

Solución a problemas de carga de imágenes externas en MantisBT

Problema

Al intentar mostrar imágenes alojadas en dominios externos dentro de los tickets de MantisBT, las imágenes no se cargan correctamente a pesar de que la sintaxis Markdown utilizada es correcta:

```
![Nombre de la imagen](https://dominio-externo.com/ruta/imagen.jpg)
```

El navegador bloquea la carga de estas imágenes aunque la URL sea accesible directamente.

Análisis mediante herramientas de desarrollo web

Al inspeccionar la consola del navegador, aparecen errores similares a:

```
Refused to load the image 'https://dominio-externo.com/imagenes/sitelight/App_500.jpg' because it violates the following Content Security Policy directive: "img-src 'self' data:".
```

Este error indica que MantisBT está implementando una política de seguridad de contenido (CSP) que restringe la carga de imágenes únicamente desde:

- El mismo origen ('self')
- URLs con esquema data: (imágenes codificadas en base64)

Documentación oficial relevante

La configuración de seguridad de MantisBT se explica en la documentación oficial:

- [Configuración del servidor web](#)
- [Configuración de seguridad](#)

Según la documentación, MantisBT implementa varias cabeceras de seguridad para proteger la aplicación, incluyendo Content-Security-Policy que puede ser personalizada mediante la configuración `$g_custom_headers`.

Soluciones

Solución 1: Desactivación total de la política CSP (NO RECOMENDADA)

Esta solución elimina completamente la protección CSP, lo que supone un riesgo de seguridad y NO se recomienda excepto para entornos de prueba aislados.

```
// Añadir al archivo config_inc.php
$g_custom_headers = array( 'Content-Security-Policy:' );
```

⚠⚠⚠ **ADVERTENCIA:** Esta configuración elimina toda la protección CSP, exponiendo potencialmente la aplicación a ataques XSS y de inyección de contenido. No usar en entornos de producción.

Solución 2: Permitir dominios específicos (RECOMENDADA)

Esta solución mantiene la seguridad general mientras permite imágenes de dominios concretos:

```
// Añadir al archivo config_inc.php
$g_custom_headers = array(
    'Content-Security-Policy: default-src \'self\'; img-src \'self\' data: https://dominio-
    autorizado.com; script-src \'self\' \'unsafe-inline\' \'unsafe-eval\'; style-src \'self\'
    \'unsafe-inline\'; frame-ancestors \'self\';'
);
```

Para permitir múltiples dominios:

```
// Añadir al archivo config_inc.php
$g_custom_headers = array(
```

```
'Content-Security-Policy: default-src \'self\'; img-src \'self\' data:
https://dominio1.com https://dominio2.com https://*.subdominio.com; script-src \'self\'
\'unsafe-inline\' \'unsafe-eval\'; style-src \'self\' \'unsafe-inline\'; frame-ancestors
\'self\';'
);
```

Para permitir cualquier dominio para imágenes (menos seguro):

```
// Añadir al archivo config_inc.php
$g_custom_headers = array(
    'Content-Security-Policy: default-src \'self\'; img-src * data:; script-src \'self\'
\'unsafe-inline\' \'unsafe-eval\'; style-src \'self\' \'unsafe-inline\'; frame-ancestors
\'self\';'
);
```

Explicación de la política CSP

La directiva Content-Security-Policy utilizada en la solución mantiene:

- `default-src 'self'`: Por defecto, todos los recursos se cargan solo del mismo origen
- `img-src 'self' data: https://dominio-autorizado.com`: Las imágenes pueden cargarse del mismo origen, vía data URLs, y desde el dominio específico
- `script-src 'self' 'unsafe-inline' 'unsafe-eval'`: Scripts necesarios para el funcionamiento de MantisBT
- `style-src 'self' 'unsafe-inline'`: Estilos CSS necesarios para MantisBT
- `frame-ancestors 'self'`: Previene clickjacking limitando qué sitios pueden incrustar MantisBT en frames

Verificación

Después de aplicar la configuración:

1. Guarde los cambios en el archivo `config_inc.php`
2. Limpie la caché del navegador
3. Recargue la página de MantisBT
4. Verifique que las imágenes desde los dominios autorizados se cargan correctamente

Solución de problemas

Si después de aplicar la configuración las imágenes siguen sin cargarse:

1. Verifique que la URL de la imagen es accesible directamente
2. Compruebe que la sintaxis de la directiva CSP es correcta (comillas simples, espacios entre dominios)
3. Examine la consola del navegador para ver mensajes de error específicos
4. Asegúrese de que no haya otras restricciones a nivel de servidor web (Apache, Nginx) que puedan estar afectando

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Revision #1

Created 21 May 2025 11:03:56 by Abkrim

Updated 21 May 2025 11:04:13 by Abkrim