Reflexión y Análisis

Vulnerabilidades(técnicas)

1. Falta de validación
    a. El servidor web del sitio clonado no valida correctamente las los datos introducidos por el usuario antes de guardarlas. El script solo recibe y las registra.
2. Ausencia de protocolos seguros
    a. El sitio clonado al ser una copia no implementa HTTPS o la validación de certificados, exponiendo las credenciales.
3. Ingeniería social (Técnica de redirección)
    a. El atacante redirige a la victima a una página web clonada donde interactúa con una interfaz falsa.

Vulnerabilidades(humanas)

1. Confianza
    a. Las personas mayormente confían en la apariencia del sitio web, mientras más idéntica sea, el usuario será más propensa a introducir sus datos.
2. Pasotismo
    a. Dicho anteriormente las personas no suelen verificar las URLs, los dominios, etc.
3. Intriga
    a. La simple curiosidad o descuido pueden hacer que un usuario introduzca información sensible a un formulario/pág.

Consecuencias para una Victima real

1. Robo de Identidad y Credenciales
    a. El atacante obtiene acceso a lo que puede incluir el acceso a correos, redes sociales, servicios bancarios, etc.
2. Acceso no autorizado
    a. Si los datos robados se utilizan para acceder a sistemas o información sensible puede resultar en brechas de datos, robo de propiedad intelectual, etc.
3. Fraude
    a. Acceso a cuentas bancarias o de pago puede llevar al robo de fondos o a transacciones fraudulentas.
4. Daño reputación
    a. Si se comprometen cuentas de redes sociales o correos, el atacante puede utilizarlas para difundir información falsa, dañar la reputación de la victima o realizar estafas a sus contactos.

Medidas preventivas

1. Verificar url
    a. Antes de introducir cualquier información, hay que comprobar cuidadosamente la dirección web en la barra del navegador (errores tipográficos, dominios extraños, subdominios, etc.)
2. Desconfiar de correos electrónicos o mensajes inesperados
    a. Ser escépticos con lo que nos llegan, correos electrónicos, mensajes de texto, notificaciones, etc. Evitar hacer clicks en enlaces o descargar archivos adjuntos de fuentes no confiables
3. Utilizar autenticación de dos pasos(2FA)
    a. Habilitar la 2FA en todas las cuentas que lo permitan, debido a que, si un atacante obtiene tu contraseña, necesitará un segundo factor para acceder a tu cuenta (como un código enviado al móvil), lo que aumenta la seguridad.

Fines educativos

1. Ética y legalidad
    a. Mucho de estos actos es un delito y puede acarrear severas consecuencias legales.
2. Impacto Real
    a. Un atacante de phishing exitoso puede arruinar la vida de una persona o causar pérdidas millonarias a una empresa.
3. Responsabilidad profesional
    a. Hay que usar el conocimiento para proteger, y no para atacar. El uso indebido puede llevar a regulaciones más estrictas que limiten el acceso a herramientas.