Bussiness Logic Abuse

Business Logic Abuse

Falla en el diseño o la implementación de una funcionalidad que permite exportarla de tal forma que se impacta de forma negativa a la empresa.

Business Logic Abuse

- Una vulnerabilidad que explota la lógica empresarial de una aplicación para obtener beneficios indebidos.
- No se trata de una vulnerabilidad técnica como las vulnerabilidades de inyección SQL o XSS, sino más bien de manipular el flujo lógico de la aplicación para obtener resultados no previstos.

Ejemplos de Business Logic Abuse

- Cambiar el precio de un artículo mediante la manipulación del flujo de la aplicación, como interceptar solicitudes de compra o modificar parámetros de URL.
- Ejemplo: Aprovechar un descuento de primer pedido múltiples veces.

Ejemplos de Business Logic Abuse

- Explotación de sistemas de recompensas y puntos
- Manipulación del flujo de la aplicación para obtener puntos o recompensas de forma no autorizada.
- Ejemplo: Aprovechar una promoción de referidos para obtener beneficios sin cumplir con las condiciones.

Consecuencias del Business Logic Abuse

- Pérdidas financieras para las empresas.
- Daño a la reputación de la marca.
- Violación de la confianza del cliente.
- Posible acción legal y reguladora.

Estrategias de Mitigación

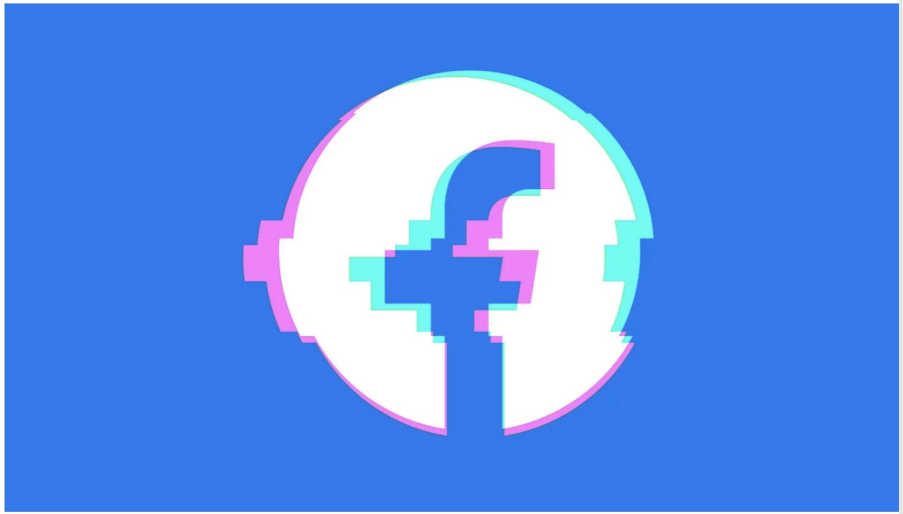
- Implementación de controles de seguridad adicionales:
  - Validación de lógica empresarial en el lado del servidor.
  - Monitoreo de patrones de comportamiento sospechoso.
  - Auditorías de seguridad regulares.
  - Capacitación del personal en seguridad de aplicaciones.

Casos de la vida real

Hacker finds bug that allowed anyone to bypass Facebook 2FA

Lorenzo Franceschi-Bicchierai @lorenzofb / 1:56 PM GMT-3 • January 30, 2023

Comme



Google Pixel screen-lock hack earns researcher $70k

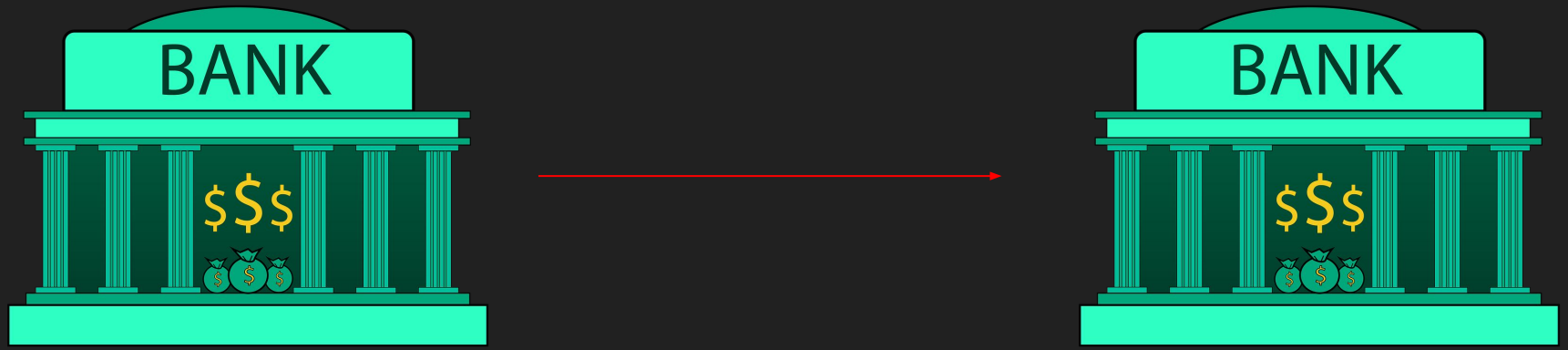
John Leyden 10 November 2022 at 16:14 UTC
Updated: 11 November 2022 at 11:23 UTC

