**UNIVERSIDAD NACIONAL DE CATAMARCA**

**Facultad de Tecnología y Ciencias Aplicadas**

**TRABAJO DE LABORATORIO:**

**“Aplicación Web para la Inscripción en Cursos de Perfeccionamiento y emisión de Certificados”**

**CÁTEDRA:** PROGRAMACIÓN III

**ALUMNOS:** Gómez Marcos **MUN:** -01327

González, Celeste-01077

**AÑO:** 2019

**Enunciado:**

Desarrollar un prototipo de aplicación web con un mínimo de features (características) que permitan evaluar el prototipo desde el punto de vista del usuario final.

**Caso de Estudio:** “Aplicación Web para la Inscripción en Cursos de Perfeccionamiento y emisión de Certificados “

En la Facultad de Tecnología y Ciencias Aplicadas (FTyCA), se dictan distintos cursos de posgrado, perfeccionamiento, simposios, etc. Se requiere el desarrollo de una aplicación web que permita la inscripción de los interesados y la emisión luego del correspondiente certificado de la asistencia o aprobación del mismo.

Las funciones mínimas principales requeridas son:

✓ La aplicación debe contemplar diferentes perfiles de usuarios, perfil de usuario administrador con permisos totales y perfil de interesado que permita interactuar con las opciones de inscripción a los cursos.

✓ La aplicación deberá permitir al usuario interesado la inscripción en los distintos cursos o eventos, los datos a consignar deberán ser: Apellido-Nombre-DNI- email – Categoría (alumno, docente, público en general).

✓ La aplicación deberá permitir gestionar los datos del curso: nombre del curso, fecha desde, fecha hasta, cantidad de horas, lugar de realización, horarios, fecha certificado, fecha límite de inscripción, autoridades certificantes, firmas, costo del curso, expositores.

✓ La aplicación deberá tener en cuenta cupos máximos y mínimos de inscriptos al curso, realizar el control de los mismos, en caso de haber cubierto el cupo máximo, indicar ese suceso al interesado y permitirle la inscripción como postulante.

✓ La aplicación deberá permitir gestionar la emisión de un cupón de pago, una vez realizada la inscripción.

✓ La aplicación deberá permitir al usuario administrador gestionar la asistencia de los inscriptos al evento, los estados pueden ser (asistencia, aprobado, expositor).

✓ La aplicación deberá permitir gestionar la emisión de los certificados una vez concluido el curso.

✓ La aplicación deberá permitir el acceso a una página principal donde se muestren los próximos cursos a realizarse.

✓ La aplicación debe proveer diferentes estadísticas, en el momento que se le solicite, con el correspondiente reporte:

• listado de inscriptos por cursos.

• Listados de inscriptos que efectuaron el pago/inscriptos que falta realizar el pago.

• Cursos realizados en una fecha determinada (fecha inicio/fecha fin).

✓ Consideraciones a tener en cuenta: Un evento puede tener 1 o muchos expositores.

Un expositor puede también ser asistente al evento en otras charlas o cursos del mismo.

