

## Google AdSense vulnerable a ataque 'phishing'

Google AdSense es un dispositivo publicitario perteneciente al popular buscador Google. Para que el dueño de una página pueda ofrecer este servicio, es necesario que se registre como usuario a través de <https://www.google.com/adsense>. Su página, aun protegida por SSL, sufre de una vulnerabilidad que puede ser aprovechada para llevar a cabo ataques de tipo phishing de una forma ridículamente sencilla.

Google AdSense permite a los dueños de las páginas mostrar en sus webs publicidad no invasiva relacionada con el perfil del visitante y proporcionada por Google. Es una vía inteligente de rentabilizar las visitas, pues los usuarios prefieren la publicidad que no molesta y además se adecua a sus necesidades o inquietudes.

Los responsables de las páginas que muestren este tipo de anuncios, deben darse de alta como usuarios en <https://www.google.com/adsense>, una página que, aun protegida por el protocolo SSL (se aprecia en la "s" de https) que se supone garantiza el cifrado de los datos, sufre de un problema de validación de páginas no existentes. Esto brinda la oportunidad a cualquiera de inyectar código en la URL que simule una página válida y desviar los datos al servidor de un tercero de una forma trivial.

La víctima burlada apenas podrá distinguir nada extraño en la barra del navegador puesto que en ella aparecerá la dirección legítima <https://www.google.com/adsense> y si comprueba el certificado de seguridad será completamente válido porque, a diferencia de otros ataques de este tipo, la página en realidad es interpretada por el propio servidor real de Google.

El fallo es un típico problema de "Cross Site Scripting" que permite la interpretación de código HTML en la barra de direcciones del navegador y ha sido descubierto por Hugo Vázquez de Infohacking, quien ya advirtiera sobre diversos fallos de seguridad de este tipo en el sistema de reservas de vuelos de Iberia, los proxy-caché de Telefónica y otras importantes organizaciones.

Más información y referencias:

(Yet another) Google Cross Site Scripting..SSL enabled customer site "AdSense"  
<http://www.infohacking.com/google/index.html>

Sergio de los Santos

Miembro de la Comisión de Seguridad de la Asociación de Internautas

Redactor de Hack Paso a Paso: <http://www.megamultimedia.com/arroba/>

Fecha artículo: 2005-01-12 12:51:01 - url artículo: <http://www.internautas.org/html/408.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)