Banco Feliz S.A
Informe De Pruebas De Penetración

Información Confidencial

Fecha: 24 de Enero de 2023

Version 1.0

Tabla de Contenido

Declaración de confidencialidad

Este documento es propiedad exclusiva de Banco Feliz S.A y Hack Force. Este documento contiene información patentada y confidencial. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento tanto de Banco Feliz S.A como de Hack Force.
Banco Feliz S.A puede compartir este documento con auditores bajo acuerdos de no divulgación para demostrar el cumplimiento de los requisitos de las pruebas de penetración.

Descargo de responsabilidad

Las conclusiones y recomendaciones reflejan la información recopilada durante la evaluación y no los cambios o modificaciones realizados fuera de ese período.
Los compromisos limitados en el tiempo no permiten una evaluación completa de todos los controles de seguridad. Hack Force priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. Hack Force recomienda llevar a cabo evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

Informacion de Contacto

Nombre	Titulo	Informacion de contacto
Banco Feliz S.A		
Willian Blanco	Gerente IT.	Email: wblanco@bancofeliz.com
Hack Force		
Ewor01	Pentester Junior	Email: ewor01@hackforce.com

Resumen de la evaluación:

Del 21 de Enero de 2023 al 24 de Enero de 2023, Banco Feliz contrató a Hack Force para evaluar la postura de seguridad de su infraestructura en comparación con las mejores prácticas actuales del sector que incluían una prueba de penetración en la red interna.

Las fases de las actividades de pruebas de penetración incluyen las siguientes:

- Planificación - Se reúnen los objetivos del cliente y se obtienen las reglas de compromiso.
- Reconocimiento - Identificar ante qué equipo se está, si es Windows o si es Linux, que puertos y servicios están corriendo en él y si es una página web que tecnologías utiliza, etc.
- Análisis de Vulnerabilidades - Realizar escaneos y enumeraciones para identificar versiones de servicios dados a través de un puerto, para lograr dar con los recursos necesarios.
- Explotación - Confirmar las vulnerabilidades potenciales mediante la explotación y realizar descubrimientos adicionales en caso de nuevos accesos.
- Informes - Documentar todas las vulnerabilidades y explotaciones encontradas, los intentos fallidos y los puntos fuertes y débiles de la empresa.

Componentes de la evaluación

Pruebas de penetración interna.

Una prueba de penetración interna emula el papel de un atacante desde dentro de la red. Un ingeniero escaneará la red para identificar posibles vulnerabilidades del host y realizar ataques comunes y avanzados a la red interna. El ingeniero tratará de obtener acceso a los hosts tratando de comprometer los diferentes servicios expuestos para así tomar control de las máquinas y filtrar datos sensibles.

Índices de gravedad de los hallazgos

La siguiente tabla define los niveles de gravedad y el rango de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Gravedad	CVSS V3 Rango de puntuación	Definición
Crítica	9.0-10.0	La explotación es sencilla y suele resultar en un compromiso a nivel de sistema. Se aconseja elaborar un plan de acción y parchear inmediatamente.
Alta	7.0-8.9	La explotación es más difícil, pero podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y parchear lo antes posible.
Moderada	4.0-6.9	Existen vulnerabilidades pero no son explotables o requieren pasos adicionales como la ingeniería social. Se aconseja elaborar un plan de acción y aplicar parches una vez resueltos los problemas de alta prioridad.
Baja	0.1-3.9	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de una organización. Se aconseja elaborar un plan de acción y parchear durante el próximo mantenimiento.
Informativa	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos detectados durante las pruebas, los controles estrictos y la documentación adicional.

Factores de Riesgo

El Riesgo se mide por 2 factores: Probabilidad e Impacto:

Probabilidad

La probabilidad mide el potencial de explotación de una vulnerabilidad. Las puntuaciones se otorgan en función de la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

Impacto

El impacto mide el efecto potencial de la vulnerabilidad en las operaciones, incluyendo la confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, el daño a la reputación y las pérdidas financieras.

Objetivo

Evaluación	Detalle
Test de Penetración Interno	192.168.0.215 192.168.0.207

Permisos de Cliente

Banco Feliz S.A proporciono a Hack Force los siguientes derechos:

- Acceso interno a la red a través de una VPN.

