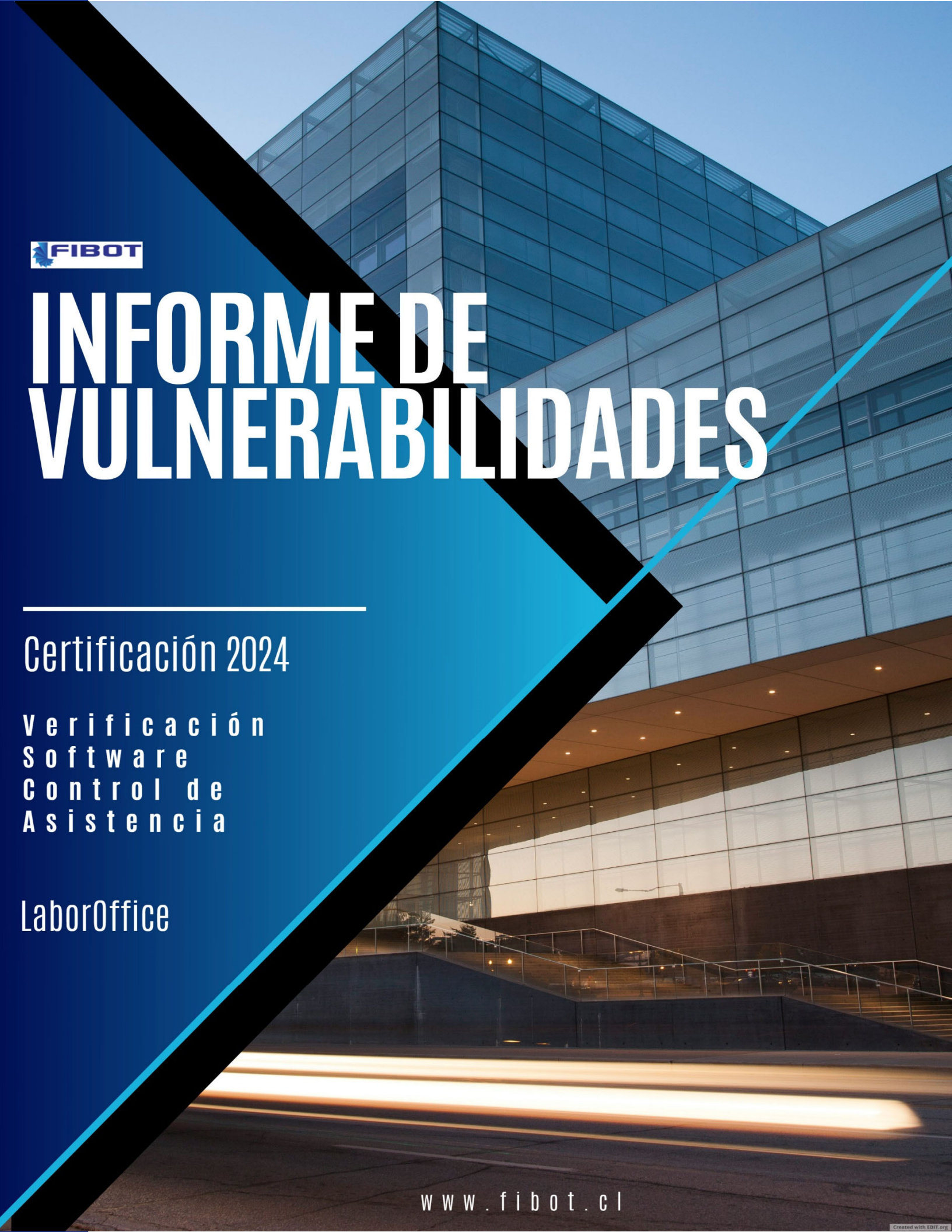


FIBOT

INFORME DE VULNERABILIDADES

Certificación 2024

Verificación Software Control de Asistencia

LaborOffice

www.fibot.cl

CONTENIDO

1. OBJETIVOS

OBJETIVO GENERAL

Examinar el nivel de seguridad existente en la aplicación web transaccional de control de asistencia laboroffice.cl, con el propósito de reconocer e identificar vulnerabilidades de seguridad presentes en ella, las que comúnmente se generan al momento de desarrollar la aplicación.

1.2. OBJETIVOS ESPECÍFICOS

- Realizar un estudio de forma pasiva de la aplicación web, donde se entenderá la lógica la aplicación, las formas de funcionamiento de ésta y sus funcionalidades utilizadas.
- Identificar vulnerabilidades a nivel de aplicación web.

2. DESCRIPCIÓN DEL SISTEMA

El Sistema de Control de Asistencia laboroffice.cl es una aplicación Web que permite a diversos clientes tener una aplicación informática para el control y administración de su personal, en relación a lo que respecta a sus asistencias.

