UNIVERSIDAD DE GRANADA

Puja Por tu Resi

TFG

Estudiante: Antonio Jiménez Martínez
Tutor: Francisco Javier Melero Rus

Fecha: 27 junio 2017

puja por tu resi

Introducción

Gestor de residencias:

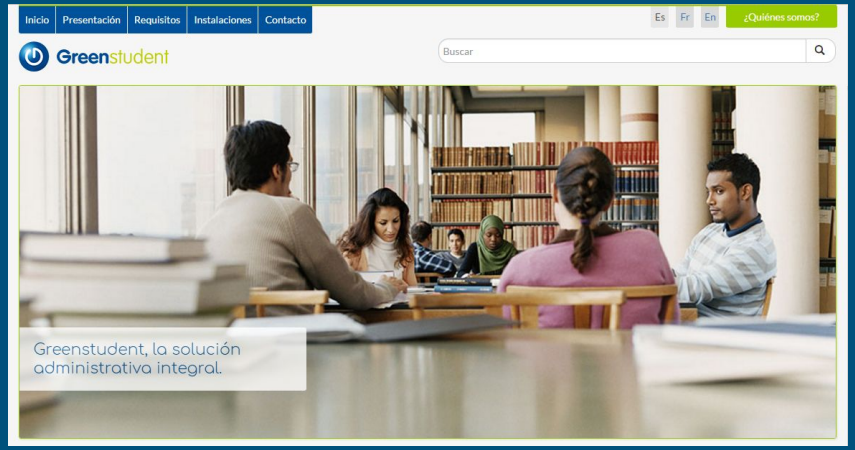
- Registrar el usuario
- Buscar habitaciones y residencias
- Pujar por una o varias habitaciones
- Asignación automática
- Firmar un contrato
- Mensajería interna
- Gestion incidencias
- Realización pago mensual

- Necesidad para el estudiante

Estado del arte

- Existe software para residencias de la tercera edad
- **GreenStudent**, software de escritorio (window), gestionar el área de la residencia.

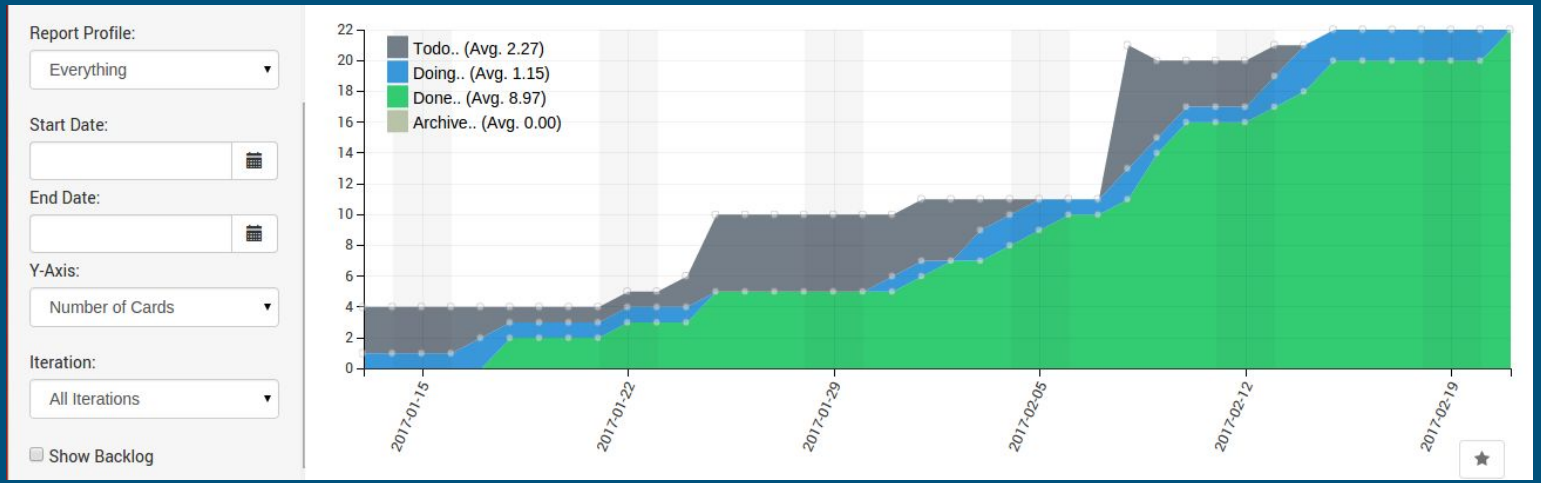
No existe ninguna aplicación web con para el usuario más importante, el estudiante.