Resumen Ejecutivo

Hack Force evaluó la postura de seguridad interna de Banco Feliz S.A mediante pruebas de penetración del 21 de Enero de 2023 al 24 de Enero de 2023. Las siguientes secciones proporcionan una visión general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

Se establecieron limitaciones de tiempo para las pruebas. Las pruebas de penetración en la red interna se permitieron durante 4
(4) días laborables.

Resumen de las pruebas

Se pudieron observar múltiples servicios expuestos y con vulnerabilidades tales como:

Servicio Ftp con versión vulnerable de vstfpd 2.4.3 y se logró explotar una vulnerabilidad para dicho servicio y así obtener el acceso total al equipo (Encontrar en PPI-001).

Utilizando el servicio Telnet se logró obtener acceso al equipo, donde se podía visualizar la información que poseía en un banner donde estaban expuestas sus credenciales y así poder ganar acceso al mismo (Encontrar en PPI-002).

Haciendo uso de la herramienta metasploit se logró vulnerar el servicio Samba de dicho equipo para así poder obtener acceso y control total del mismo (Encontrar en PPI-003).

Haciendo uso de netcat mediante una conexión inversa logramos conectarnos al equipo mediante una vulnerabilidad expuesta en el puerto 1524 sobre el servicio Ingreslock que nos permitía entablar la conexión sin problemas (Encontrar en PPI-004).

Haciendo uso de metasploit logramos vulnerar el servicio VNC extraer las credenciales de conexión a dicho servicio, en el cual posteriormente nos conectamos mediante una herramienta de escritorio remoto y tomar control sobre el equipo (Encontrar en PPI-005).

Se logró concluir que la siguiente aplicación web bWAPP tiene múltiples vulnerabilidades, una de ellas HTML Injection, lo que nos permitía alterar dicho contenido de la página (Encontrar en PPI-006).

Luego se siguió inspeccionando y como usa un protocolo de conexión insegura HTTP se pudo realizar un ataque denominado Man In The Middle y así obtener las credenciales en texto claro (Encontrar en PPI-007).

Se encontró otra vulnerabilidad la cual nos permitía inyectar código en el equipo, denominada como PHP Code Injection y así se obtuvo una conexión reversa para ganar acceso al equipo (Encontrar en PPI-008).

Utilizando Burpsuite una herramienta para interceptar conexiones, lo que se conoce como proxy, se logró determinar que el sitio era vulnerable a sql injection, modificando así la petición interceptada por el proxy y reenviándola nuevamente al sitio en el cual nos mostró un error de base de datos MYSQL (Encontrar en PPI-009).

El resto de las conclusiones fueron altas, moderadas, bajas o informativas. Para más información sobre los resultados, consulte la sección Resumen técnico.

Notas y recomendaciones de las pruebas

Los resultados de las pruebas de la red de Banco Feliz S.A son indicativos de una organización que se somete a su primera prueba de penetración, como es el caso. Muchos de los hallazgos descubiertos son vulnerabilidades dentro de los servicios más comunes utilizados habitualmente y que poseen configuraciones por defecto o servicios desactualizados lo que conlleva a que estén expuestos a múltiples vulnerabilidades.

Durante las pruebas, destacaron algunas constantes: un parcheado débil, lo que conllevo a que la mayoría de los servicios expuestos fueran vulnerables debido a la antigüedad de estos, lo que condujo al compromiso inicial del equipo ya que son uno de los puntos de apoyo que un atacante intenta utilizar en una red.

Recomendamos que Banco Feliz S.A realice evaluaciones periódicas de vulnerabilidad**:** Como parte de una estrategia eficaz de gestión de riesgos de la organización, las evaluaciones de vulnerabilidad deben llevarse a cabo de forma regular. Hacerlo permitirá a la organización determinar si los controles de seguridad instalados están correctamente instalados, funcionando según lo previsto y produciendo el resultado deseado

Implantar un programa de gestión de parches: La aplicación de un programa coherente de gestión de parches es un componente importante para mantener una buena postura de seguridad. Esto ayudará a limitar la superficie de ataque que resulta de ejecutar servicios internos sin parches.