En la

DNS records

name	class	type	data	time to live
latam1.laboroffice.cl	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
laboroffice.cl	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
laboroffice.cl	IN	NS	ns1.dns-parking.com	86400s (1.00:00:00)
laboroffice.cl	IN	NS	ns2.dns-parking.com	86400s (1.00:00:00)
97.105.175.18.in-addr.arpa	IN	PTR	ec2-18-175-105-97.eu-west-2.compute.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns1-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns2-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns3-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns4-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	SOA	server: ns-159.awsdns-19.com email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	300s (00:05:00)

Imagen 2.1 se visualiza la dirección IP y el DNS de la aplicación Web.

DNS records

name	class	type	data	time to live
latam1.laboroffice.cl	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
laboroffice.cl	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
laboroffice.cl	IN	NS	ns1.dns-parking.com	86400s (1.00:00:00)
laboroffice.cl	IN	NS	ns2.dns-parking.com	86400s (1.00:00:00)
97.105.175.18.in-addr.arpa	IN	PTR	ec2-18-175-105-97.eu-west-2.compute.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns1-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns2-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns3-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	NS	ns4-24-eu-west-2.ec2-rdns.amazonaws.com	300s (00:05:00)
105.175.18.in-addr.arpa	IN	SOA	server: ns-159.awsdns-19.com email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	300s (00:05:00)

Imagen 2.1 Dirección IP y DNS

2.1. ACCESO AL SERVIDOR

Los clientes/usuarios fundamentalmente clientes de PRGTEC, deben ser capaces de conectarse a este servidor desde cualquier dirección IP. Por medio de cualquier dispositivo habilitado para la web (teléfonos inteligentes, tablet, computador de escritorio, notebook, etc.) los que pueden acceder a la aplicación.

2.2. POSIBLES FUENTES DE ATAQUE

A través de nuestras conversaciones con la contraparte y nuestra comprensión del funcionamiento del sistema, FIBOT ha evaluado la fuente de ataque más probable para la empresa que son los clientes de la empresa, cliente y usuarios de la aplicación. Las fuentes secundarias de ataque pueden ser competidores de PRGTEC. Finalmente, es posible que otros actores no autenticados usen técnicas de escaneo para localizar servidores vulnerables en línea, motivados por diversas razones.

2.3. MOTIVACIÓN

Los atacantes pueden estar motivados por tener acceso a datos no autorizados como información sobre otros clientes o adquirir Propiedad Intelectual de PRGTEC.

2.4. OBJETIVO DEL ATAQUE

En el caso de este estudio, el objetivo de ataque se define como la URL https://latam1.laboroffice.cl/ y potencialmente todo su entorno de red, el que se vería afectado por un ataque.

2.5. PERFIL DE RIESGO | PROBABILIDAD

De acuerdo a reuniones preliminares con el Cliente, se dejó establecido que la información / datos dentro del sistema potencialmente contiene información sensible de los clientes y ha sido calificada como de valor medio-alto comercialmente y, por lo tanto, la probabilidad de ataque se califica como media.

3. PRUEBAS DE PENETRACIÓN

Esta prueba de penetración se realizó mediante el uso de una metodología propia de FIBOT teniendo en consideración estándares propios de la industria, como así también, otras metodologías de carácter libre como OWASP TOP 10, además, de los resultados ofrecidos por diversas herramientas automáticas de tipo escáner.

3.1. NIVELES DE EVALUACIÓN DEL RIESGO

FIBOT utiliza nomenclatura estándar para informar los niveles de evaluación de riesgo de Informacional, Bajo, Medio, Alto o Crítico que se asignan en base a las siguientes definiciones (se realiza una evaluación de la probabilidad de que el riesgo realmente existente no se pueda verificar positivamente mediante pruebas y se incluya en esta evaluación).

Alto

Un problema que, si se explota, tiene el potencial de tener un impacto severo en la confidencialidad, disponibilidad y / o integridad de sus activos de información; el problema puede ser relativamente sencillo de descubrir o la explotación técnica de esto puede ser relativamente trivial.

Medio

Un problema que, si se explota, tiene el potencial para un nivel moderado de impacto en la confidencialidad, disponibilidad y / o integridad de sus activos de información; El descubrimiento del problema puede requerir un nivel razonable de capacidad técnica y también puede ser técnicamente difícil de explotar o requerir un nivel razonable de recursos / tiempo.

Bajo

Un problema que, si se explota, tiene un nivel potencialmente bajo de impacto en la confidencialidad, disponibilidad y / o integridad de sus activos de información; también puede ser técnicamente difícil de explotar en la realidad o requerir una asignación significativa de recursos / tiempo.

Informativo

Como su nombre indica solo entrega información, pero que bien utilizada por los atacantes se pueden conseguir ataques a versiones específicas de software.

3.2. USUARIOS DE PRUEBAS

No se utilizó la cuenta valida de un usuario para realizar las pruebas.

