Informe técnico sobre análisis de código estático para el software Presupuestos de Aragón Versión 1.0

Perito:

Nombre: Juan Diego Gomez Gomez

Cédula: 1049656137

Email: juan.gomezg@usantoto.edu.co

Contenido del informe

1. Propósito de la evaluación

El propósito de la evaluación del software "Presupuesto de Aragón" se basa en detectar posibles errores de programación que produzcan fallos y vulnerabilidades en el sistema, de esta forma se podría mejorar la calidad de software en cuanto a seguridad, estéticas y estándares de calidad.

Además, es necesario hacer mediciones de calidad con algunas métricas como la densidad de comentarios, la complejidad cognitiva, la complejidad ciclomática, entre otros.

Otra parte de propósito es velar por plasmar toda la información que se obtenga de tal manera que se hagan las indicaciones y consejos necesarios para mejorar el software.

2. Producto a evaluar

Presupuesto de Aragón es un sitio dedicado a la visualización de los Presupuestos Generales de Aragón suficientemente intuitiva como para ser comprendida por personas sin experiencia previa en política presupuestaria, pero a la vez suficientemente detallada para permitir a aquellas personas interesadas y expertas en este asunto; de tal manera que profundice de una manera ágil y efectiva.

La versión 1.0 del software a evaluar posee 4 funcionalidades que:

- Visualización de gastos e ingresos presupuestados, de forma jerárquica y según las cuatro clasificaciones usadas en los presupuestos:
    - Funcional (para qué se gasta).
    - Económica (en qué se gasta, o cómo se ingresa).
    - Financiación (origen y tipo de los fondos)
    - Orgánica o Institucional (quién gasta/ingresa).
- Mostrar la información de los programas presupuestarios al máximo nivel de desglose existente, el nivel de partida.
- Mostrar la evolución de los presupuestos desde 2006.
- Permitir la búsqueda de texto libre en el conjunto de los presupuestos para encontrar cualquier dato de forma sencilla.

3. Especificación de la(s) herramientas usadas para medición

SonarQube:

Es un software o plataforma open source que facilita evaluar el código fuente y verificar los estándares que este debe tener por normativa. En este caso, Utiliza Sonar Scanner la cual posee las siguientes características:

- Detección de bugs.
- Detección de vulnerabilidades.
- Detección de código maloliente o "Code Smell".
- Detección de código duplicado.
- Recomendaciones de estándares de codificación.
- Mantenimiento al código.
- Medición de la complejidad ciclomática.
- Escrito en Java versión 8 y 11
- Permite analizar 27 lenguajes de programación(Java, Php, HTML, CSS , ...), cuenta con la documentación de reglas correspondiente para cada lenguaje.

4. Especificación de la Norma de calidad

La Norma **ISO 25000**, estipula una guía para el uso de estándares internacionales llamados "System and Software *Quality* Requirements and Evaluation" (SQuaRE). La norma establece criterios para los de requisitos de calidad de productos software, sus métricas y su evaluación, e incluye un modelo de calidad para unificar las definiciones de calidad de los clientes con los atributos en el proceso de desarrollo.

El uso que tiene la **ISO 25000** "Software Product Quality Requirements and Evaluation" (SQuaRE) y sus ramificaciones es organizar y unificar la especificación de requerimientos de calidad del software y evaluación de la calidad del software, soportada por el proceso de medición de calidad del software.

5. Requerimientos específicos de calidad funcionales y técnicos.

La empresa requiere que se evalué los siguientes requerimientos funcionales y técnicos específicos

Ítem	Requerimiento de calidad	Prioridad
1	Que el software pueda funcionar en sistemas operativos Android, MacOS, Windows XP, Windows 7 y Windows 10 (en 32 y 64 bits)	Alta
2	Que permita trabajar en forma rápida e intuitiva (cuente con ayudas visuales y auditivas interactivas en el software).	Alta
3	Que tenga soporte multi idiomas, especialmente inglés y español	Media
4	Que permita adecuar su estilo de visualización para adecuarse a personas con limitaciones visuales (Ley 1680 de 20 de noviembre de 2013)	Alta
5	Implementación de Ley 1581 del 2012 – Protección de datos (HABEAS DATA)	Baja
6	Permita generar reportes en EXCEL Y PDF.	Alta
7	Funcionalidad/módulo para reportar errores técnicos o funcionales desde el software.	Media
8	Permitir acceso a 100 usuarios simultáneos	Alta
9	Tolerancia a fallos (caída de red, apagones eléctricos frecuentes).	Media
10	Integración con office	Baja
11	Cumplimiento del 80% con el estándar OWASP, priorizando en las vulnerabilidades de robo de información, XSS, SQL injection y ransomware.	Alta
12	Capacidad de respaldo y recuperación de información desde el software.	Media
13	El software debe demandar mínimos recursos de hardware (cpu Intel celeron, 2 gigas de Ram)	Media

Cada uno de los ítems tendrán su descripción acontinuación:

1. Como el software ya se encuentra implementado en la web se pudo comprobar que este, funciona en cualquier plataforma sin ningún problema incluyendo los dispositivos móviles.

   Cumplimiento: 100%.

2. La plataforma cuenta con un diseño bastante sencillo en la parte gráfica y por otra parte siempre existe una explicación de como usar cada apartado de tal manera que se puede usar sin necesidad de tener conocimientos en política presupuestaria, Se recomienda hacer un tipo de tutorial para el manejo de algunas herramientas que su explicación es confusa.

   Cumplimiento: 91%.