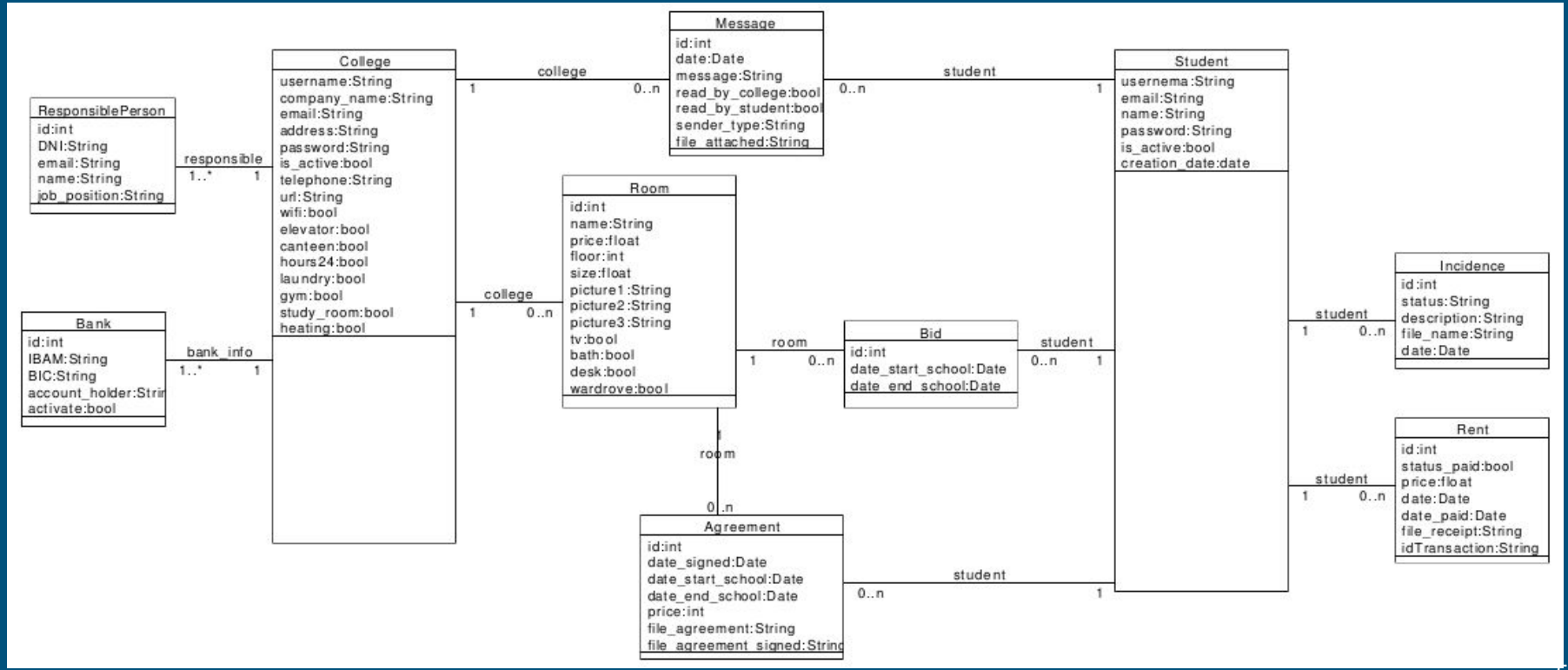
Metodología SCRUM

Etapa inicial de definición de la aplicación

4 iteraciones, cada Sprint: diseño, implementación, testeo y documentación



Diseño - Análisis diagrama de clases

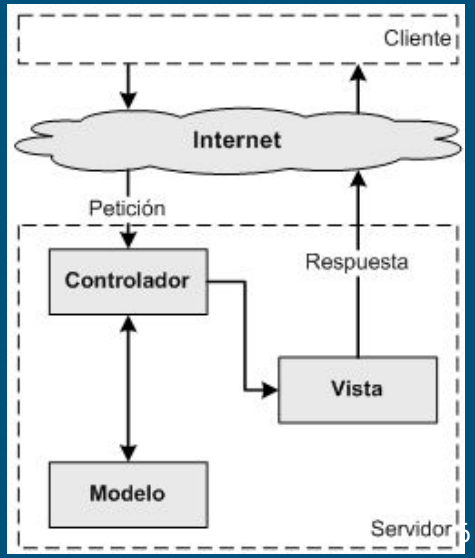


Tecnologia Utilizada - Back end

Symfony

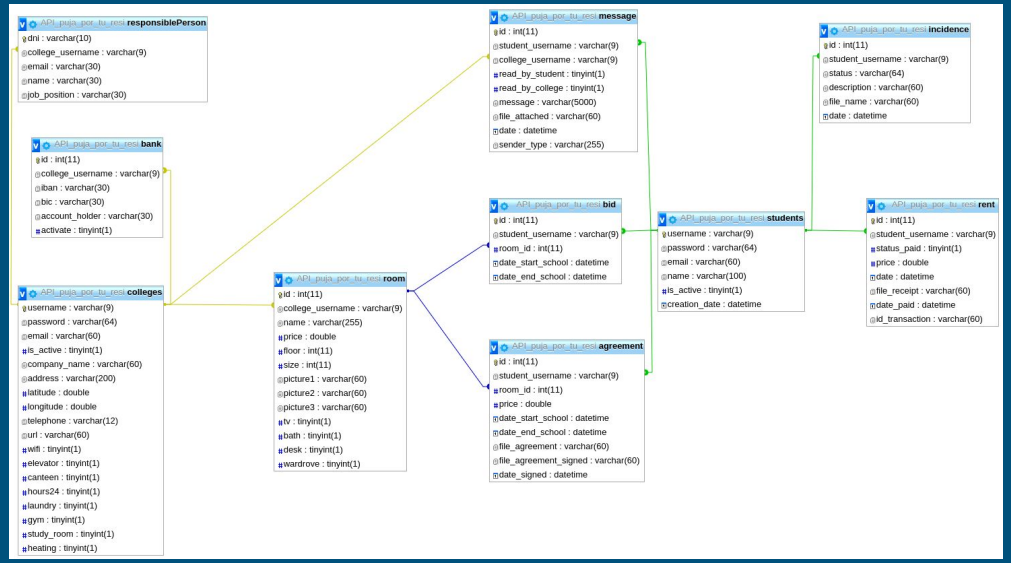
- Creación de la API, patrón MVC

POST	/Room/create/	This method create a room for a College. Can be called by user (College).
GET	/Room/download/{filename}	Download pictures rooms. Can be called by user (College/STUDENT/ADMIN).
GET	/Room/get/{id}	Get room of the id of a user (College). Can be called by user (College).
GET	/Room/getAll/	Get list of rooms of a College. Can be called by user (College).
GET	/Room/getAllCompanyName/	Get the companyName of all the colleges. This function can be called by User (College/Student/ADMIN).
GET	/Room/getSearch/	Get all the colleges with the data of college and all the OFFERED room. The college and the room should pass the restrictions: price, equipment, specific_college. This function can be called by User (College/Student/ADMIN)
GET	/Room/getSearchAll/	Get all the colleges with the data of college and all the OFFERED room. This function can be called by User (College/Student/ADMIN).
POST	/Room/remove/{id}	Remove room of the id of a user (College). Can be called by user (College).
GET	/Security/checkSesion/	This method verify if a user (which role) is connected in the system. Can be called by user (College/Student).
POST	/Signin/college/	This method sign up a user (College) in the system. It is not necessary to be authenticate.
POST	/Signin/student/	This method sign up a user (Student) in the system. It is not necessary to be authenticate.
GET | POST	/login	This method allow to a user to login the systme. Can be called by user (College/Student).
GET | POST	/remmemberPassword	This method allow to a user to remmeber the password the systme. Can be called by user (College/Student).



Tecnologia Utilizada - Back end

- Gestión de la base de datos.