Hacking News | Vulnerabilities | Mobile

Android security pwned by PUK reset trick

Casos de la vida real

```
{
"Transferencia": true,
"Desde": "Hacker",
"Hacia": "Victima",
"Valor_a_transferir":"-15000"
}
```

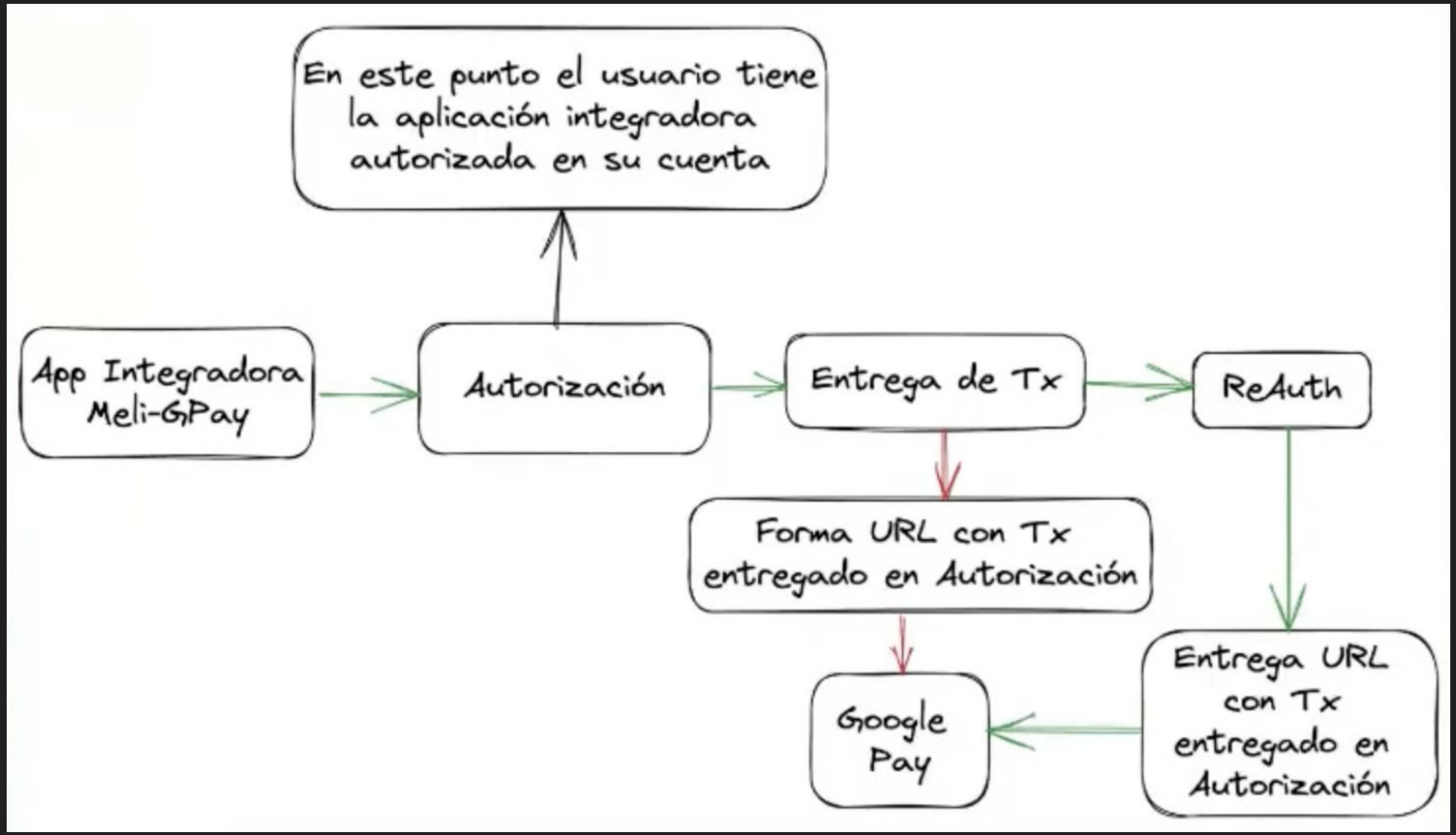


```
{
"Transferencia": true,
"Desde": "Hacker",
"Hacia": "Victima",
"Valor_a_transferir":"-15000"
}
```


$15.000

$0

Bypass ReAuth Google Pay


En este punto el usuario tiene la aplicación integradora autorizada en su cuenta
App Integradora Meli-GPay
Autorización
Entrega de Tx
ReAuth
Forma URL con Tx entregado en Autorización
Google Pay
Entrega URL con Tx entregado en Autorización

```
46      public boolean validateTransaction(String userId) {
47  +       return this.userId.equals(userId) && Boolean.TRUE.equals(this.isReauthValidated);
```

Laboratorio

https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls

Conclusiones

- Business Logic Abuse es una vulnerabilidad que explota la lógica empresarial de una aplicación.
- Puede tener graves consecuencias financieras y de reputación.
- La mitigación requiere una combinación de medidas técnicas y procesos de seguridad.