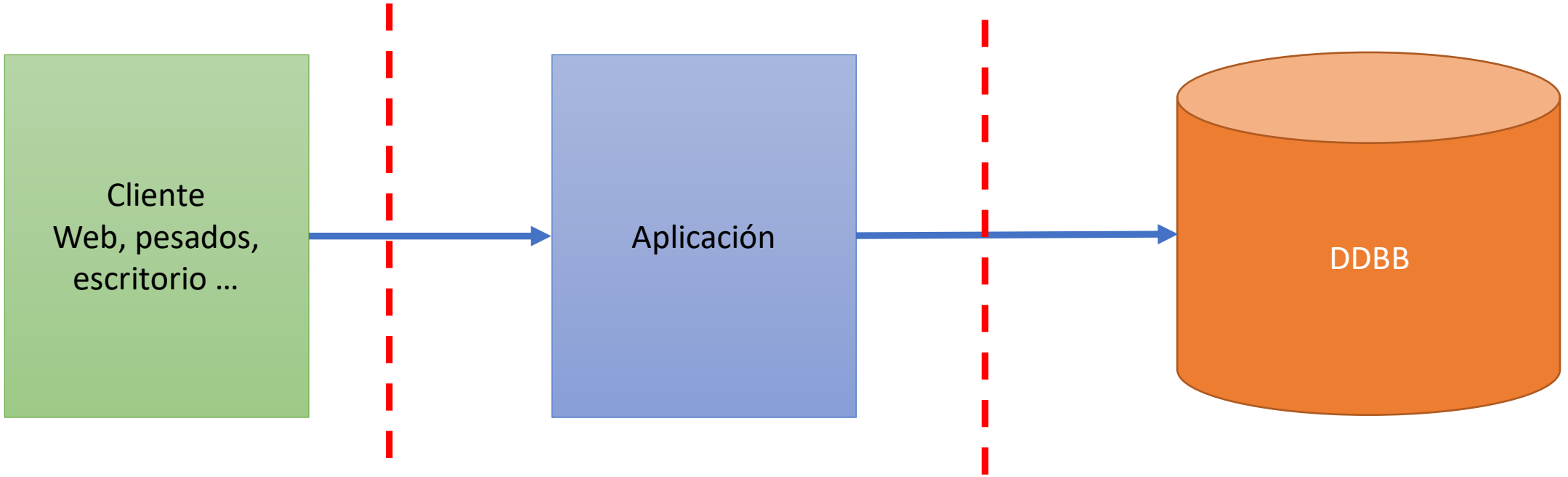
https://github.com/desarrollo-seguro/web-java-4

Contenidos

1. Arquitecturas servidor java, transiciones de páginas, SPAs y apis REST.
2. Spring MVC y Spring Boot: especificaciones vs frameworks
3. Estándares OWASP y OWASP Testing Guide
4. Verificación de la gestión de sesiones
5. Verificación del control de acceso
6. Verificación de entrada maliciosa
7. Verificación de la criptografía
8. Verificación del logging y manejo de errores
9. Verificación de la protección de datos
10. Verificación de la seguridad en las comunicaciones
11. Verificación de la configuración de seguridad HTTP
12. Verificación de los controles maliciosos
13. Verificación de la lógica de negocio
14. Verificación de los recursos y ficheros