3. El sitio no tiene un soporte multi-idioma, ya que está enfocado a usuarios o la población de Aragón, España pero de igual forma se recomienda crear un soporte en inglés ya que es uno de los idiomas universales debido a que esta solo posee soporte en español.

   Cumplimiento: 30%.

4. El sitio de estas ayudas visuales para personas con problemas de visión, solo posee una apartado donde proporciona una lupa para el texto o cambiar el tamaño de la fuente.

   Cumplimiento: 50%.

5. El sitio no posee ningún apartado donde se maneje información personal por lo cual este ítem tiene una prioridad muy bajo así que se recomendaría que si el sitio en un futuro piensa manejar un login tiene que tener en cuenta un mensaje o un formulario donde aclare que sus datos estarán seguros y implementar seguridad en el sitio.

Cumplimiento: 100%.

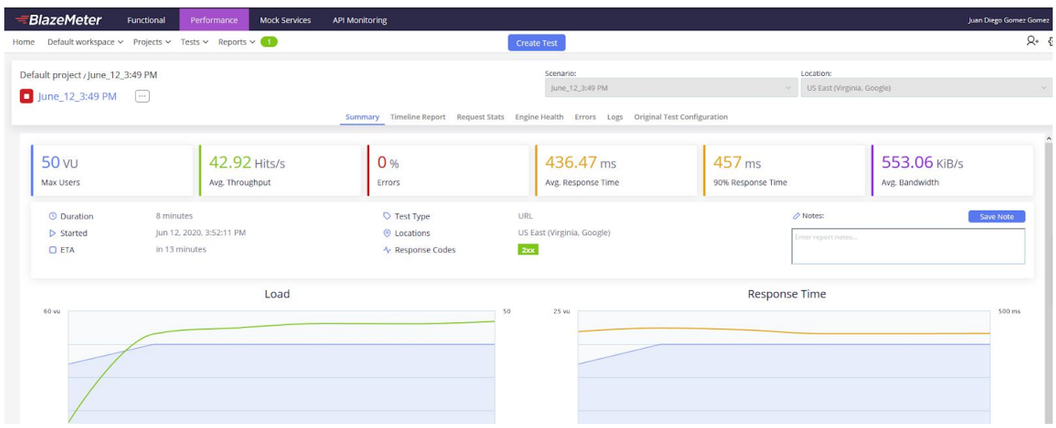
6. El sitio la mayoría de presupuestos por ingresos se puede exportar en formato PDF o CSV por lo cual esta muy completo en esta parte.

   Cumplimiento: 100%.

7. Cuando el usuario ingresa información errónea el sitio web tiene la capacidad de indicar cuáles son los errores. Además, se administra correctamente los errores comunes 404 (cuando no se encuentra una página o el enlace está defectuoso)y500 (cuando ocurre un problema del lado del servidor).En la parte administrativa no cuenta con funcionalidades o módulos para generar informes de errores técnicos, Se recomienda mejorar la notificación de errores debido a que sigue poco estético cuando manda algún tipo de error

   Cumplimiento: 80%.

8. Según con las prueba realizadas en BlazeMeter para revisar la sobrecarga de un sitio web vemos que sigue funcionando de una manera muy buena arrojando muy buen tiempo de respuesta, lamentablemente no pudimos hacer la prueba con más de 50 usuarios debido a que el Free Test solo podía sobrecargar el sitio con 50 usuarios.



   Cumplimiento: 100%.

9. El sitio web requiere una conexión a internet para funcionar, se adquirió el servicio de alojamiento en la nueve por lo cual estos se aseguran del funcionamiento continuo del servidor.

   Cumplimiento: 100%.

10. El sitio web tiene funcionalidades para integración con office mas especifico con Excel debido a que exporta presupuestos o información en ese formato.

    Cumplimiento: 100%.

11. El Sitio cuenta con protección de SQL injection y ataques comunes de robo de información, se recomienda tapar o parchar lo que son las rutas ya que estas pueden estar enviando información en estas.

    Cumplimiento: 50%.

12. El sitio web tiene buen respaldo de información ya que hacen de forma recursiva el extractos de presupuesto de la página principal del gobierno de Aragón.

    Cumplimiento: 100%.

6. Atributos de calidad.

Los atributos de calidad que se utilizaran para la evaluación del Software “Presupuesto de Aragón”, de acuerdo a lo especificado en el siguiente cuadrado:

Tabla 1 Atributos de calidad

ATRIBUTOS INTERNOS	Características del software que determinan su habilidad para satisfacer las necesidades propias e implícitas.
ATRIBUTOS EXTERNOS	Características del software que determinan su habilidad para satisfacer las necesidades explícitas e implícitas.
ATRIBUTOS EN USO	Características del software que determinan los requerimientos de los usuarios finales de manera que satisfagan sus necesidades.