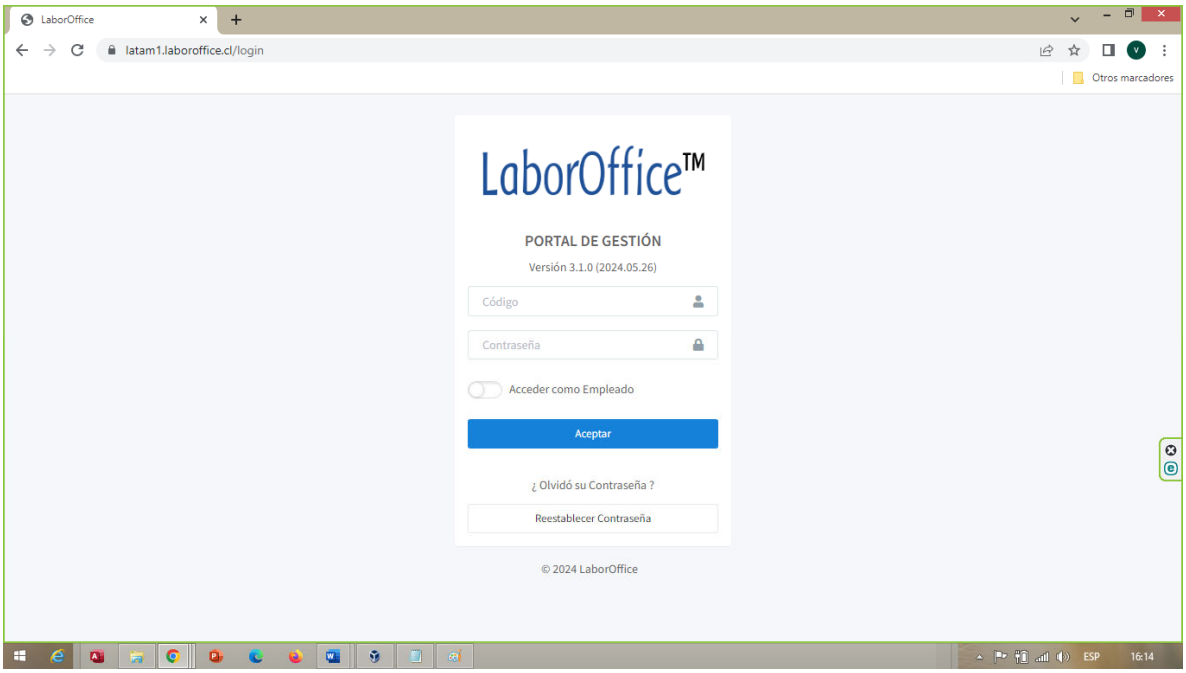
Se realizaron las pruebas tomando como base el que un intruso quisiera comprometer el sistema.

3.3. PRUEBAS OWASP TOP 10

3.3.1. INYECCIÓN

Las aplicaciones basadas en Web que permiten ingresos de información como usuario, contraseña pueden ser susceptibles a los ataques de inyección SQL, lo que permitir a un atacante:

- Ver datos no autorizados.
- Editar datos sin autorización.
- Ejecutar procedimientos almacenados.



