Pontificia Universidad Católica de Chile

Escuela de Ingeniería
Departamento de Ciencia de la computación
IIC2513 – Tecnologías y aplicaciones web
I – 2016
Profesor John Owen

ENTREGA 4

PROYECTO SEMESTRAL 1-2016

El proyecto de este semestre consistirá en un catálogo de productos online, de 2 familias de productos y promociones.

El proyecto se desarrollará en 5 entregas parciales más la entrega final:

~~E3. Viernes 8 de abril – Maquetas en HTML + CSS~~

E4. Viernes 29 de abril – Autenticación y manejo de usuarios

E5. Viernes 13 de mayo – Catálogos y administrador

E6. Viernes 27 de mayo – Mejoras varias y compra

E7. Viernes 10 de junio – APIs REST

EF. Viernes 24 de junio – Mejoras varias y detalles

REPOSITORIO Y ENTREGAS

Esta entrega se realizará en los grupos registrados en la entrega 3, al igual que el resto del proyecto semetral. El grupo no podrá cambiar durante el transcurso del proyecto.

ENTREGA: REPOSITORIO Y SERVIDOR

A partir de esta entrega 4, inclusive, cada grupo deberá contar con un repositorio **privado** en bitbucket (bitbucket.org) – de preferencia un repositorio Git. Cada integrante del grupo debe tener al menos acceso de escritura en el repositorio (aunque se recomienda acceso de administrador para cada uno); además, ***debe darse acceso de lectura a cada uno de los tres ayudantes y al profesor del curso***.

Las entregas serán evaluadas de acuerdo a ***la copia presente en el repositorio del grupo al momento de la entrega***.

Además, también desde esta entrega, cada grupo deberá tener su aplicación ***funcionando en un servidor como Heroku*** o equivalente.

Abandono de un grupo

En caso de que **un alumno no continúe con el proyecto**, será evaluado con la nota mínima en todas las entregas siguientes (incluyendo la entrega y presentación final, reprobando automáticamente el curso de acuerdo a las reglas publicadas en el programa).

Para **el integrante restante**, que deberá continuar sólo con el proyecto, se aplicarán reglas especiales en cada entrega (aunque probablemente esto no evitará que la carga individual sea mayor).

Estos casos excepcionales deben ser avisados a la brevedad al profesor.

Entrega 4

Usuarios

Esta entrega consistirá en la gestión de usuarios. Su aplicación debe considerar 2 tipos de usuarios:

- Usuario regular o cliente – es el usuario que puede comprar en su aplicación, ver comprar efectuadas, etc (independiente de que la aplicación podría permitir la compra de visitantes sin una cuenta de usuario).
- Usuario administrador – es el usuario que puede gestionar los catálogos, agregar / cambiar / quitar productos y promociones; agregar manualmente usuarios, cambiarlos o desactivarlos.

Con esto en mente, su aplicación debe contar un modelo de usuarios apropiado.

Acceso de administración

Además del modelo de usuarios, en esta entrega deberás implementar un acceso autenticado (login) para la administración del sistema, bajo la url "/admin", la que debe solicitar autenticarse y sólo debe permitir ingresar con una cuenta de administrador.

Una vez ingresado al sistema como administrador, todas las urls de administración deben comenzar con /admin, por ejemplo, /admin/listar_usuarios (preferir urls "estándares" y no este feo ejemplo)

Una vez autenticado un usuario administrador, este usuario debe poder:

- Ver el listado de usuarios.
- Crear un nuevo usuario.
- Ver los datos de un usuario.
- Editar los datos básicos de un usuario (a excepción de la contraseña).
- Cambiar la contraseña de un usuario (en una operación separada al editar).
- Bloquear (desactivar) una cuenta de usuario.
- Reactivar una cuenta de usuario.

Acceso "normal"

Por otra parte, bajo la url "normal", "/", aún la aplicación no tiene nada, pero considerar mientras tanto un "placeholder" del catálogo (algo como un "aquí va el catálogo").

En esta url, un usuario normal o un administrador debe poder ingresar (autenticarse, login). Una vez autenticado, el sistema debe mostrar que está autenticado y permitir:

- Ver sus datos de usuario (obviamente sólo los que un usuario "normal" tenga permitido ver).
- Cambiar su contraseña.
- Salir del sistema (logout).

Además, si el usuario es un administrador, debe tener un enlace para ir a la sección de administración.

Finalmente, antes de autenticarse, el sistema debe proveer una forma de que un usuario recupere el acceso a su cuenta ("no recuerdo mi clave"), por ejemplo, enviando por mail un enlace único que permita cambiar la contraseña o generar una nueva.

Restricciones

No pueden usar ninguna librería / gema, a excepción de las que vienen al crear una nueva aplicación Rails y las que necesiten para conectarse a la base de datos de su elección.

Plazo y forma de entrega

El plazo máximo de entrega es el viernes 29 de abril, a las 23:59 hrs. La forma de entrega consistirá en:

- Tener la aplicación corriendo, disponible para la corrección
- Un repositorio, según se explica anteriormente. Para la corrección se usará una copia del código tras el último commit anterior al plazo máximo de entrega.