6.1. Asignación de puntajes para atributos de calidad.

Los puntajes establecidos a los atributos de calidad seleccionados de acuerdo a las necesidades, se muestran en la siguiente tabla:

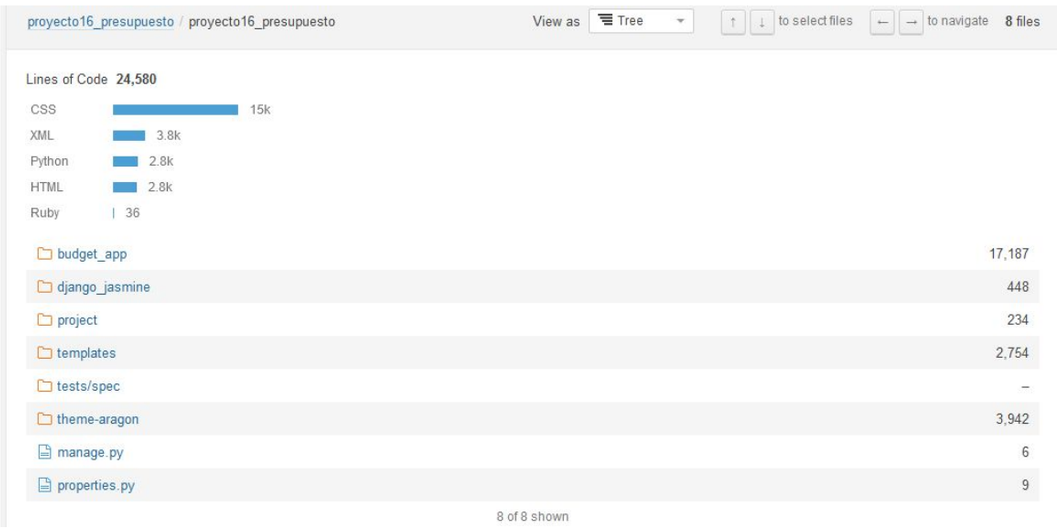
Tabla 2, Asignación de pesos sobre la medición de atributos.

Tipo de atributo	Puntaje
Atributos internos	65
Atributos externos	35
Total	**100**

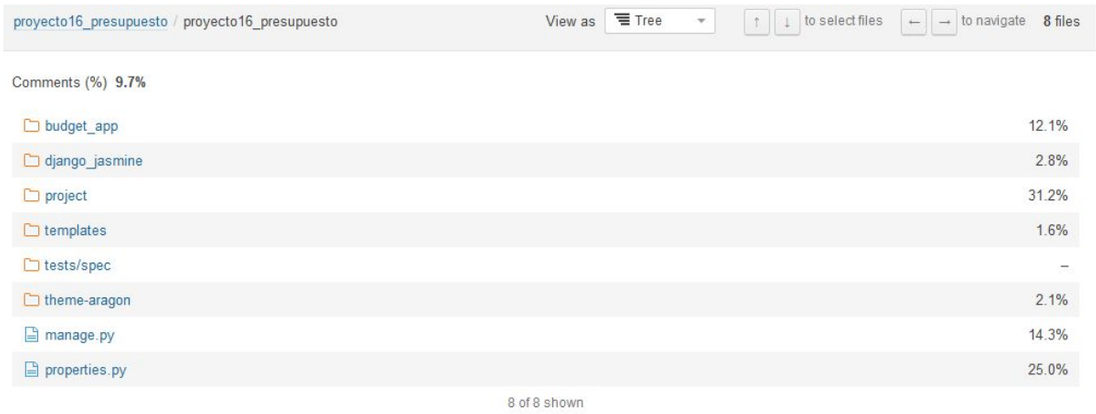
6.2. Atributos internos.

6.2.1. Tamaño de sistemas y código fuente (20%)

- Total de líneas de código: **24.580**



- Densidad de comentarios: 9.7%

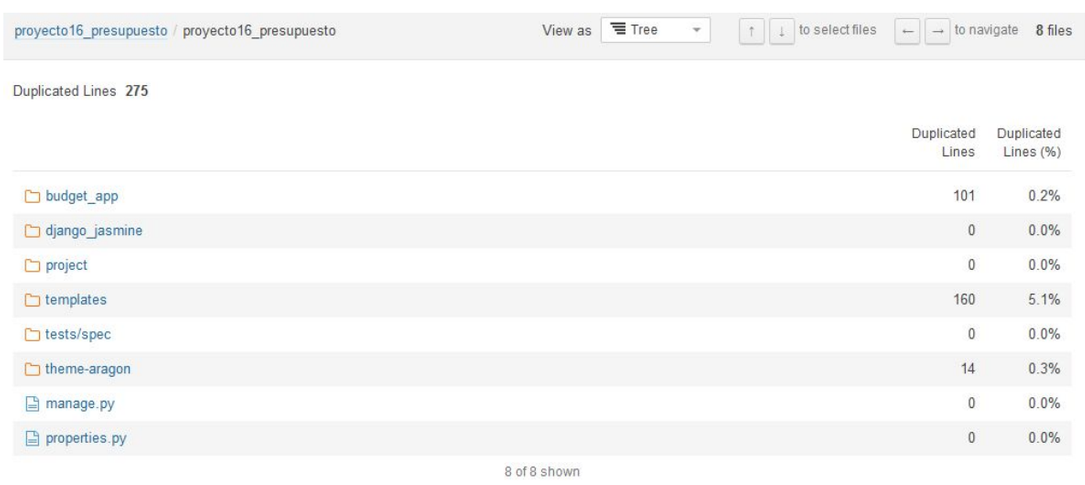

proyecto16_presupuesto / proyecto16_presupuesto View as Tree ↑ ↓ to select files ← → to navigate 8 files

Comments (%) **9.7%**

budget_app	12.1%
django_jasmine	2.8%
project	31.2%
templates	1.6%
tests/spec	–
theme-aragon	2.1%
manage.py	14.3%
properties.py	25.0%

8 of 8 shown

- Duplicidad de código: 270 líneas de código duplicado donde la mayoría proviene de los templates.