**Especificación de Requisitos de la Aplicación:**

**Requisitos Funcionales:**

1. El sistema deberá permitir el acceso a dos tipos de usuario: usuario Administrador y usuario Aspirante o Inscripto.
2. El sistema deberá permitir al usuario administrador, llevar un registro de los Cursos que se dicten en la F.Tec.y Cs.Aplicadas.
3. El sistema deberá permitir al usuario administrador, llevar un registro de los Expositores correspondientes a cada curso.
4. El sitema deberá permitir al usuario administrador, llevar un registro de las Autoridades correspondientes a cada curso.
5. El sistema deberá permitir al usuario administrador, gestionar estos registros.
6. El sistema deberá permitir al usuario administrador asociar a cada curso uno o más Expositor.
7. El sistema deberá permitir al usuario administrador, asociar a cada curso una o más Autoridades Certificantes.
8. El sistema deberá permitir al usuario administrador, asociar un Expositor y/o Autoridad certificante al momento de cargar un nuevo Curso.
9. El sistema deberá permitir al usuario administrador, quitar un curso a un Expositor o Autoridad Certificante si se lo desea.
10. El sistema deberá permitir al usuario administrador, la consulta de datos de los cursos cargados.
11. El sistema deberá permitir al usuario administrador, la consulta de datos de los Expositores cargados.
12. El sistema deberá permitir al usuario administrador, la consulta de datos de las Autoridades Certificantes cargadas.
13. El sistema deberá mostrar los cursos próximos en el home del mismo.
14. El sistema deberá permitir controlar el cupo máximo de inscriptos a un curso.
15. El sistema deberá permitir llevar un registro de los Inscriptos a un curso.
16. El sistema deberá permitir gestionar estos datos.
17. El sistema deberá permitir el registro de usuarios aspirantes.
18. El sistema deberá mostrar a los usuarios aspirantes, información de los cursos.
19. El sistema deberá permitir a los usuarios aspirantes, inscribirse a varios cursos.
20. El sistema deberá permitir a los usuarios aspirantes, cancelar la incripción a un curso.
21. El sistema deberá indicar al usuario aspirantes, la condición de inscripción al curso: Postulante o Inscripto.
22. El sistema deberá emitir un Cupón de Pago al momento de realizar la inscripción.
23. El sistema deberá generar un pdf con el correspondiente cupón de pago.
24. El sistema deberá permitir al administrador llevar un control de pagos de los inscriptos a un curso.
25. El sistema deberá permitir al usuario administrador la gestión de Cupón de Pagos.
26. El sistema deberá permitir al usuario administrador la gestión de Certificados.
27. El sistema deberá permitir al usuario administrador generar tipos de Certificados: Aprobado, Asistencia o Expositor según corresponda.
28. El sistema deberá permitir al usuario inscripto consultar sus certificados.
29. El sistema deberá permitir al usuario inscripto consultar lsus cursos inscriptos.
30. El sistema deberá permitir al usuario administrador solicitar estadisticas.
31. El sistema deberá permitir al usuario administrador solicitar estadisticas de inscriptos que no realizaron un pago.
32. El sistema deberá permitir al usuario administrador solicitar estadisticas de inscriptos por curso.
33. El sistema deberá permitir al usuario administrador solicitar estadisticas de cursos por fechas.

**Requisitos No Funcionales:**

1. El sistema debe ser desarrollado utilizando el Framework full Stack Grails.
2. El sistema debe poder adaptarse a cualquier dispositivo mediante una Aplicación Web con Diseño Responsivo.
3. El sistema debe brindar las medidas de Seguridad correspondientes teniendo en cuenta los diez riesgos críticos definidos por OWASP.
4. El sistema debe brindar una API Rest que permita integrar este con futuros desarrollos.
5. El sistema deberá incorporar las validaciones correspondientes a la hora de procesar los datos ingresados por los usuarios.

**Técnicas para brindar seguridad a una Aplicación Web aplicadas al Trabajo de laboratorio:**

1. **.Inyecciones SQL:**

Las fallas de inyección, ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.

Con Grails todo el acceso estándar a la base de datos a través de objetos de dominio [GORM](http://docs.grails.org/latest/guide/GORM.html) se escapa automáticamente a SQL para evitar ataques de inyección SQL.

Por ejemplo: se utilizan parámetros con nombre para pasar el valor de estos en lugar de la llamada análoga usando un GString.

**def** **vulnerable**() { **def** books = Book.find("from Book as b where b.title ='${params.title}'")}

def safe() {

def books = Book.find("from Book as b where b.title = ?",

[params.title])

}

**2.Prevención de secuencias de comandos de sitios cruzados (XSS)**

Los ataques Cross Site Scripting (XSS) son un vector de ataque común para aplicaciones web. Por lo general, implican enviar código HTML o Javascript en una forma tal que cuando se muestra ese código, haciendo que por ejemplo pueda [acceder a las cookies de sesión de otros usuarios.](https://blog.codinghorror.com/protecting-your-cookies-httponly/)

Por defecto, Grails lo hace de forma segura y escapa a todo el contenido en ${}expresiones en GSP. Todas las etiquetas GSP estándar también son seguras por defecto, escapando a cualquier valor de atributo relevante. Aunque esto no garantiza que una aplicación sea invulnerable a un ataque al estilo XSS. Es fácil cambiar a un valor predeterminado inseguro, lo que aumenta el riesgo de que se introduzca una vulnerabilidad.

**3. Autenticación**

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son

implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y

contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la

identidad de otros usuarios (temporal o permanentemente).

Para esto se implementa un mecanismo de autenticación simple usando [interceptores](http://docs.grails.org/latest/guide/theWebLayer.html#interceptors) . Esto es suficiente para casos de uso simples. .Los interceptores le permiten aplicar la autenticación en todos los controladores o en un espacio URI.

También se incorpora en esta aplicación el el control de tiempo de vida de sesiones, ya que no se encuentran configurados correctamente. Se desactiva la sesión al dejar de interactuar un determinado intervalo de tiempo.

Otra solución o prevención a estos ataques, aplicados en la aplicación desarrollada es la encriptación de clave.