Mod Security Logs

ModSecurity

Por qué NO conviene “desactivar reglas globalmente” y cómo beneficia al servidor

---

1. ¿Qué es ModSecurity?

ModSecurity (o **ModSec**) es un **cortafuegos de aplicaciones web (WAF)** que inspecciona cada petición HTTP antes de que llegue a tu sitio.
Detecta patrones de ataque (SQL-Injection, XSS, bots, etc.) y puede **bloquear** o **registrar** la petición.

---

2. Resultados reales en Castris

> Con una instalación robusta y una depuración progresiva de falsos positivos (por usuario, URL y software), el número de hackeos **ha descendido a niveles que no veíamos desde 2001**.

En otras palabras, **cada regla bien ajustada = un intento de intrusión menos**.

---

3. El error habitual: “Rule desactivada globalmente”

Mito	Realidad
“Si una regla salta como falso positivo, quítala para todos.”	Esa regla puede seguir bloqueando ataques en otras webs e incluso al usuio que se quejo de esa regla. Desactivarla globalmente abre un agujero innecesario.

---

4. Cómo gestionar falsos positivos de forma responsable

1. **Identificar el caso concreto** (URL, usuario, software).
2. **Revisar el log de ModSecurity**: ver la **ID de la regla** que se dispara.
3. **Excluir la regla solo para ese contexto** (ubicación, dominio, etc.).
4. **Documentar** la exclusión para futuras auditorías.

Esto se traduce en:

> *Regla madura + exclusión localizada* → **Seguridad intacta y cero molestias** para el usuario legítimo.

---

5. Beneficios de esta metodología

- **Menos hackeos**: reglas útiles siguen activas para el resto del servidor.
- **Soporte eficiente**: el equipo sabe dónde y por qué se excluyó.
- **Historial limpio**: facilita nuevos ajustes sin “parches” confusos.
- **Confianza del usuario**: menos falsos bloqueos y sitio más seguro.

---

6. Conclusión

Desactivar reglas globalmente es una “solución rápida” que **socava la seguridad**.
Con un proceso de revisión puntual y controlado:

1. Se mantiene la **protección integral de ModSecurity**.
2. El usuario final navega sin bloqueos injustificados.
3. El equipo de soporte puede rastrear, justificar y revertir cualquier cambio.

Respetar las reglas = proteger el servidor y la reputación del proyecto.

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 #2
Created 2025-06-19 08:29:54 UTC by Abkrim
Updated 2025-06-19 08:58:46 UTC by Abkrim