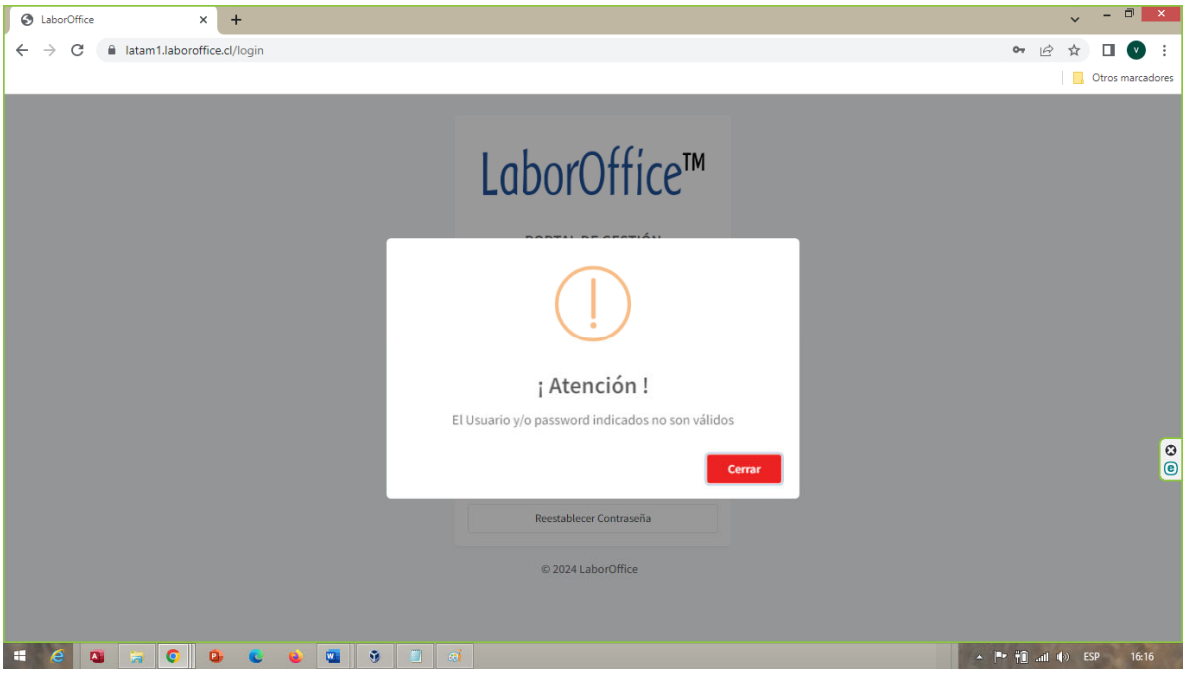
Página de login de la aplicación

Para proporcionar la confianza de que el método de análisis de entrada del usuario adoptado proporciona una protección adecuada contra los ataques de inyección SQL, se seleccionó una muestra de entradas y fue sometido a las entradas SQL comunes, p. "' OR 1 = 1 --" (en una cláusula numérica) o "'or' '='" (en una cláusula alfanumérica). Las versiones canónicas de los metas caracteres también se intentaron cuando correspondía.

Estos ataques están diseñados para devolver errores de los sistemas de backend los cuales son:

- Excepciones de código
- Sentencias SQL
- Errores del sistema operativo
- Demoras en la respuesta
- Respuestas diferenciales

Se examinaron las respuestas del servidor ante un ataque de inyección de SQL obteniendo como resultado que la aplicación no es vulnerable a este tipo de ataque.



Página de login de la aplicación con respuesta de error

3.3.2. QUEBRAR AUTENTICACIÓN Y GESTIÓN DE SESIÓN

El propósito de estas pruebas es para validar los métodos empleados para autenticar un usuario en el sistema. El proceso de autenticación se examinó para identificar los posibles puntos débiles y luego se sometió a los ataques con el fin de evaluar la susceptibilidad a esas debilidades.

ENUMERACIÓN

Durante la enumeración, se analizó el proceso de inicio de sesión de la aplicación para encontrar cualquier información sensible disponible durante la autenticación.

Las credenciales de inicio de sesión (es decir, nombre de usuario y contraseña) se envían junto con los detalles de las sesiones relevantes en un HTTP POST.

Se enumeraron los mecanismos típicamente utilizados para controlar la sesión y fueron probados para determinar su idoneidad.

Se identificaron las siguientes cookies utilizadas por la aplicación laboroffice.cl:

- laboroffice_session
- XSRF-TOKEN

Las pruebas indicaron que las cookies se utilizan como tokens responsables de establecer y mantener sesiones de usuario.

ATAQUES

La información de la fase de enumeración se utilizó para diseñar posibles ataques en el proceso de inicio de sesión. Los ataques empleados fueron:

- Fuerza Bruta

Se empleó el ataque de fuerza bruta en la página de inicio de sesión, este ataque consiste en recuperar la clave intentando con todas las combinaciones (Ej.: "AAAAAAAAAA", "AAAAAAAAAB", "AAAAAAAAAC" - "ZZZZZZZZZZ") hasta encontrar aquella que permite el acceso.

En este caso la aplicación no es susceptible a la realización de un ataque de fuerza bruta, independiente de que sea posible la ejecución de programas externos que realicen pruebas constantes, la aplicación queda a la espera de otra respuesta.