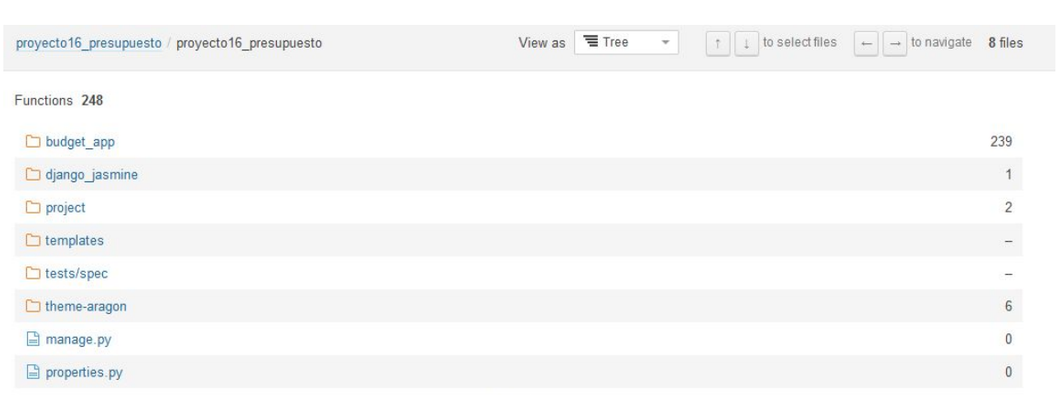

proyecto16_presupuesto / proyecto16_presupuesto View as Tree ↑ ↓ to select files ← → to navigate 8 files

Duplicated Lines **275**

	Duplicated Lines	Duplicated Lines (%)
budget_app	101	0.2%
django_jasmine	0	0.0%
project	0	0.0%
templates	160	5.1%
tests/spec	0	0.0%
theme-aragon	14	0.3%
manage.py	0	0.0%
properties.py	0	0.0%

8 of 8 shown

- Cantidad de funciones: 248 donde su gran mayoria provienen de Budget_app


proyecto16_presupuesto / proyecto16_presupuesto View as Tree ↑ ↓ to select files ← → to navigate 8 files

Functions **248**

budget_app	239
django_jasmine	1
project	2
templates	–
tests/spec	–
theme-aragon	6
manage.py	0
properties.py	0

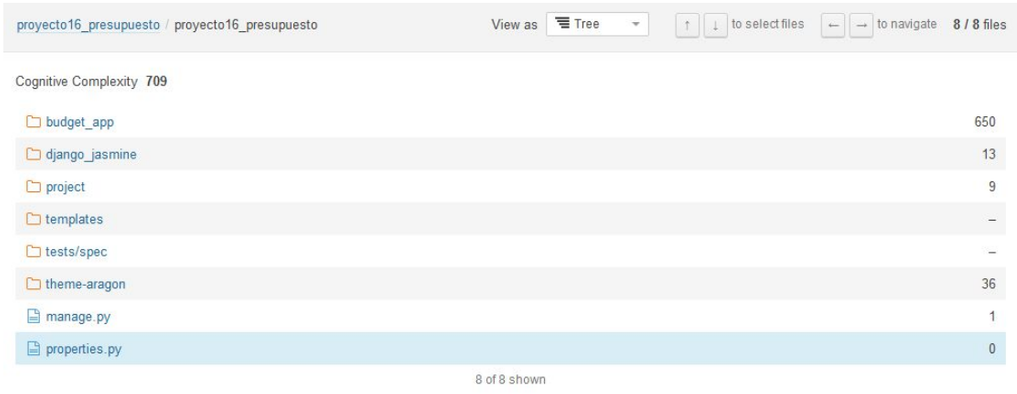
8 of 8 shown

Donde la gran mayoría de las funciones son para transformar los informes CSV.

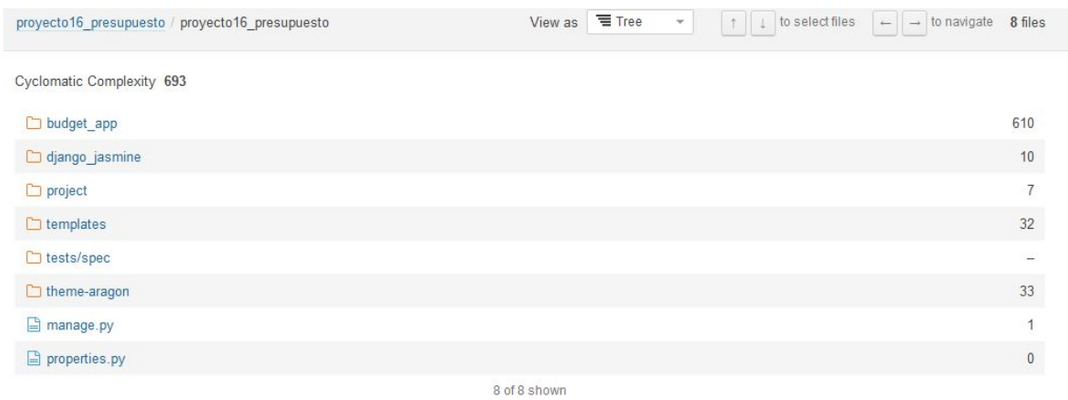
```
#
# ECONOMIC BREAKDOWN
#
def write_economic_breakdown(c, writer):
    writer.writerow(['#Año', 'Id Capítulo', 'Nombre Capítulo', 'Id Artículo', 'Nombre Artículo', 'Id Concepto', 'Nombre Conce
    for year in set(c['economic_breakdown'].years.values()):
        for chapter_id, chapter in c['economic_breakdown'].subtotals.iteritems():
            write_breakdown_item(writer, year, chapter, 'expense', [chapter_id, None, None], c['descriptions']['expense'])
            for article_id, article in chapter.subtotals.iteritems():
                write_breakdown_item(writer, year, article, 'expense', [chapter_id, article_id, None], c['descriptions']['exp
                for heading_id, heading in article.subtotals.iteritems():
                    write_breakdown_item(writer, year, heading, 'expense', [chapter_id, article_id, heading_id], c['descripti

def economic_policy_breakdown(request, id, format):
    return policies_show(request, id, '', _generator("%s.economica" % id, format, write_economic_breakdown))

def write_detailed_economic_breakdown(c, writer):
    writer.writerow(['#Año', 'Id Capítulo', 'Nombre Capítulo', 'Id Artículo', 'Nombre Artículo', 'Id Subconcepto', 'Nombre Su
    for year in set(c['economic_breakdown'].years.values()):
        for chapter_id, chapter in c['economic_breakdown'].subtotals.iteritems():
            write_breakdown_item(writer, year, chapter, 'expense', [chapter_id, None, None], c['descriptions']['expense'])
            for article_id, article in chapter.subtotals.iteritems():
                write_breakdown_item(writer, year, article, 'expense', [chapter_id, article_id, None], c['descriptions']['exp
                for heading_id, heading in article.subtotals.iteritems():
                    for subheading_id, subheading in heading.subtotals.iteritems():
                        write_breakdown_item(writer, year, subheading, 'expense', [chapter_id, article_id, subheading_id], c[

def economic_programme_breakdown(request, id, format):
    return programmes_show(request, id, '', _generator("%s.economica" % id, format, write_detailed_economic_breakdown))
```