Siguiendo estas recomendaciones Banco Feliz S.A debería lograr prevenir posibles ataques dentro de su red.

Puntos fuertes y débiles

A continuación se identifican los principales puntos fuertes detectados durante la evaluación:

1. Se observó múltiples servicios desactualizados
2. Al igual que muchas páginas web con plugins y tecnologías antiguas
3. Exploits que otorgaban acceso al Sistema como Root

A continuación se identifican los principales puntos débiles clave identificados durante la evaluación:

1. Servicio FTP desactualizado
2. Servicio Telnet antiguo
3. Servicio Samba desactualizado
4. Servicio Ingreslock
5. Servicio VNC desactualizado
6. Inyección de código HTML
7. Protocolo inseguro HTTP
8. Inyección de código PHP
9. Inyecciones SQL

Resumen e informe de vulnerabilidades

Las tablas siguientes ilustran las vulnerabilidades encontradas por impacto y las soluciones recomendadas:

Resultados de la prueba de penetración interna

5	2	2	0	0
Crítica	Alta	Moderada	baja	Informativa

Encontrando	Gravedad	Recomendación
Pruebas de Penetración Interna		
PPI-001: Servicio FTP desactualizado versión utilizada 2.3.4	Crítica	Actualizar Vsftpd a la versión más reciente.
PPI-002: Servicio Telnet servicio antiguo	Crítica	Utilizar SSH en su versión más reciente en lugar de Telnet.
PPI-003: Servicio Samba desactualizado	Crítica	Actualizar Samba a la versión más reciente.
PPI-004: Servicio Ingreslock, se obtiene una bindshell con máximos privilegios	Crítica	Actualizar el servicio a su versión más reciente o desactivarlo.
PPI-005: Servicio VNC desactualizado	Crítica	Cifrar las conexiones VNC, actualizar el servicio y usar contraseñas robustas.
PPI-006: Inyección de código PHP	Alta	La sanitización y el manejo de la entrada del usuario son primordial para la seguridad de las aplicaciones PHP.
PPI-007: Inyección de código SQL	Alta	Una medida habitual consiste en duplicar las comillas simples que aparecen en la información introducida por el usuario antes de incorporarla a una consulta SQL.
PPI-008: Protocolo inseguro HTTP	Moderada	Utilizar la versión segura del protocolo, la cual sería HTTPS.
PPI-009: Inyección de código HTML	Moderada	Se debe comprobar si cada entrada contiene algún código script o HTML