1. Arquitecturas servidor java, transiciones de páginas, SPAs y apis REST

Arquitecturas: Evolución

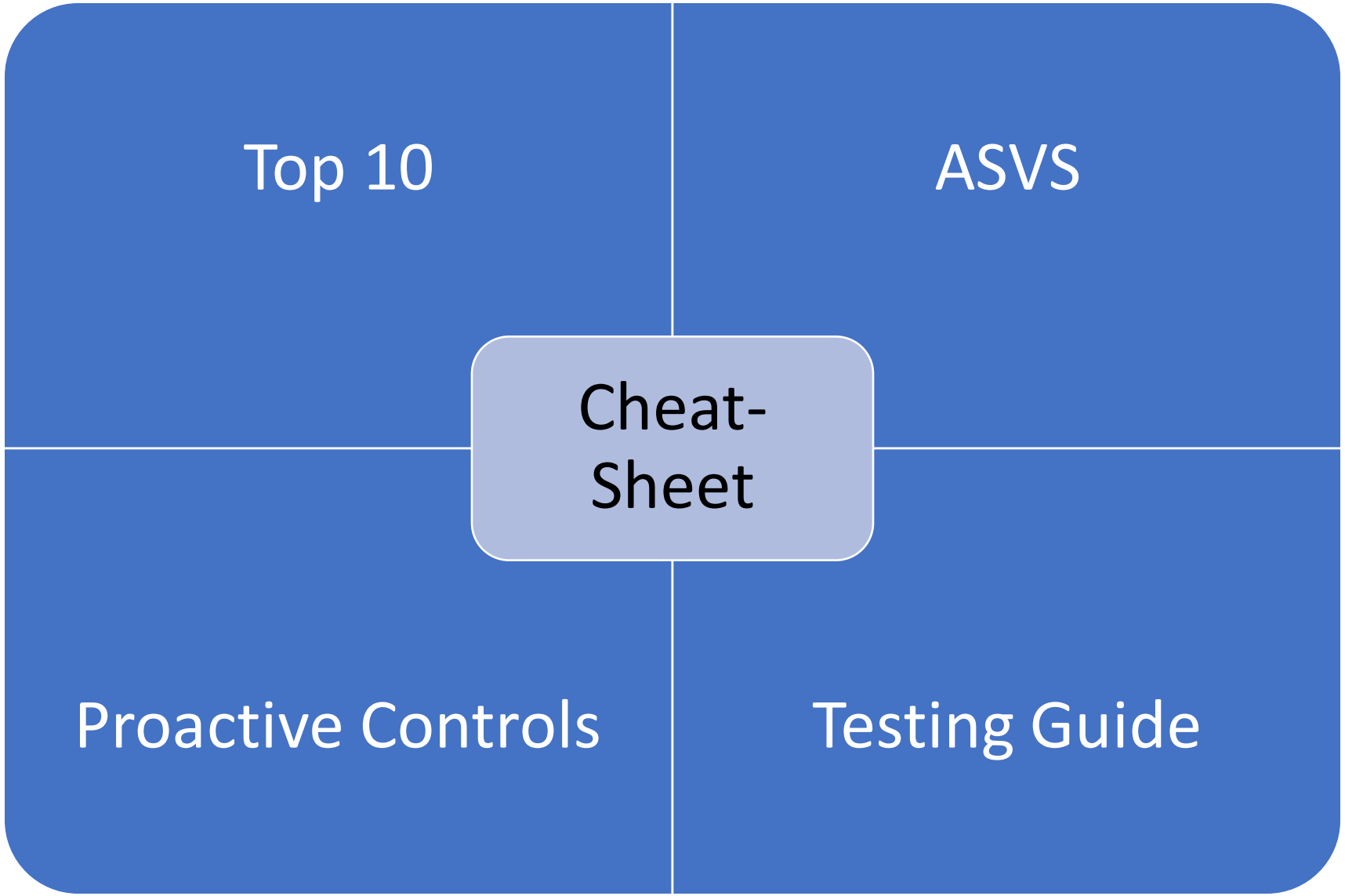


2. Spring MVC y Spring Boot: especificaciones vs frameworks

Un poco de historia

- Java: ¿Lenguaje para lavadoras?
- Evolución relativamente rápida, soporte para aplicaciones Web
- Muy relacionado con el mundo Open Source
- Durante unos años se extendió a otros modelos: aplicaciones móviles
- Las controversias con Oracle
- Spring, modelo alternativo a JEE (JakartaEE)
- Inyección de dependencias… revisited

3. Estándares OWASP y OWASP Testing Guide



Y unimos a estos el Security Knowledge Framework:
https://owasp.org/www-project-security-knowledge-framework/

Pen-Testing

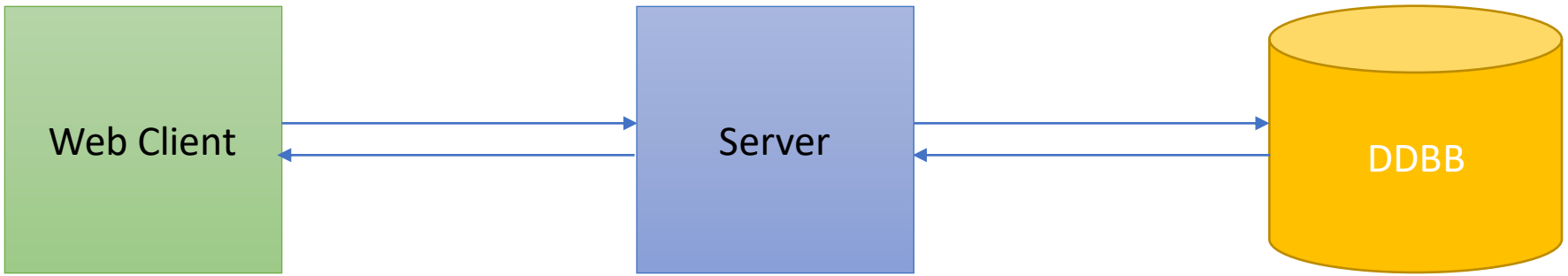
1. Planificación y reconocimiento
2. Escaneo
3. Obteniendo acceso
4. Mantener el acceso
5. Análisis y contramedidas
6. … vuelta al 1