Tecnologia Utilizada - Back end

- Automatización


```
#login (call twice to login with the cookies)
response = s.post("http://localhost:8000/login",  data = form_data, headers = headers,cookies = n_cookies)
response = s.get("http://localhost:8000/login",  headers = headers,cookies = s.cookies)

#API request /Agreement/assignedRooms/
print("assigne room\n")
response = s.post( "http://localhost:8000/Agreement/assignedRooms/", headers = headers,cookies = s.cookies)
print(response.text)
print("\n")
```

Tecnologia Utilizada - Front end

```javascript
/**
 * Display the location of the latitude and logitude on map
 * @param {id} id of the div
 * @param {latitude} latitude of the position
 * @param {longitude} longitude of the position
 */
function init_map(id, latitude, longitude) {
    //get latitude,longitude from the college
    var uluru = {
        lat: latitude,
        lng: longitude
    };
    var map = new google.maps.Map(
        document.getElementById(id), {
            zoom: 13,
            center: uluru
        }
    );
    var marker = new google.maps.Marker({
        position: uluru,
        map: map
    });
}
```

```javascript
var xmlHttp = new XMLHttpRequest();
var url = window.location.protocol + "//" + window.location.host + port + "/ProfileCollege/get/";
xmlHttp.open("GET", url, true);
xmlHttp.withCredentials = true;
xmlHttp.send();
xmlHttp.onreadystatechange = function() {
    if (xmlHttp.readyState == 4 && xmlHttp.status == 200) {
        var output = JSON.parse(xmlHttp.responseText);
        console.log(output)
        if (output.success) {
            display_specific_college("college_profile_", output.data);
            display_username("tab_profile_college_username", output.data.username);
        } else {
            showErrorMessagesPage("showdata", output.message, output.success);
        }
    }
}
```

- Gestión historial
- Validar datos entrada
- Hacer web dínamica
- Comunicarse con el servidor (AJAX)
- API de Google maps

Tecnologia Utilizada - Front end

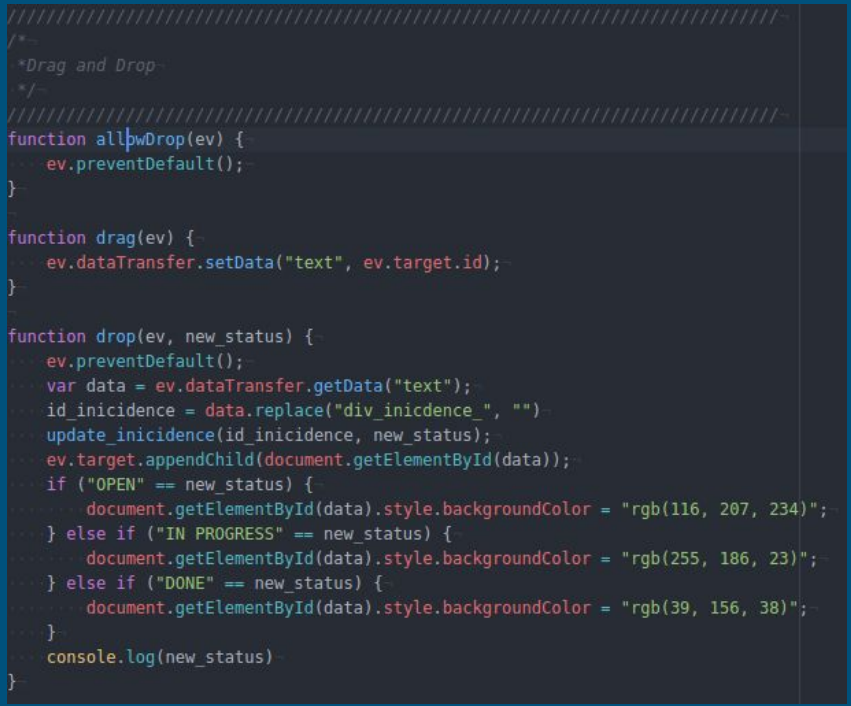
- Seleccionar varios elementos en una lista
- Cabecera de la tabla siempre visible
- Barra rango de precios

```
/**
 * keep in the top the thead of the table
 * @param tab_table
 */
function floatThead_table(tab_table) {
    var $table = $('#' + tab_table + ' table');
    $table.floatThead({
        scrollContainer: function($table) {
            return $table.closest('.wrapper');
        }
    });
}
```

```
/**
 * Display the range of price
 */
function display_range_price(id) {
    $("#" + id).slider({
        range: true,
        min: 0,
        max: 2000,
        values: [75, 1500],
        slide: function(event, ui) {
            $("#amount").val(ui.values[0] + "€ -" + ui.values[1] + " €");
        }
    });
    $("#amount").val(get_min_range_prince(id) + " € - " + get_max_range_prince(id) + " € ");
}
```