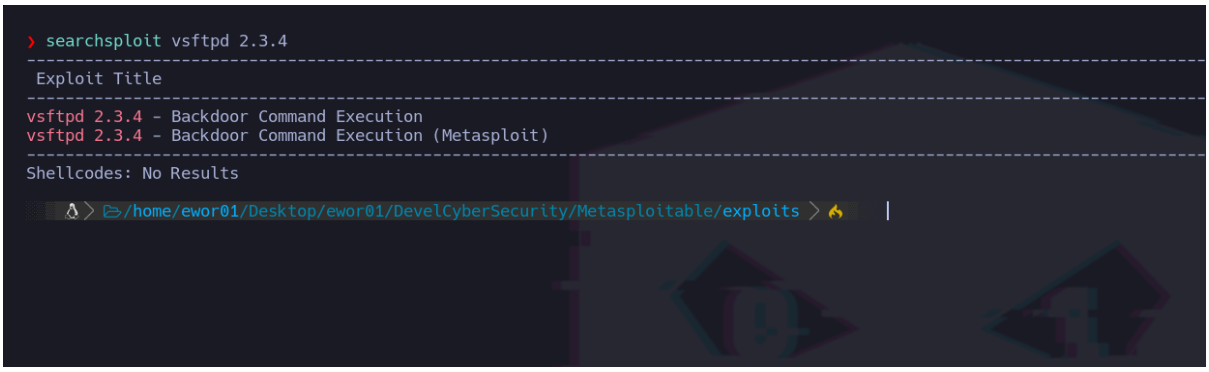
Resumen técnico

Resultados de la prueba de penetración interna

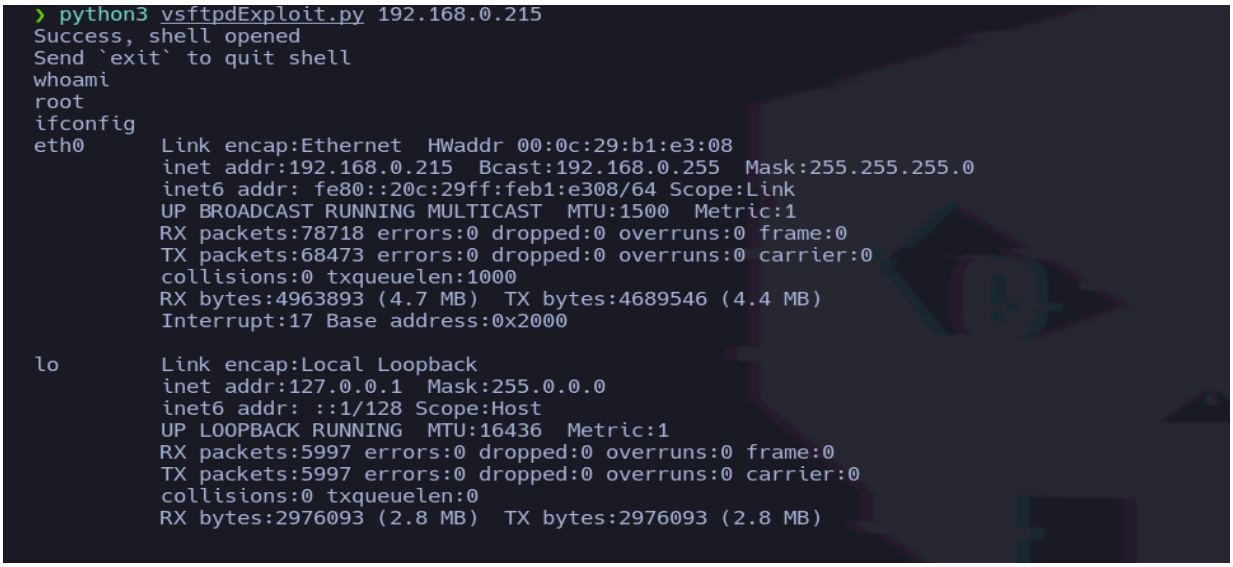
Encontrado PPI-001: Servicio FTP desactualizado versión utilizada 2.3.4 (Critica)

Descripcion:	Banco Feliz S.A utiliza el servicio FTP en su versión desactualizada permitiendo así la explotación de la vulnerabilidad vsftpd en su versión 2.3.4 la cual permite la ejecución de código.
Riesgo:	Probabilidad: Alta – Este ataque es muy efectivo en todas las versiones antiguas de Vsftpd. Impacto: Muy Alto – La ejecución de código permite a los atacantes tomar el control del sistema.
Referencias:	https://www.cvedetails.com/cve/CVE-2011-2523

Evidencia



Podemos observar los exploit para esa versión de vsftpd.



Corrección:
Actualice a la última versión del software.

Encontrado PPI-002: Servicio Telnet demasiado antiguo (Critica)

Descripción:	Banco Feliz S.A utiliza el servicio Telnet el cual se considera inseguro debido a su antigüedad.
Riesgo:	Probabilidad: Alta – Este ataque es muy efectivo ya que Telnet se considera un protocolo de comunicación obsoleto. Impacto: Muy Alto – Ya que existen múltiples exploit para el servicio Telnet.
Referencias:	https://nvd.nist.gov/vuln/detail/CVE-1999-0619