Páginas mezclando datos + presentación

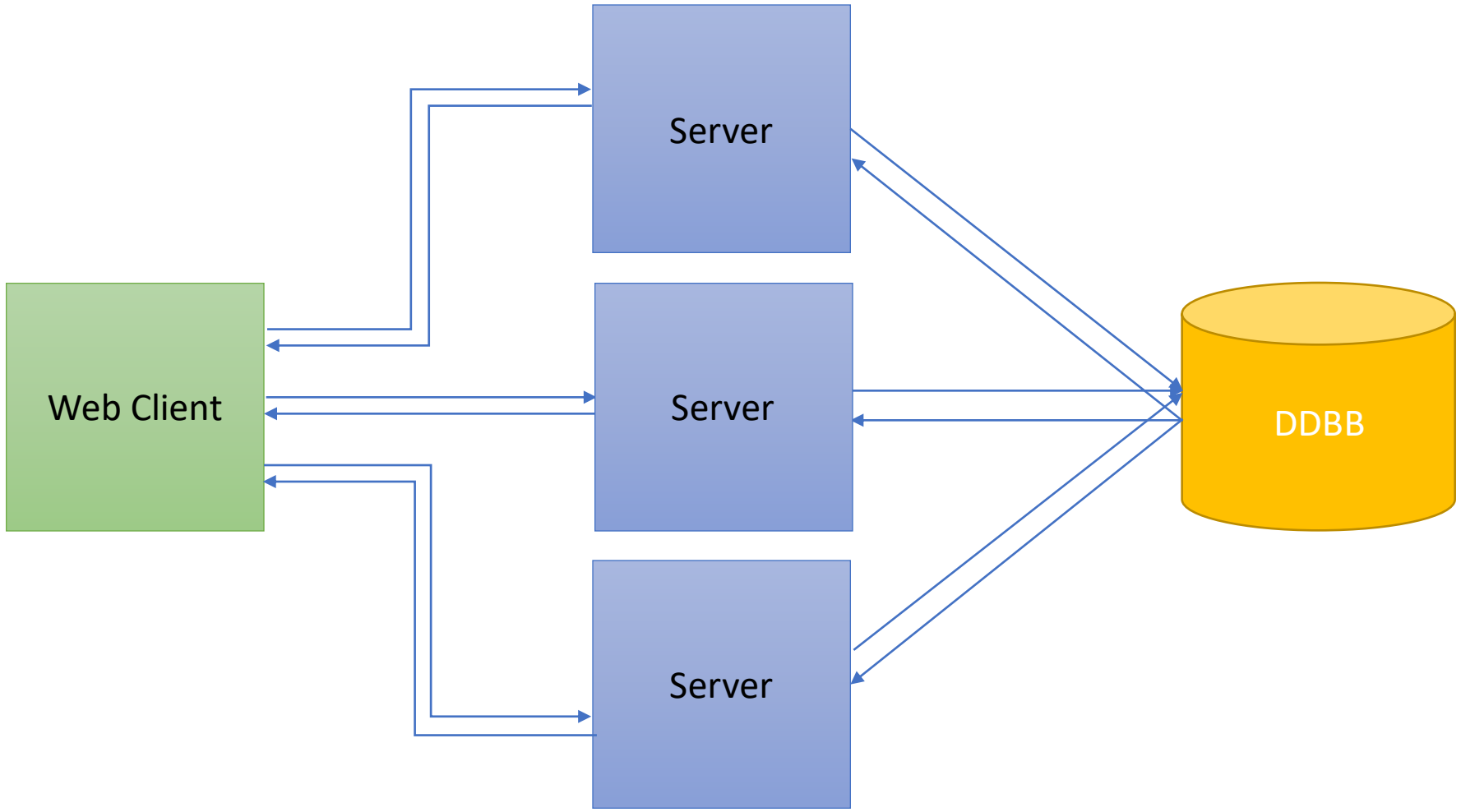
```
<html>
  <head>

  </head>
  <body>

      DATO_X

      <form method='METHOD'>
          <input name='campo1' value='DATO_1'>
          <input name='campo2' value='DATO_2'>
      </form>
      DATO_Y
  </body>
</html>
```

4. Verificación de la gestión de sesiones

Single Servers: SessionID (stateful)



Multiple Servers: JWT (stateless)



ascentic/

SSO Flow