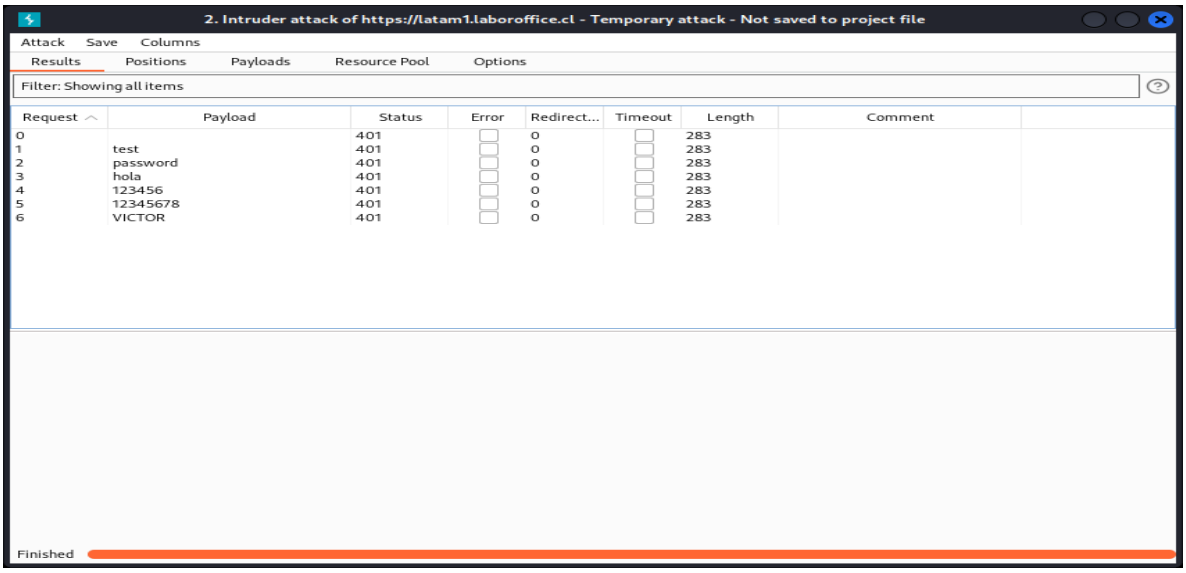


Imagen 0.1 Prueba de usuarios-contraseña

- Enumeración de usuario válido a través de mensajes de error

El inicio de sesión de usuario no permite que los nombres de usuario se determinen a través de mensajes de error, es decir, no es posible determinar si el inicio de sesión se intentó con un nombre de usuario no válido o una contraseña no válida o ambos. como se muestra en la Imagen 3.2.

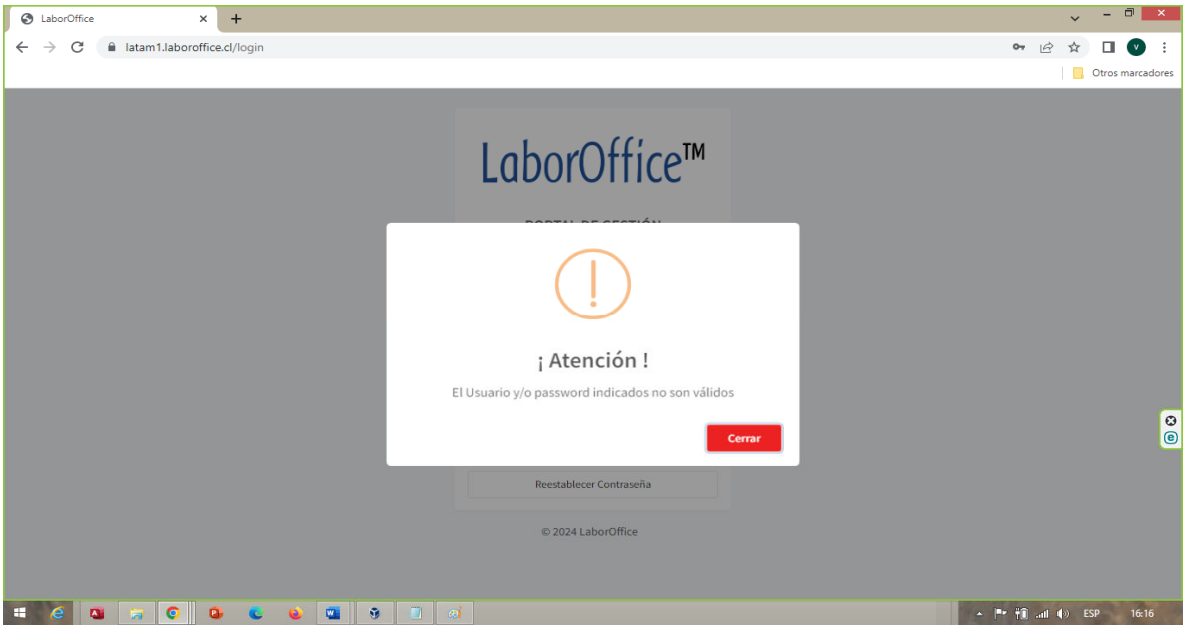


Imagen 0.2 Respuestas de inicio de sesión no válido

- Obtener credenciales de inicio de sesión del navegador web

La mayoría de los navegadores modernos ofrecen almacenar nombres de usuario y contraseñas cuando se ingresan para la conveniencia del usuario. Si la función está habilitada, las credenciales ingresadas por el usuario se almacenan en su computadora local y el navegador las recupera en futuras visitas a la misma aplicación.

Durante las pruebas, los principales navegadores ofrecieron almacenar el nombre de usuario y la contraseña para iniciar sesión en la aplicación de Control de Asistencia LABOROFFICE como lo indica la Imagen 3.3. Esto puede presentar un riesgo si un usuario almacena la contraseña en una máquina no confiable o compartida, por lo que se recomienda instruir a los usuarios para que nunca utilicen esta opción o inhabilitar por código o parámetros esta funcionalidad.