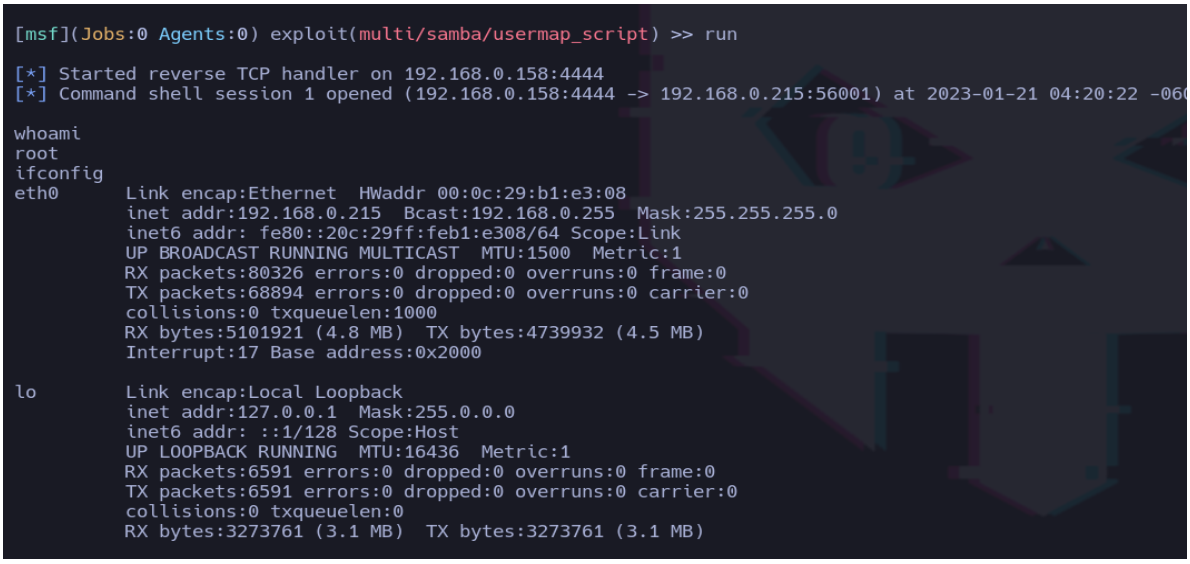
Evidencia

Corrección:
El servicio Telnet es un protocolo inseguro y obsoleto y debe ser desactivado. Existen alternativas seguras como SSH.

Encontrado PPI-003: Servicio Samba desactualizado (Critica)

Descripción:	Banco Feliz S.A utiliza el servicio Samba en versiones muy antiguas lo que conlleva a múltiples ataques, en este caso se utilizó metasploit para lograr ejecución de código.
Riesgo:	Probabilidad: Alta – Este ataque es muy efectivo ya que Samba es un servicio muy utilizado pero al estar desactualizado es una vía potencial de ataque. Impacto: Muy Alto – Ya que existen múltiples exploit para el servicio Samba
Referencias:	https://www.cvedetails.com/cve/CVE-2007-2447/?q=CVE-2007-2447