Tecnologia Utilizada - Front end

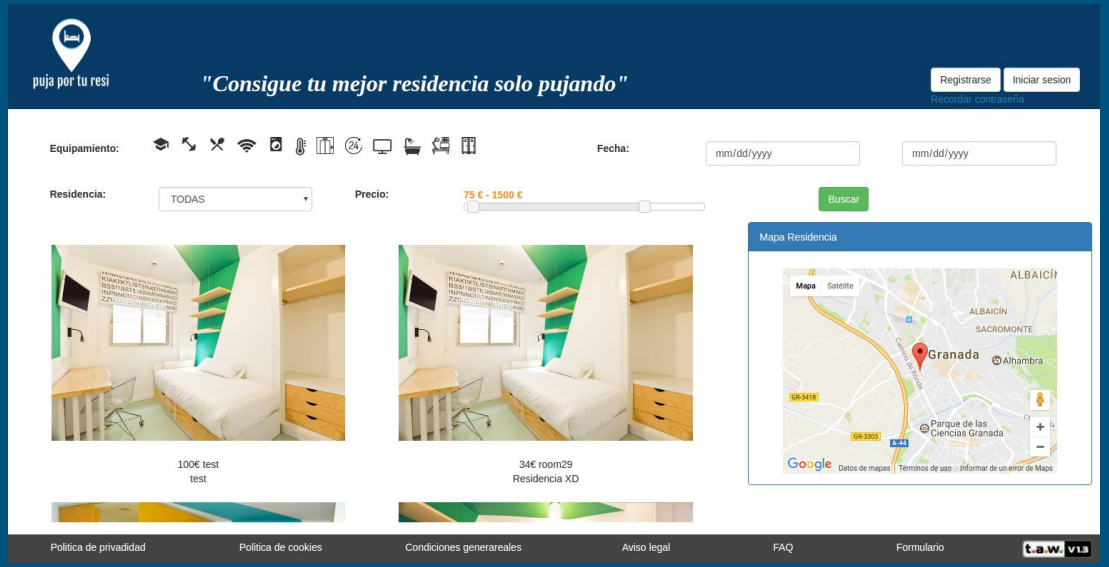
- Elementos especificos
  - Nav
  - Header
  - Footer
  - section.
- Drag and Drop
- Iconos

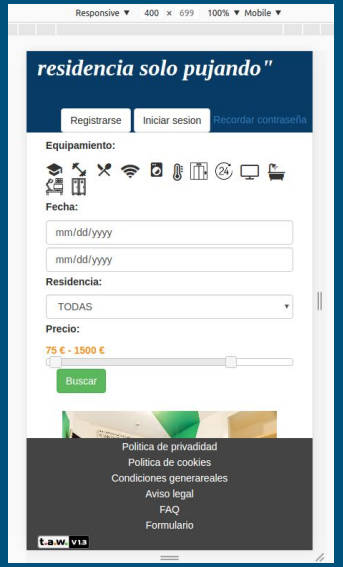


```
////////////////////////////////////////////////////////////////////////////////
/*
 *Drag and Drop
 */
////////////////////////////////////////////////////////////////////////////////
function allowDrop(ev) {
    ev.preventDefault();
}

function drag(ev) {
    ev.dataTransfer.setData("text", ev.target.id);
}

function drop(ev, new_status) {
    ev.preventDefault();
    var data = ev.dataTransfer.getData("text");
    id_inicidence = data.replace("div_inicdence_", "")
    update_inicidence(id_inicidence, new_status);
    ev.target.appendChild(document.getElementById(data));
    if ("OPEN" == new_status) {
        document.getElementById(data).style.backgroundColor = "rgb(116, 207, 234)";
    } else if ("IN PROGRESS" == new_status) {
        document.getElementById(data).style.backgroundColor = "rgb(255, 186, 23)";
    } else if ("DONE" == new_status) {
        document.getElementById(data).style.backgroundColor = "rgb(39, 156, 38)";
    }
    console.log(new_status)
}
```

