Secure Information Disclosure

**==========**
**By Dedalo (Dédalo)**
**==========**
**===www.seguridadblanca.blogspot.com ===**
**==========**

Últimamente he estado leyendo muchas cosas sobre las redes sociales, sus errores de privacidad y configuración que no solo cometen los usuarios sino los programadores, ahora yo les voy a enseñar está técnica de pen-test en la cual se puede sacar información no autorizada.

¿De qué se trata el Bug?

- Bueno el bug básicamente es un error de configuración del administrador o del usuario que permite ver más contenido personal de una persona de lo que se debería ver, y por esto se puede conocer mucho de una persona y causar problemas sociales.

¿Cómo se explota?

- Les pongo como ejemplo un último bug que he visto en facebook, por medio de un exploit diseñado en PHP se pueden ver imágenes de personas que no son ni siquiera tus conocidos, este error no es solo del programador por hacer malas consultas sino del usuario por no saber manejar bien su perfil y con esto si yo fuera un secuestrador podría obtener imágenes de la víctima.

¿Que podría pasar si soy vulnerable?

- Pues si tu web es vulnerable a un Secure Information Disclosure lo mejor es hacer un backup y cerrar tu web por mantenimiento y corregir el bug ya sea por un error de Full Path Disclosure, Mala programación de las sentencias Sql o cualquier tipo de bug que permita ver un poco mas haya de lo permitido.

¿Recomendaciones?

- Yo les recomiendo que al encontrar un consultor en seguridad informática o un pen-tester se aseguren que este también examine esta vulnerabilidad en especial si eres el administrador de ya sea un banco o de una red social o simplemente de una web que al mostrar más información de la debida puede ser demandada, y además no siempre son errores del lenguaje de programación sino errores que se dan por un mal orden de las sentencias de su base de datos.

Saludos
Dedalo (Dédalo)
http://www.seguridadblanca.blogspot.com