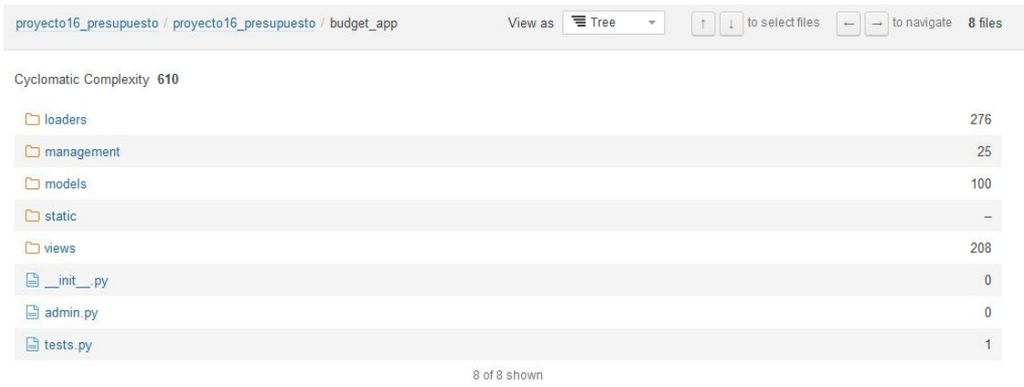
6.2.2. Complejidad del software(20%)

- Complejidad Cognitiva: Con un total de 709 y donde tenemos que la parte con mayor complejidad es donde están las vistas y la lógica de la calculadora de presupuesto que es **budget_app**.



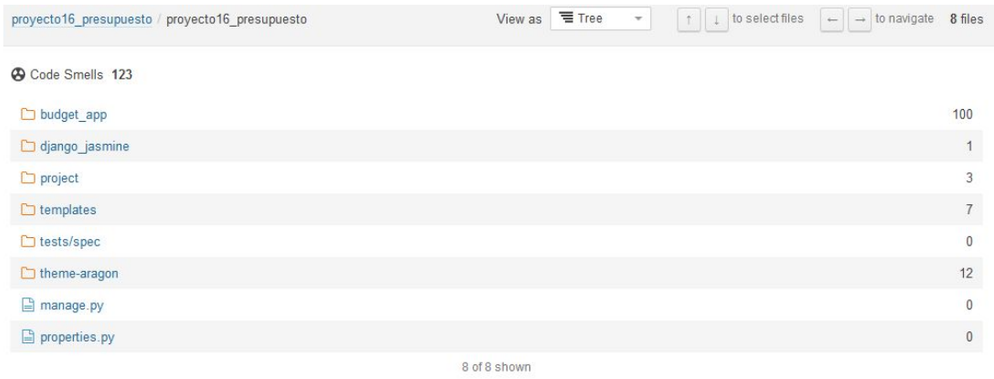
- Complejidad Ciclomática: Con un total de 693 y donde tenemos que la parte con mayor complejidad es donde están las vistas y la lógica de la calculadora de presupuesto que es **budget_app** donde se centra en este archivo "***aragon_bulk_budget_loader.py"***.