En la página del curso se habilitará un cuestionario donde podrán informar la dirección de su repositorio privado. Recordar entregar los privilegios apropiados a todos los ayudantes y al profesor del curso.

Ayudantía de ayuda

El día viernes 29 de abril habrá una ayudantía para la resolución de dudas y apoyo de trabajo, en el módulo 5 (15:30 a 16:50) en la sala B16.

Evaluación

La evaluación de esta entrega responderá a la siguiente rúbrica:

Entrega 4

Ptje ítem	Ítem / aspecto	Excelente (5)	Bueno (4)	Deficiente (2)	No logrado (0)
5	Funcionalidades para administrador: administración de usuarios (lista de funcionalidades que puede hacer un admin)	Cumple con todo, con la separación solicitada (listar / crear / ver / editar / cambiar contraseña / bloquear / reactivar)	Cumple con todo, pero con otra separación (por ejemplo, sólo un editar para cambiar claves y datos de usuario)	No cumple con todas las funcionalidades, pero al menos con listar, crear, ver y editar usuarios.	No cumple con las funcionalidades, incluso falla en al menos 1 entre: listar, crear, ver o editar.
2	Funcionalidades para todos los usuarios: ver cuenta, cambiar contraseña	Hay una funcionalidad especial para cambiar mi contraseña y para ver mi cuenta (donde se muestra sólo datos que son del usuario y no del sistema como "usuario bloqueado" o fecha de creación / update). Funciona siempre con el usuario "logueado" (sin id de usuario en la URL)	Es posible ver datos del usuario y cambiar la contraseña del usuario actual.	Es posible ver datos del usuario o cambiar la contraseña del usuario actual.	Ninguna de las 2 funcionalidades implementadas.
2	Funcionalidades públicas: "olvidé mi clave"	Existe un mecanismo para recuperar el acceso a la cuenta a un usuario que ha olvidado su contraseña. Este mecanismo garantiza en alguna medida que sólo el legítimo dueño de la cuenta puede recuperar el acceso. Además, no impide el acceso al usuario si otra persona maliciosa inició el proceso.	Existe un mecanismo (…), y garantiza (…) al legítimo dueño. Sin embargo, una vez iniciado el proceso, debe completarse para que la cuenta pueda volver a usarse.	Existe un mecanismo para recuperar el acceso a la cuenta, pero este es deficiente, sin ninguna garantía que sólo el legítimo dueño puede recuperar el acceso.	No hay un mecanismo para recuperar el acceso a la cuenta que funcione. (Es decir, o no hay, o este no funciona).
3	Autenticación del sistema y sesión	Hay un sistema de autenticación de usuarios (login). Una vez autenticado, un usuario puede "salir" del sistema (logout). Mientras el usuario no salga, permanecerá autenticado en cada página que visite.	Hay un sistema de autenticación que mantiene autenticado al usuario, aunque no hay una forma de salir.	Hay un sistema de autenticación, pero el usuario no permanece autenticado.	No hay un sistema de autenticación.

Entrega 4

Ptje ítem	Ítem / aspecto	Excelente (5)	Bueno (4)	Deficiente (2)	No logrado (0)
3	Perfilamiento de las funcionalidades	Las funcionalidades de administrador están restringidas sólo a usuarios autenticados como administrador. Además, las funcionalidades para usuarios "normales" están restringidas a un usuario autenticado.	Bien la restricción para administración, pero falla para usuarios normales (o directamente no hay restricción para usuarios normales).	Hay problemas en la restricción a las funcionalidades para usuario administrador, pero existen algunos controles de acceso.	No hay restricciones de acceso a las funcionalidades de administrador que de alguna pudieran filtrar sólo a administradores.
2	Manejo de sesión	La sesión se maneja de manera segura, minimizando la información que se intercambia con el cliente cada vez. Esta información no es trivial de falsear por un tercero y es validada con datos que se almacenan en el servidor.	N/A	O bien se intercambia mucha información innecesaria con el cliente cada vez o bien esta información es fácil de falsear por terceros o esta información no es validada (sólo 1 falla).	Hay más de 2 de estas fallas o no se mantiene sesión.
4	Almacenamiento de contraseñas	No se almacenan las contraseñas, sino un valor representante que no permite obtener la contraseña desde éste (como un hash o equivalente). Además, se han utilizado mecanismos que impiden o dificultan descubrir las contraseñas para un atacante que logra obtener estos valores representantes.	No se almacenan las contraseñas, sino un valor representante com un hash. Los datos no se han preparado para protegerlos de un atacante que logra obtener estos valores.	N/A	Se almacenan las contraseñas o un valor representante identificatorio (por ejemplo, las contraseñas encriptadas)
2	Layout	Se ha implementado el layout de la entrega 3 con mejoras (visuales o de usabilidad)	Se ha implementado el layout de la entrega 3 (sin cambios significativos)	Se ha implementado un layout diferente a la entrega 3	No hay layout