Tecnologia - Front end

- Dar estilo y apariencia. Bootstrap para diseño responsive





Seguridad

- **Brute Force**

Autenticación de usuarios ->encriptar la contraseña a través de Bcrypt

```
security:

    encoders:
        AppBundle\Entity\College:
            algorithm: bcrypt
        AppBundle\Entity\Student:
            algorithm: bcrypt
```

- **Command execution/injection**

Ejecución de un comando maligno -> validar y no ejecutar valores de entrada

```
class Validate
{

    /**
     * Validate URL.
     *
     * @param validator_module  $validator
     * @param string $url    url
     *
     * @return bool
     */
    public function validateURL($validator,$url)
    {


    /**
     * Validate IBAN
     *
     * @param validator_module  $validator
     * @param string $IBAN    IBAN
     *
     * @return bool
     */
    public function validateIBAN($validator,$IBAN)
    {
```

Seguridad

- **Cross-site request forgery (CSRF)**

Ejecución acción con altos privilegios -> métodos necesita roles y autentificación

```
access_control:
- { path: ^/api/doc, roles: IS_AUTHENTICATED_ANONYMOUSLY }
- { path: ^/Signin/, roles: IS_AUTHENTICATED_ANONYMOUSLY }
- { path: ^/remmemberPassword, roles: IS_AUTHENTICATED_ANONYMOUSLY }
- { path: ^/login, roles: IS_AUTHENTICATED_ANONYMOUSLY }
- { path: ^/lucky/, roles: IS_AUTHENTICATED_ANONYMOUSLY }
#AGREEMENT CONTROLLER
- { path: ^/Agreement/create/ , roles: ROLE_ADMIN }
- { path: ^/Agreement/remove/ , roles: ROLE_STUDENT }
- { path: ^/Agreement/accept/ , roles: ROLE_STUDENT }
- { path: ^/Agreement/assignedRooms/ , roles: ROLE_ADMIN }
- { path: ^/Agreement/download/ , roles: [ROLE_STUDENT, ROLE_COLLEGE, ROLE_ADMIN] }
- { path: ^/Agreement/getCurrentSigned/ , roles: ROLE_STUDENT }
- { path: ^/Agreement/getList/ , roles: ROLE_STUDENT }
- { path: ^/Agreement/roomVerifyUnsigned/ , roles: ROLE_COLLEGE }
- { path: ^/Agreement/removeUnsigned/ , roles: ROLE_ADMIN }
```

Seguridad

- **Upload file**

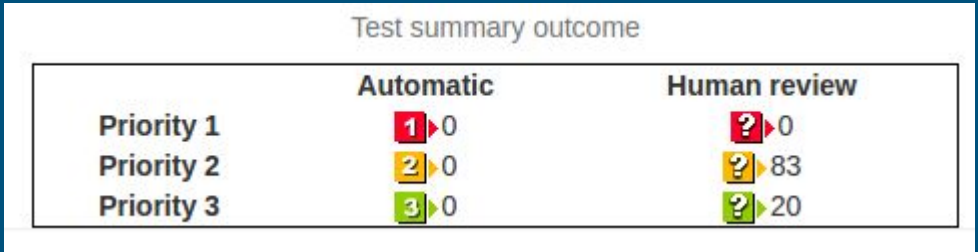
Subir archivo malicioso -> validar formato y tamaño, limitar subidas y un nombre único.

```
$file=$request->files->get('file_agreement_signed');
if (!$this->get('app.validate')->validatePDFFile($this->get('validator'),$file) and !$this->get('app.validate')->validateImageFile($this->get('validator'),$file)){
    return $this->returnjson(false,'Archivo no es valido (PFD- IMG).');
}
$filename=md5(uniqid()).'.'.$file->getClientOriginalExtension();
$file->move($this->container->getParameter('storageFiles'),$filename);
```

- **Cross-site scripting (XSS)**

Añadir script en los texto de entrada -> escapar los datos de entrada, no se ejecuten

Accesibilidad web



Test summary outcome

	Automatic	Human review
Priority 1	0	0
Priority 2	0	83
Priority 3	0	20

t.a.w. VÁLIDO V1.3

Una vez pasado los test automáticos y manuales de prioridad 1 con la herramienta **TAW**, conseguimos un nivel “A” de accesibilidad web.

Objetivo, la web sea accesible por más usuarios.