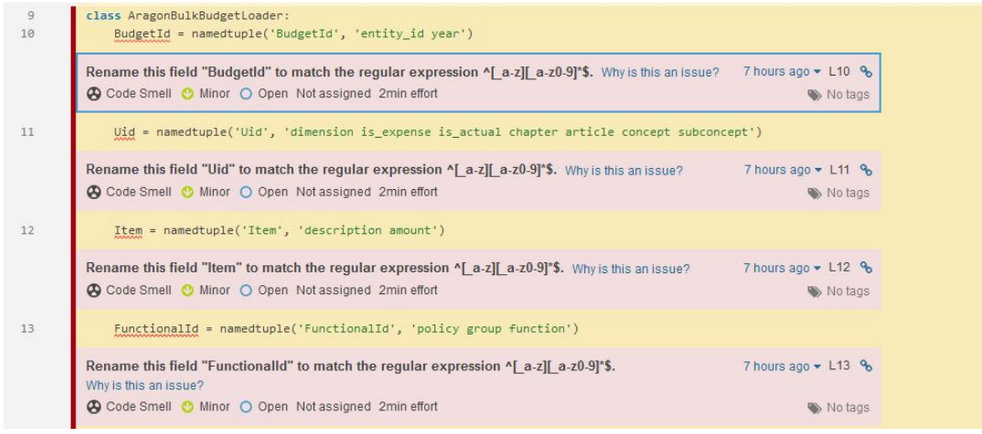


6.2.3. Deuda técnica (20%)

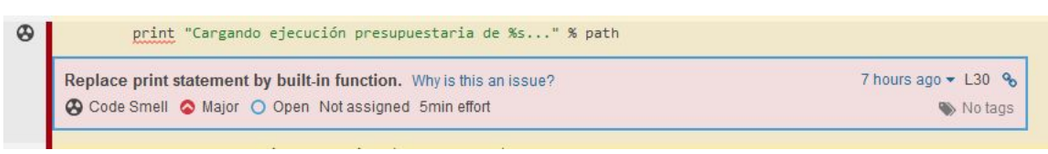
- Código malolientes tiene una cantidad de 123 en todo el proyecto donde se ve que el mayor problema viene de **budget_app**.



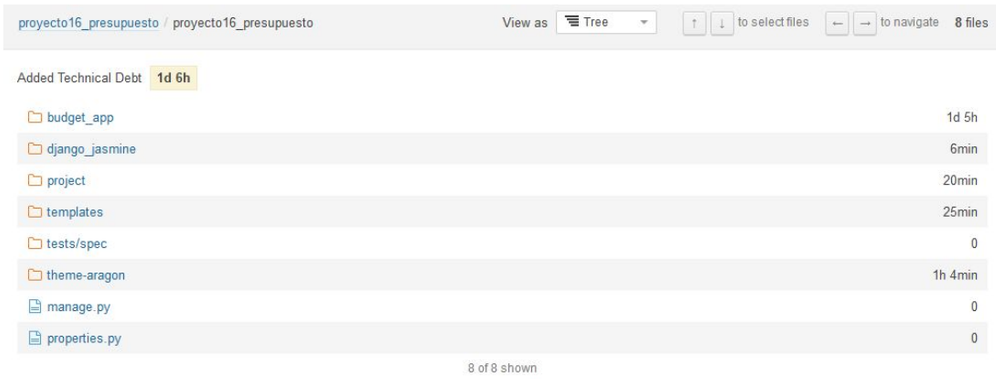
Donde la gran mayoría simplemente tienen problemas en estándares de nombres de variables, estos inconvenientes se solucionan manejando los nombres en lowercase.



Otro de los casos era cambiar los remplazar los ***print*** con una función.

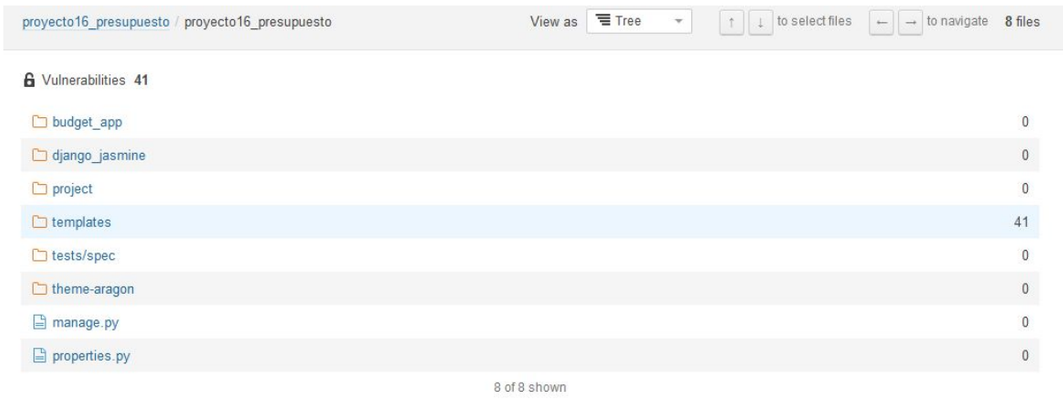


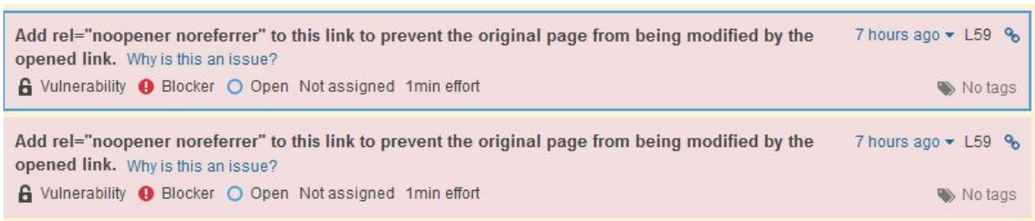
- Deuda: posee una deuda de 1 dia con 6 horas donde se centra nuevamente la gran mayoría de tiempo en el módulo **budget_app.**