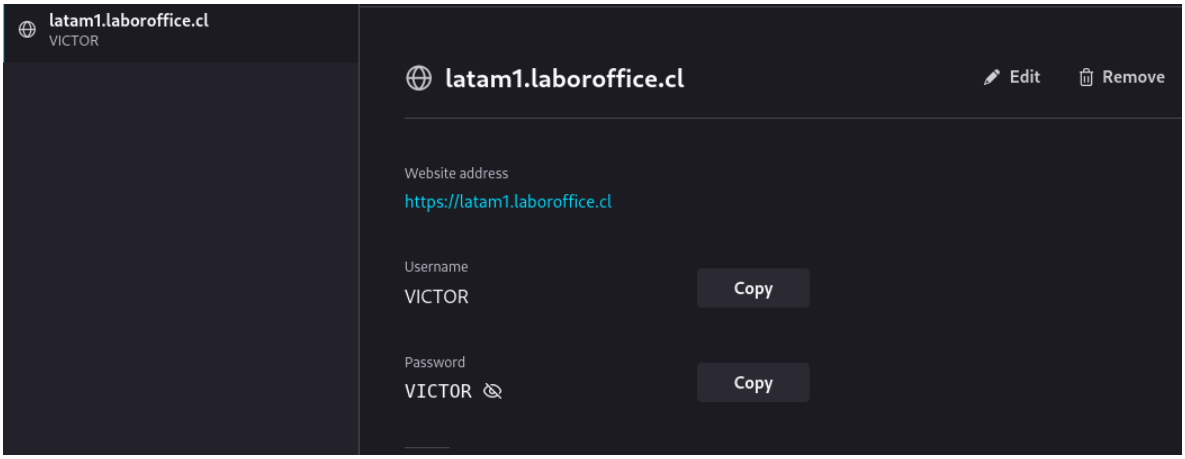


Imagen 0.3 Funcionalidad habilitada

- Credenciales de inicio de sesión con autocompletar

Cuando esta característica está habilitada, las credenciales ingresadas por los usuarios permanecen en la cache de su computadora local y el navegador las recupera en futuras visitas a la misma aplicación. Esto representa un riesgo después de guardada la contraseña en una máquina no confiable o compartida. Solo basta con ingresar el usuario para que el sistema devuelva la contraseña como lo indica la Imagen 0.4. Sin embargo, el uso correcto de algunas características del lenguaje puede evitar esta situación.

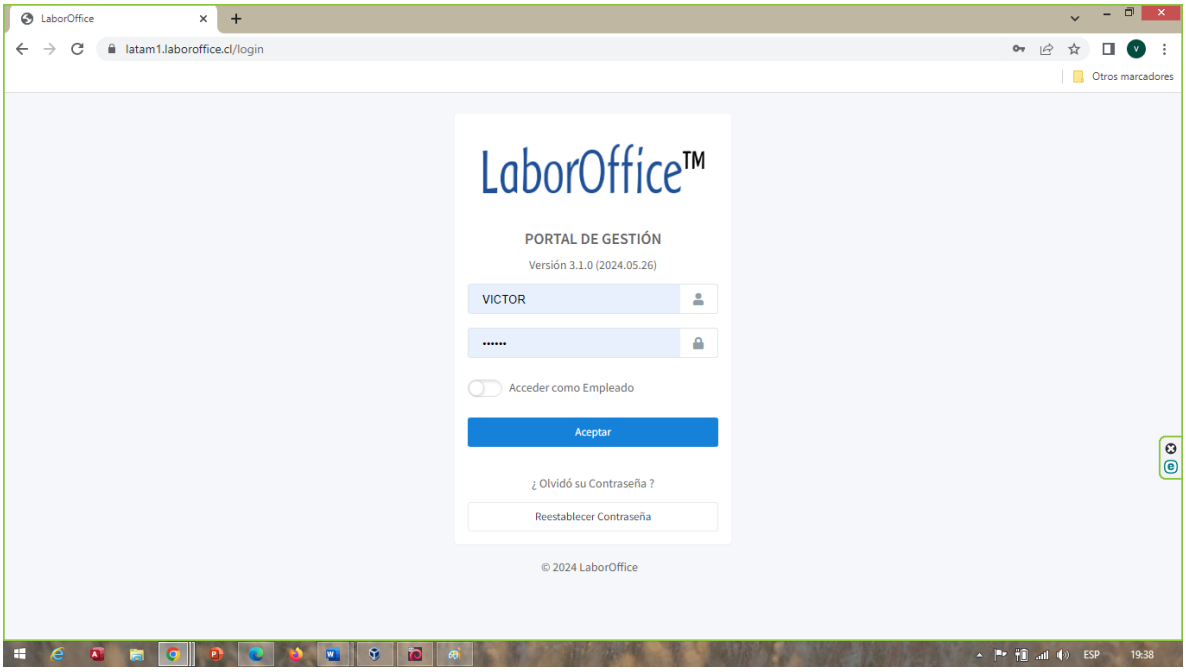


Imagen 0.4 Contraseña con autocompletar habilitado

- Obtener las credenciales de inicio de sesión de tráfico de la red

Los inicios de sesión a la aplicación se proporcionan a través del protocolo cifrado HTTPS. Esto significa que los atacantes no pueden escuchar datos de texto sin cifrar, ni interceptar las credenciales de inicio de sesión.