Testeo Software - **Test unitarios y funcionales**

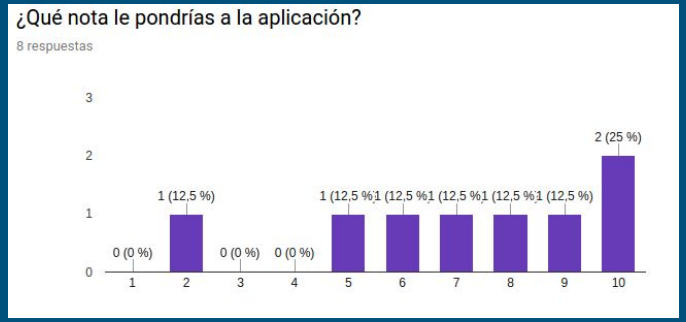
- Comprobar correcto funcionamiento código.
- Usamos PHPUnit (Symfony)
- **TDD**, los test lanzados cada vez que se añadía una funcionalidad.

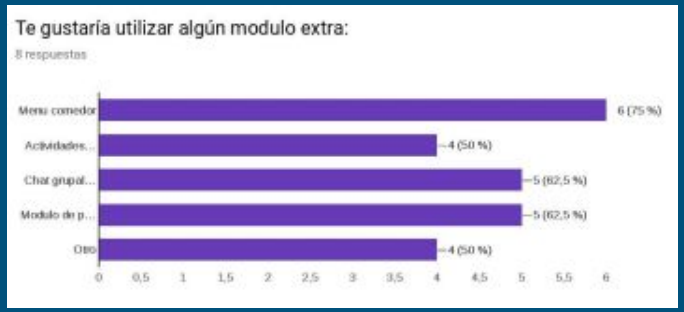
- Problemas:
  - Crear archivo temporales
  - Autenticar al usuario
- Sirven para encontrar bug.
- Son un control de calidad sobre:
  - Requisitos
  - Historias de usuario

```
jimenez@jimenez-PC:~/Escritorio/API_puja_por_tu_resi$ phpunit
PHPUnit 3.7.28 by Sebastian Bergmann.

Configuration read from /home/jimenez/Escritorio/API_puja_por_tu_resi/phpunit.xml.dist

..........

Time: 3.43 seconds, Memory: 33.50Mb

OK (11 tests, 22 assertions)
jimenez@jimenez-PC:~/Escritorio/API_puja_por_tu_resi$
```

Testeo Software - **Test de usabilidad**

- Los posible usuarios prueben y valoren la web.
- Acceder a una demo
- Rellenar un formulario
  - Han votado que le gustaría tener en la web, como módulo extra
  - Que es lo que mas y menos interesante.

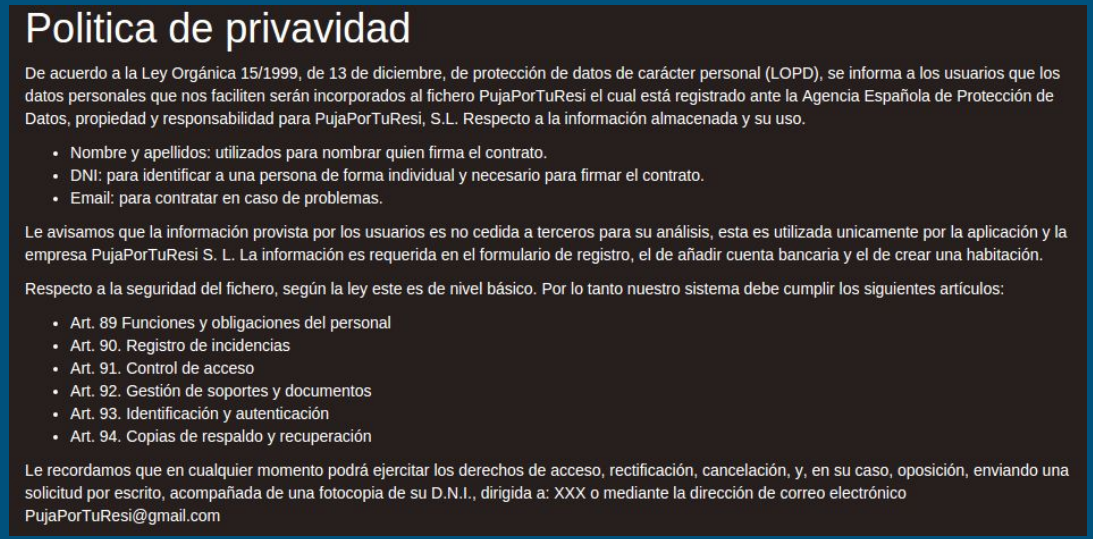




DEMO

Actividades Legales - Política privacidad

- Garantizar el honor y la intimidad personal (LOPD, Constitución Española).
- Agencia de proteccion de datos controla el cumplimento de la ley.
- Mostrar que datos se recogen, como son guardados y cual es su uso.