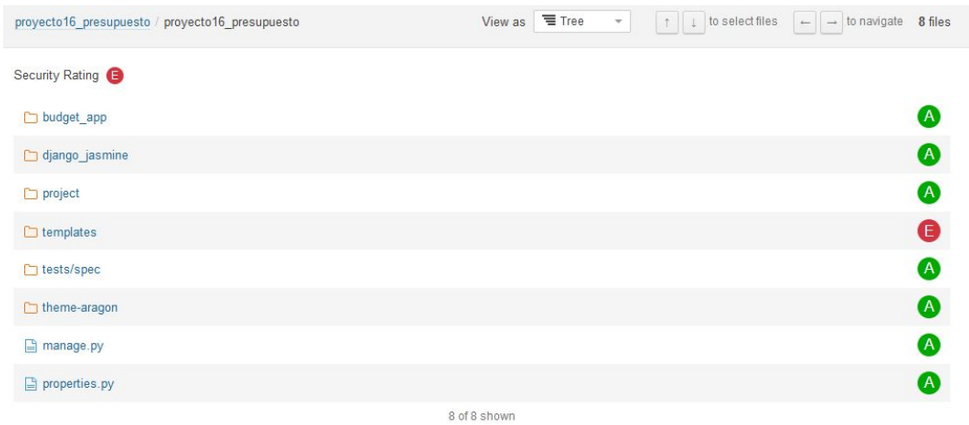
6.2.4. Seguridad(20%)

- Vulnerabilidades: se encontraron 21 vulnerabilidades donde todas hacen referencia a la falta del atributo rel="noopener noreferrer" en los enlaces para evitar pasar nuestra información personal a la nueva pestaña a la que nos dirigimos.

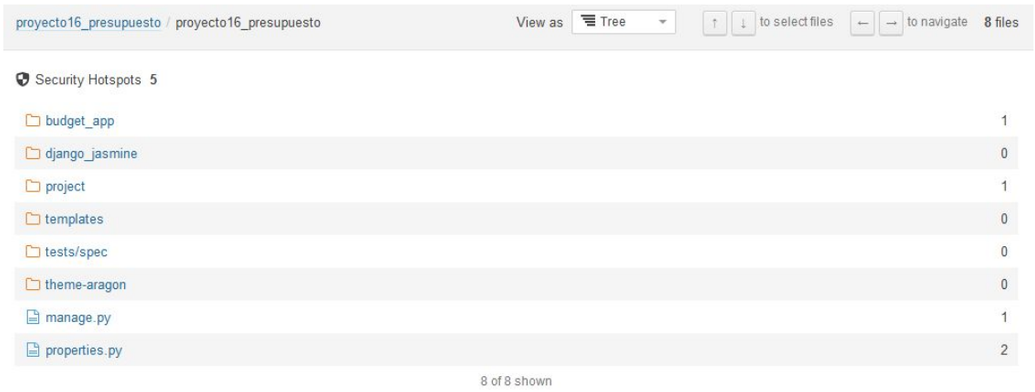




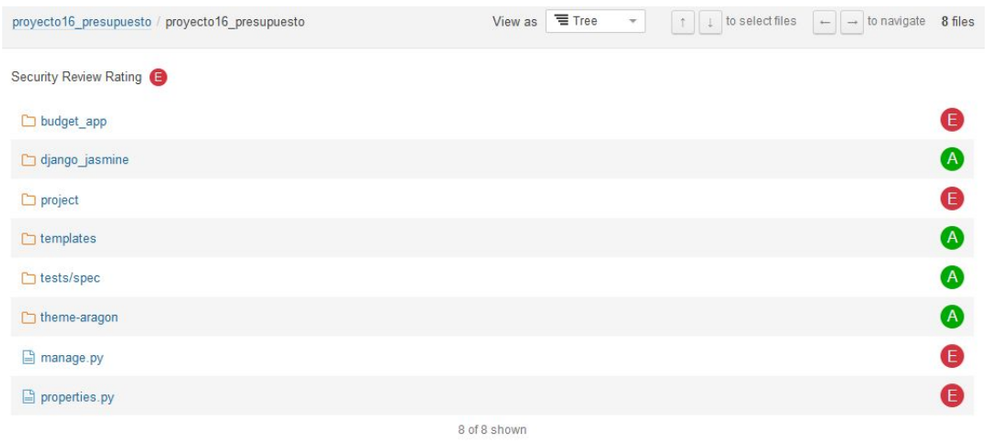
  - Clasificación: La clasificación de seguridad se encuentra en "***E"*** cuando hay al menos una vulnerabilidad.



