Hackean Una Cuenta En PayPal Con Un Sólo Clic

Paypal es uno de los servicios de transferencia de pago «más seguros» que cualquier persona puede usar, pero, siendo realistas, **ningún sistema informático puede brindar seguridad**. Este servicio propiedad de eBay, ha demostrado ser vulnerable en el pasado, ya que se podría realizar fraude de forma fácil. Ahora se ha hecho provecho de una vulnerabilidad critica de las aplicaciones web, que podría permitir a un atacante **tomar el control de la cuenta de PayPal** de los usuarios con sólo un clic, afectando a más de 156 millones de usuarios de PayPal.

Un investigador de seguridad egipcia, Yasser H. Ali, ha descubierto tres vulnerabilidades críticas en el sitio web de PayPal incluyendo ***CSRF***, bypass por Auth token y Restablecimiento de la pregunta de seguridad, que podría ser utilizado por los ciberdelincuentes en los ataques dirigidos.

Cross-Site Request Forgery (CSRF o XSRF) es un método que se usa para atacar a un sitio web, en el que un atacante necesita convencer a la víctima a **hacer clic en un HTML** especialmente diseñado página que hará una petición a la página web vulnerable.

Yasser demostró el paso a paso de la vulnerabilidad en el video de prueba de concepto (PoC), utilizando un solo exploit que combina las tres vulnerabilidades. De acuerdo con la demo, a través de CSRF un atacante es capaz de asociar en secreto un nuevo ID de correo electrónico secundaria (Email del atacante) a la cuenta de la víctima en Paypal , y también restablecer las respuestas de las preguntas de seguridad de la víctima.

PayPal utiliza seguridad por medio de tokesn Auth para detectar las peticiones del titular de la cuenta, pero el

señor **Yasser** anulada con éxito para **generar el código de explotación** para los ataques dirigidos, como se muestra en el video.

> *Yasser dijo: «me enteré de que la autenticación con CSRF es reutilizable para esa dirección de correo electrónico de usuario o nombre de usuario específico, esto significa que si un atacante encontró algunos de estos CSRF Tokens, él puede hacer que las acciones en el comporte de cualquier usuario conectado «.*

Una vez ejecutado, el exploit añadirá el correo electrónico de identificación del atacante a la cuenta de la víctima, que podría ser utilizado para restablecer la contraseña de la cuenta usando la opción de la página web de Paypal «He olvidado la contraseña». Sin embargo, el atacante no puede cambiar la contraseña de la víctima sin responder a las preguntas de seguridad configuradas por el usuario al registrarse.

Yasser encontró otro **bug en PayPal,** el cual permite restablecer las preguntas y respuestas de seguridad elegidas por el usuario, por lo tanto, esto le facilita pasar por alto la característica de seguridad de PayPal por completo con el fin de restablecer la nueva contraseña para la cuenta de la víctima.

El equipo de **seguridad de Paypal** ha parcheado la vulnerabilidad después que Yasser ha informado sobre el bug en el Programa de Recompensas. Hace tres meses, Yasser encontró error similar en el sitio web de eBay que permitía a los hackers robar cualquier cuenta de eBay en tan sólo 1 minuto.