Politica de privavidad

De acuerdo a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), se informa a los usuarios que los datos personales que nos faciliten serán incorporados al fichero PujaPorTuResi el cual está registrado ante la Agencia Española de Protección de Datos, propiedad y responsabilidad para PujaPorTuResi, S.L. Respecto a la información almacenada y su uso.

- Nombre y apellidos: utilizados para nombrar quien firma el contrato.
- DNI: para identificar a una persona de forma individual y necesario para firmar el contrato.
- Email: para contratar en caso de problemas.

Le avisamos que la información provista por los usuarios es no cedida a terceros para su análisis, esta es utilizada unicamente por la aplicación y la empresa PujaPorTuResi S. L. La información es requerida en el formulario de registro, el de añadir cuenta bancaria y el de crear una habitación.

Respecto a la seguridad del fichero, según la ley este es de nivel básico. Por lo tanto nuestro sistema debe cumplir los siguientes artículos:

- Art. 89 Funciones y obligaciones del personal
- Art. 90. Registro de incidencias
- Art. 91. Control de acceso
- Art. 92. Gestión de soportes y documentos
- Art. 93. Identificación y autenticación
- Art. 94. Copias de respaldo y recuperación

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación, y, en su caso, oposición, enviando una solicitud por escrito, acompañada de una fotocopia de su D.N.I., dirigida a: XXX o mediante la dirección de correo electrónico PujaPorTuResi@gmail.com

Actividades Legales en la web

Política de cookies

Este es un fichero alojado en la memoria el cual puede ser utilizado por la web o por terceros.

Nuestra web está exenta a destacar, puesto que usa cookies de autenticación.

Aviso legal

Este recoge información sobre quién hay detrás, LSSI: Nombre y domicilio, Inscripción registro mercantil, etc.

Condiciones generales de contratación y uso

Explica las condiciones de contratación y uso de la web.

- Forma de pago y proceso de puja
- Idioma del contrato
- Obligaciones del vendedor y comprador
- Forma de confirmar la operación de compra

Trabajos Futuros

- Aplicación móvil para Android, IOS y Window
- Gestión de comedor
- Módulo de actividades extra
- Chat grupal entre todos los residentes
- Módulo de pago con Paypal
- Módulo de valoración
- Comercialización

Comercialización, Plan de negocio

- Ubicada en España, trabaja de forma remota
- Clientes directos: residencia y portales de anuncios
- Clientes indirectos: estudiantes
- Recursos: servidores, dominio web, ordenadores, recursos humanos
- Futuros competidores
- Canal de distribución: redes sociales y anuncios
- Misión: vender el producto a través de la satisfacción de los estudiantes
- Cuota mensual dependiente del número de habitaciones de la residencia

Licencia (GPLv3)- Github

GNU General Public License, version 3: el código puede ser utilizado por cualquiera y comercializado bajo la misma licencia (copyleft).

Github, utilizado para el control de versiones.

- Historial de código
- Poder acceder desde cualquier lugar

Asignaturas relacionadas

- *Fundamentos de programación y programación orientada a objetos y metodología de la programación*, estas son la base del proyecto software
- *Fundamentos de base de datos y estructura de datos,* diseño base de datos
- *Ingeniera, empresa y sociedad y Diseño y gestión de proyectos*.
- *Sistemas de información basados en web,* creación del cliente, API.
- *Desarrollo de software,* diseño del software.

Conclusión

- Enfrentarse a un proyecto gran escala
- La encuesta ha valorado la aplicación correctamente
- Continuaremos trabajando en el proyecto
- Aprender nuevas tecnologías
- El número de estudiante que va a la web para buscar alojamiento está creciendo en la actualidad

Muchas gracias

Preguntas