Evidencia

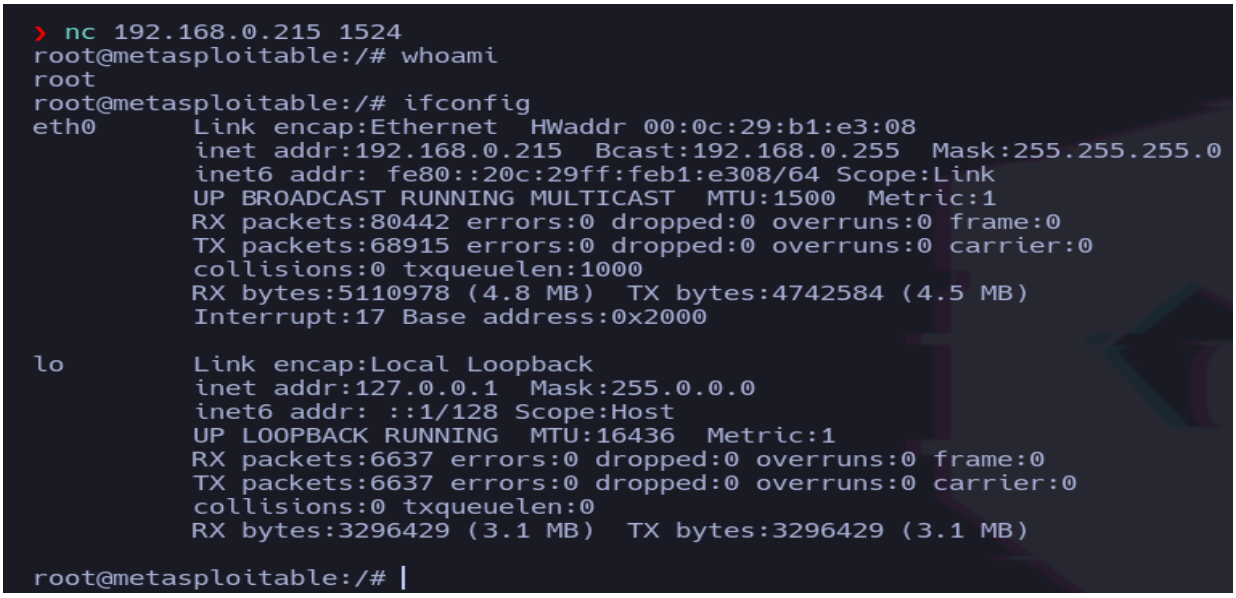


Corrección:
El servicio Samba debe ser desactivado en caso de o utilizarse y si se utiliza se recomienda actualizar a la última versión.

Encontrado PPI-004: Servicio Ingreslock (Critica)

Descripción:	Banco Feliz S.A utiliza el servicio Ingreslock para conexiones TCP lo cual conlleva a una ejecución de código al estar activado dicho servicio y desactualizado.
Riesgo:	Probabilidad: Alta – Este ataque es muy efectivo ya que nos na la posibilidad de ejecutar código en el equipo. Impacto: Muy Alto – Los atacantes pueden aprovechar este problema para ejecutar código y comprometer el sistema.
Referencias:	No hay referencias.

Evidencia

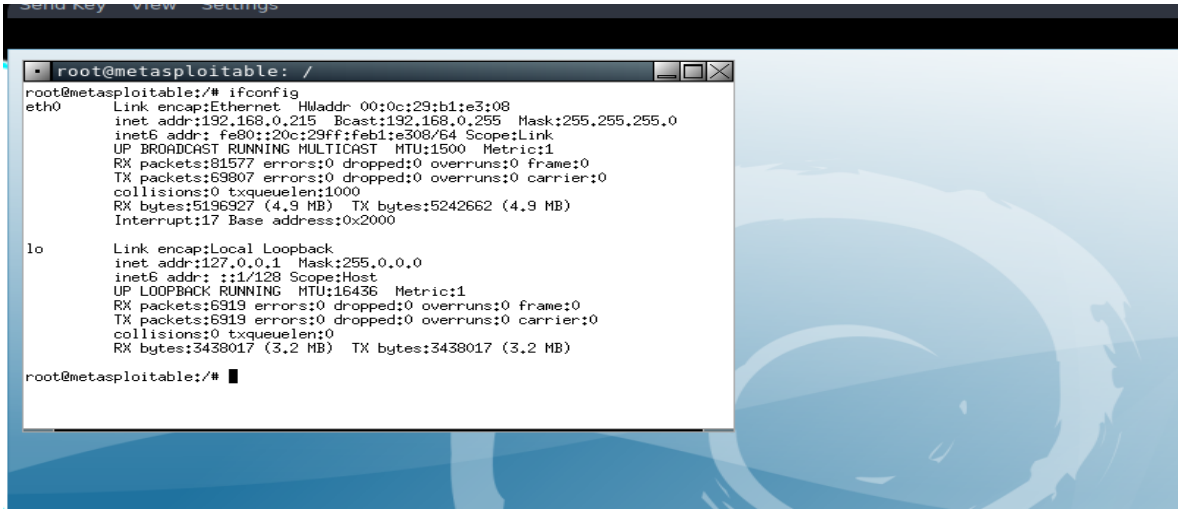


Corrección:
Una solución temporal seria desactivar el servicio.