- Ataque de aproximación de sesión

Se recopilaron muestras de estos identificadores de sesión para evaluar cualquier patrón en su generación. Las muestras se analizaron para patrones obvios en la generación.

El análisis indica que los identificadores de sesión no tienen una mayor aleatoriedad. Razón por la cual un atacante puede determinar el valor de un identificador de sesión válido en un plazo razonable y por lo tanto secuestrar una sesión válida.

En relación a su duración y basado en nuestras pruebas los identificadores de sesión expiran en un período de tiempo razonable.

Se recomienda fortalecer los procedimientos de generación de los identificadores de sesión, para así evitar posibles ataques de aproximación de sesión.

- Repetición de sesiones

Las aplicaciones que no expiran correctamente las sesiones válidas pueden ser susceptibles a la reproducción de entrada de sesión para obtener acceso a la sesión.

Después de cerrar la sesión con la función hecha para esto, se intentó reproducir las solicitudes realizadas durante la sesión. Estas solicitudes fueron procesadas sin éxito por el servidor, y sobre esta base, se concluye que la sesión se destruye adecuadamente en el lado del servidor y, por lo tanto, no es posible reproducir el inicio de sesión / sesión.

Sin embargo, si se cierra la pestaña del navegador y posteriormente se vuelve a cargar la URL, esta retoma la sesión dejada anteriormente, lo mismo sucede si se decide navegar hacia adelante o hacia atrás y se vuelve a la aplicación, está retoma la sesión sin inconvenientes.

Se recomienda revisar todo lo que involucre un cierre de sesión con todas las posibles alternativas que entrega una navegación.

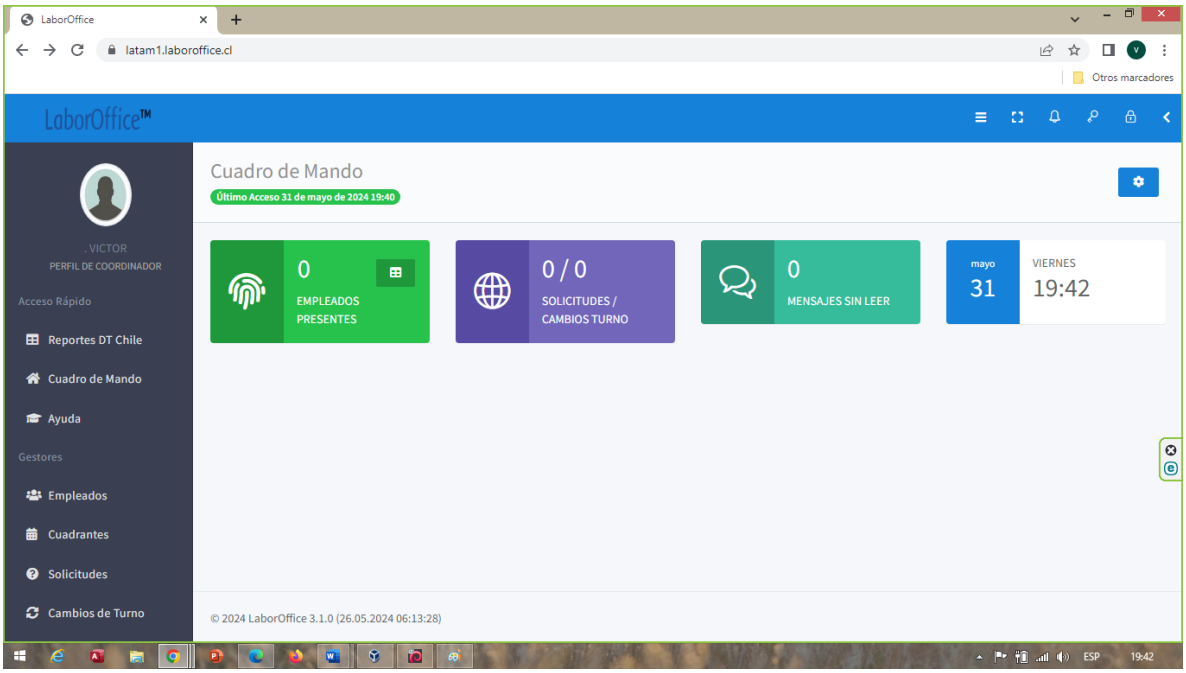


Imagen 0.5 Repetición de Sesiones

- Fijación de sesión

Cualquier identificador de sesión que se establezca antes de que el usuario se autentique y no cambia durante la sesión podría exponer la aplicación a un ataque de fijación de sesión.

Con respecto al inicio de sesión en este caso, no se detectó que las cookies utilizadas en el manejo de la sesión se configuraran antes del inicio de sesión, y por lo tanto un atacante no autenticado no podría recuperar una cookie sin consolidar antes de la autenticación.