- Puntos de acceso de la seguridad

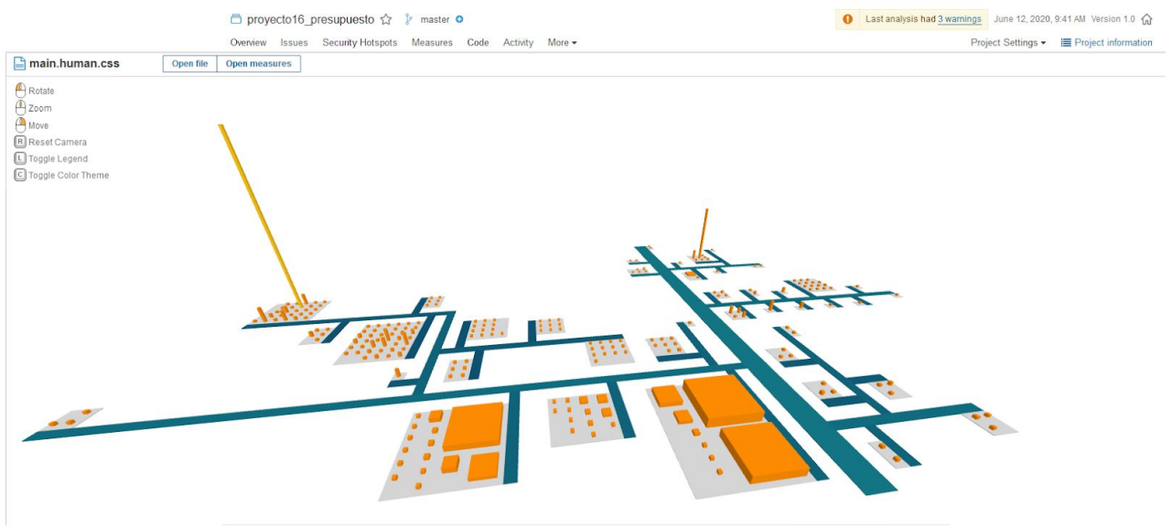


- Clasificación: La clasificación de seguridad se encuentra en "***E"*** cuando hay al menos una Security Hotspots.



6.2.5. 3d code metrics (20%)

En el siguiente gráfico se muestran algunas gráficas 3D del proyecto generadas en SonarQube usando el plugin SoftVi 3D y un breve análisis de estas, donde los edificios largos representa mucha complejidad ciclomática y muchas líneas de código, por otra parte los edificios gordos representa mucha complejidad ciclomática y pocas líneas de código.



6.3. Atributos Externos.

6.3.1. Usabilidad (20%)

En esta sección se demuestra la facilidad de usar este sitio web donde se evalúa los siguientes puntos:

- **La efectividad:** Cumple correctamente con las funciones que tiene. Los enlaces y botones son claros y están ubicado en partes visibles para llevar a la acción deseada.
  Usabilidad: 100%
- **La eficiencia:** La navegación del sitio web es entendible a simple vista. Tiene un diseño sencillo que permite la fácil interacción y navegabilidad.Los títulos de las secciones concuerdan con el contenido y maneja una ortografía adecuada.
  Usabilidad: 100%
- **La satisfacción**: Realmente el sitio es muy cómodo y yo personalmente creería que por la terminología que usa yo lo recomendaría luego de 5 horas investigando todo las herramientas que hay en el software.

  Usabilidad: 87%

  Promedio de usabilidad de 95.6%

6.3.2. Fiabilidad (30%)

El sitio web cuenta con mensajes adecuados cuando ocurre un error realizando una acción como actualizar una publicación, tiene las páginas de los errores HTTP 404, y 500.

Fiabilidad: 95%

6.3.3. Mantenibilidad (50%)

En cuanto mantenimiento del software tenemos que los lenguajes de programación tiene buena documentación y los lenguajes usados se pueden mantener por mucho tiempo ya que son lenguajes robustos, de tal manera, que no quedarán obsoletos con facilidad.

Mantenibilidad: 80%.

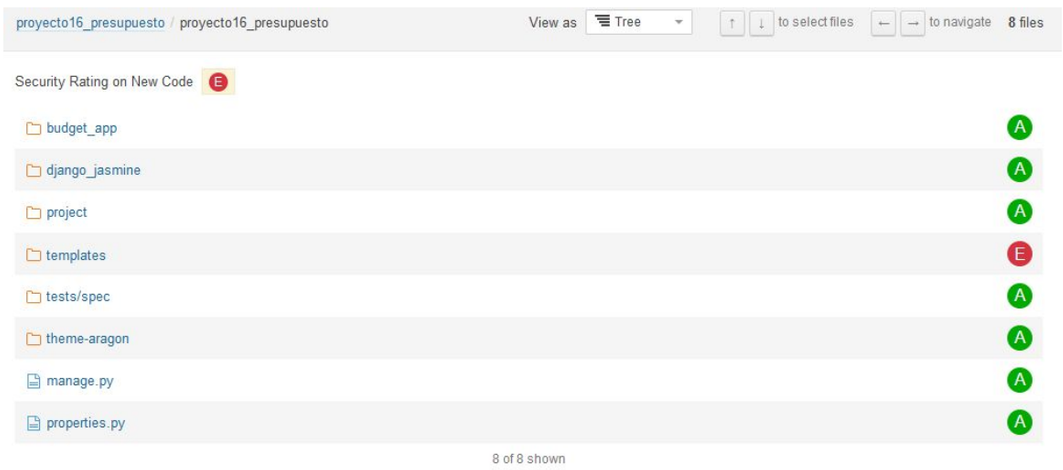
7. Recomendaciones y conclusiones

7.1. Seguridad

- El sitio web cuenta con protección ante ataques comunes de robo de información.

7.2. Confiabilidad

- La seguridad de todos los módulos son buenos a excepción del módulo de templates, pero este solo necesita solucionarlo agregando el atributo rel="noopener noreferrer" con eso se soluciona.



7.3. Usabilidad

- El sitio cuenta con un buen diseño para los equipos de escritorio y tambien es comodo en su diseño móvil.
- El sitio es sencillo de utilizar.

8. Bibliografía

Normas ISO/IEC 25000. Tomado de https://iso25000.com/index.php/normas-iso-25000

9. Firma del perito

Responsable de la evaluación	**Firma**
Nombre: Juan Diego Gomez Gomez Empresa: CRISMAX S.A. GitHub: **JuanDiegoGomezGomez**	JUANDIEGOGOMEZ