Encontrado PPI-005: Servicio VNC desactualizado (Critica)

Descripción:	Banco Feliz S.A utiliza el servicio VNC para conexiones de escritorio remoto, pero posee el software desactualizado lo que da entrada a los atacantes de comprometer el equipo.
Riesgo:	Probabilidad: Alta – Este ataque es muy efectivo ya que es uno muy utilizados por los atacantes para obtener el control del equipo. Impacto: Muy Alto – Los atacantes pueden aprovecharse de este servicio y acceder de manera remota mediante software de conexión de escritorio remoto Y comprometer el sistema.
Referencias:	https://www.rapid7.com/db/modules/auxiliary/scanner/vnc/vnc_login/ - VNC Authentication Scanner

Evidencia



Corrección:
Actualizar el servicio VNC a su versión más reciente, utilizar conexiones encriptadas y contraseñas robustas.

Encontrado PPI-006: Inyección de código PHP (Alta)

Descripción:	Se identificó una página web de Banco Feliz S.A la cual permite la inyección de código PHP, permitiendo a un atacante comprometer el equipo.
Riesgo:	Probabilidad: Moderada – Este ataque es muy efectivo en páginas web con versiones de PHP antiguas. Impacto: Alto – Los atacantes pueden ejecutar código en el equipo comprometido y hacer movimientos laterales para escalar privilegios y obtener control total.
Referencias:	https://owasp.org/www-community/attacks/Code_Injection https://cwe.mitre.org/data/definitions/77.html

Evidencia

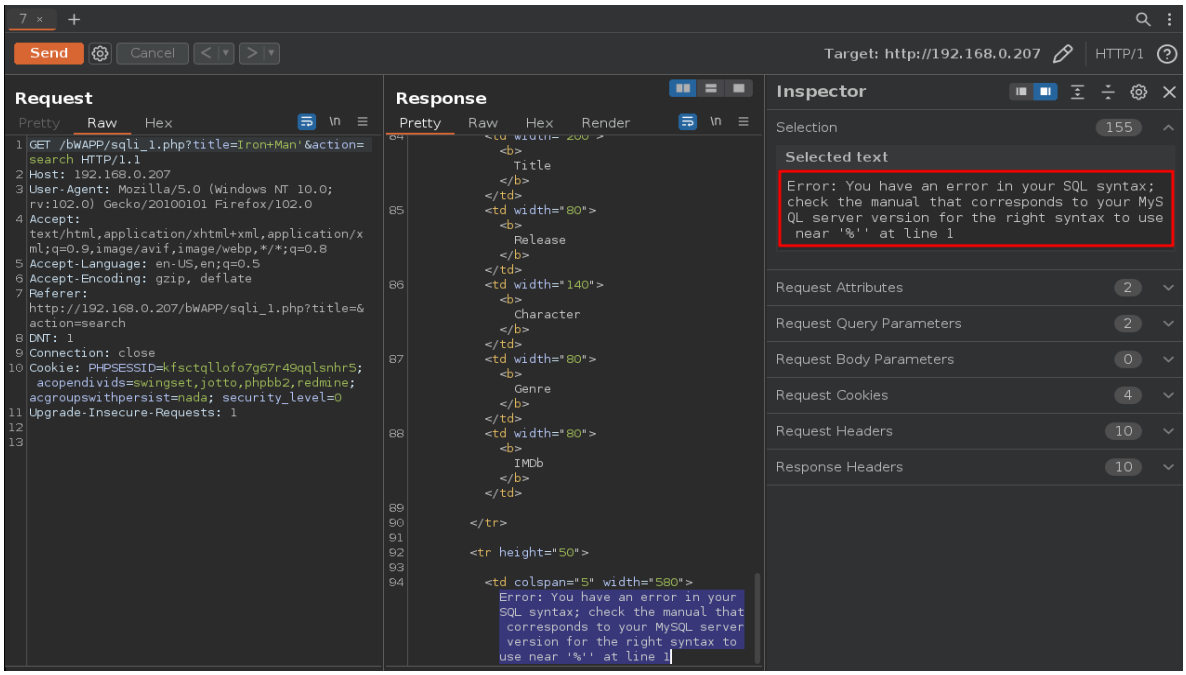
Podemos observar que con la siguiente inyección de código obtenemos una Reverse Shell.

Corrección:
La sanitización y el manejo de la entrada del usuario son primordial para la seguridad de las aplicaciones PHP. Siempre que acepte entradas de usuario, debe asegurarse de que son válidas, almacenarlas y procesarlas de tal manera que no permitan ataques contra la aplicación.

Encontrado PPI-007: Inyección de código SQL (Alta)

Descripción:	Se identificó una página web de Banco Feliz S.A la cual permite las inyecciones SQL, permitiendo a un atacante filtrar información confidencial de la base de datos de la aplicación.
Riesgo:	Probabilidad: Moderada – Este ataque es muy efectivo en páginas web antiguas. Impacto: Alto – Los atacantes pueden ejecutar código en el equipo comprometido filtrar información de la base de datos y extraer credenciales para comprometer totalmente el equipo.
Referencias:	https://portswigger.net/web-security/sql-injection https://cwe.mitre.org/data/definitions/89.html https://capec.mitre.org/data/definitions/66.html

Evidencia

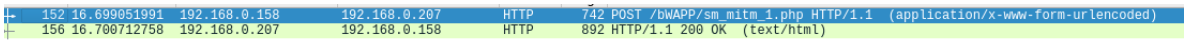


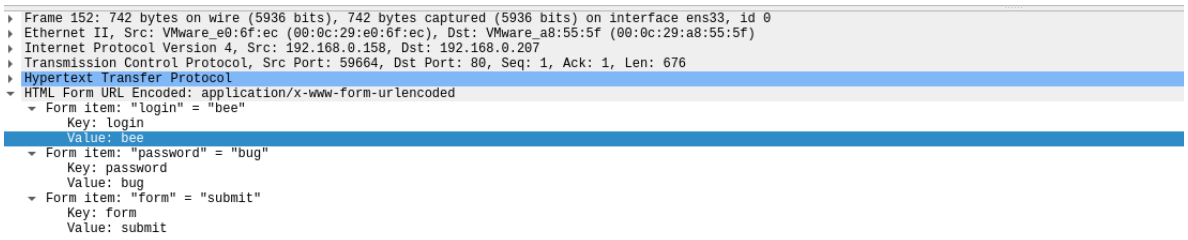
Corrección:
Una medida habitual consiste en duplicar las comillas simples que aparecen en la información introducida por el usuario antes de incorporarla a una consulta SQL. Siempre que acepte entradas de usuario, debe asegurarse de que son válidas, almacenarlas y procesarlas de tal manera que no permitan ataques contra la aplicación.

Encontrado PPI-008: Protocolo Inseguro HTTP (Moderada)

Descripción:	Se identificó una página web de Banco Feliz S.A la cual cuenta con el protocolo inseguro HTTP permitiendo así a un atacante interceptar las conexiones y poder llegar a ver credenciales en texto claro ya que la conexión no posee cifrado.
Riesgo:	Probabilidad: Moderada – Este ataque es muy efectivo en páginas web que usan el protocolo antiguo el cual sería HTTP. Impacto: Moderada – Los atacantes pueden interceptar la conexión mediante una herramienta como wireshark y poder filtrar las credenciales en texto claro de las páginas que utilizan este cifrado.
Referencias:	https://nvd.nist.gov/vuln/detail/CVE-2022-3245

Evidencia





Corrección:
Dejar de utilizar el protocolo HTTP ya que utiliza conexiones sin cifrar, en su lugar utilizar HTTPS que con la versión 1.3 de TLS ya que las anteriores se consideran vulnerables.

Encontrado PPI-009: Inyección de código HTML (Moderada)

Descripción:	Se identificó una página web de Banco Feliz S.A la cual es vulnerable a la inyección de código HTML no se considera muy grave pero se pueden hacer redirecciones maliciosas entre otras cosas.
Riesgo:	Probabilidad: Moderada – Este ataque es muy efectivo en páginas web que no está sanitizado correctamente su código HTML. Impacto: Moderada – Los atacantes pueden hacer por por ejemplo un Login falso en una página y ocultar el original y mediante un poco de ingeniería social hacer que la víctima introduzca sus datos.
Referencias:	https://wiki.owasp.org/index.php/Testing_for_HTML_Injection_(OTG-CLIENT-003) https://www.acunetix.com/vulnerabilities/web/html-injection/

Evidencia

Corrección:
Los scripts de las aplicaciones o páginas web deben filtrar los metacaracteres de la entrada del usuario.