- Interceptación de identificador de sesión

Todo el tráfico se envía a través del protocolo cifrado HTTPS. Esto significa que tanto antes como después de la autenticación exitosa, un atacante con acceso al tráfico de red o a dispositivos como un servidor proxy no podría usar el identificador de sesión para secuestrar sesiones de usuario activas. Esto está en consonancia con las buenas prácticas de seguridad.

Además de usar conexiones cifradas, se recomienda el uso de ciertas configuraciones:

- Secuestro de sesión

La sesión se basa en las cookies devueltas desde el navegador a través de solicitudes. Las pruebas indican que es posible tener sesiones simultáneas bajo la misma cuenta de usuario. Si un ataque como Cross-Site Scripting tuviera éxito, un atacante podría interceptar la sesión sin ser detectado. Recomendamos no permitir el inicio de sesión simultáneo para ayudar a prevenir el secuestro de la sesión en el caso de Cross-Site Scripting u otro ataque de robo de sesión.

3.3.3. ENTIDADES EXTERNAS XML (XXE)

En sistemas modernos y la llegada de nuevas tecnologías, siempre es posible ir agregando nuevas y mejores funcionalidades a los mismos, pero también involucra agregar nuevas vulnerabilidades. Así por ejemplo la tecnología XML provee nuevas características a los servicios Web, sin embargo, los atacantes pueden explotar las vulnerabilidades que le permitan subir archivos XML con contenido hostil.

Para el caso de la aplicación **LaborOffice**, no se pudo detectar el uso de esta tecnología en el desarrollo de la aplicación.

3.3.4. QUEBRAR CONTROL DE ACCESO

Cuando las restricciones de lo que pueden hacer los usuarios autenticados no se aplican correctamente, los atacantes pueden acceder a funcionalidades y/o datos no autorizados, acceder a otras cuentas de usuarios, ver archivos confidenciales, modificar datos de otros usuarios, cambiar derechos de acceso, etc.

- *Referencias inseguras a objetos directos*

Una referencia de objeto directa ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, como un archivo, directorio, registro de base de datos o clave, como una URL o parámetro de formulario. Un atacante puede manipular referencias directas de objetos para acceder a otros objetos sin autorización, a menos que haya una verificación de control de acceso en su lugar.

En nuestras pruebas, la funcionalidad de autenticación / autorización de la aplicación impide que un usuario obtenga acceso a los datos o registros de otro usuario modificando el valor clave que identifica los datos.

3.3.5. CONFIGURACIÓN DE SEGURIDAD INCORRECTA

Una aplicación Web requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, bases de datos y plataforma. Todas estas configuraciones deben ser definidas, implementadas y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código hechas para la aplicación.

3.3.6. DESERIALIZACIÓN INSEGURA

La deserialización insegura es una vulnerabilidad que se produce cuando se usan datos no confiables que controla el atacante permitiendo infringir un ataque de denegación de servicio (DoS), desvíos de autenticación y ataques de ejecución remota de código.

Las pruebas realizadas sobre la aplicación no mostraron que tuviera problemas de este tipo.

3.3.7. USO DE COMPONENTES CON VULNERABILIDADES CONOCIDAS

Los componentes, como librerías, frameworks y otros módulos de software, se ejecutan con los mismos privilegios que la aplicación. Si un componente es vulnerable y explotado, un ataque puede facilitar una pérdida seria de información o incluso la pérdida de control de un servidor. Las aplicaciones y APIs utilizan componentes con vulnerabilidades conocidas que pueden debilitar la defensa de una aplicación y permitir varios ataques e impactos.

- *Utilización de componentes desactualizados*

Todos los componentes deben estar actualizados a las configuraciones y versiones de seguridad adecuadas. Algunos scripts de terceros pueden contener vulnerabilidades de seguridad conocidas que son fácilmente identificadas y explotadas por atacantes.

En el caso particular de esta aplicación, no se han detectado componentes desactualizados y que contengan vulnerabilidades conocidas que puedan ser explotadas por terceros

3.3.8. MONITOREO Y REGISTRO INSUFICIENTE

La vulnerabilidad de registro y monitoreo insuficiente se produce cuando los eventos críticos para la seguridad no se registran correctamente y el sistema no está supervisando los acontecimientos actuales. Sin lugar a dudas, la falta de estas funcionalidades puede hacer que las actividades maliciosas sean más difíciles de detectar y afecta el manejo efectivo de incidentes cuando ocurre un ataque.

Durante las pruebas realizadas se identificó que la aplicación cuenta con un sistema de auditoría que va registrando las actividades que realizan los usuarios correctamente autenticados en ella.

Por otra parte, mientras se realizaba este análisis no se recibió ningún tipo de retroalimentación con respecto a las múltiples pruebas que se realizaron sobre la aplicación, normalmente este tipo de monitoreo está a cargo de empresas externas que deben reportar cualquier tipo de actividad extraña, ya que esto puede ser un indicativo de algún tipo de ataque en proceso.

3.3.8. PUERTOS ABIERTOS

El servidor solo está utilizando solo los puertos estrictamente necesarios para cumplir con su función.

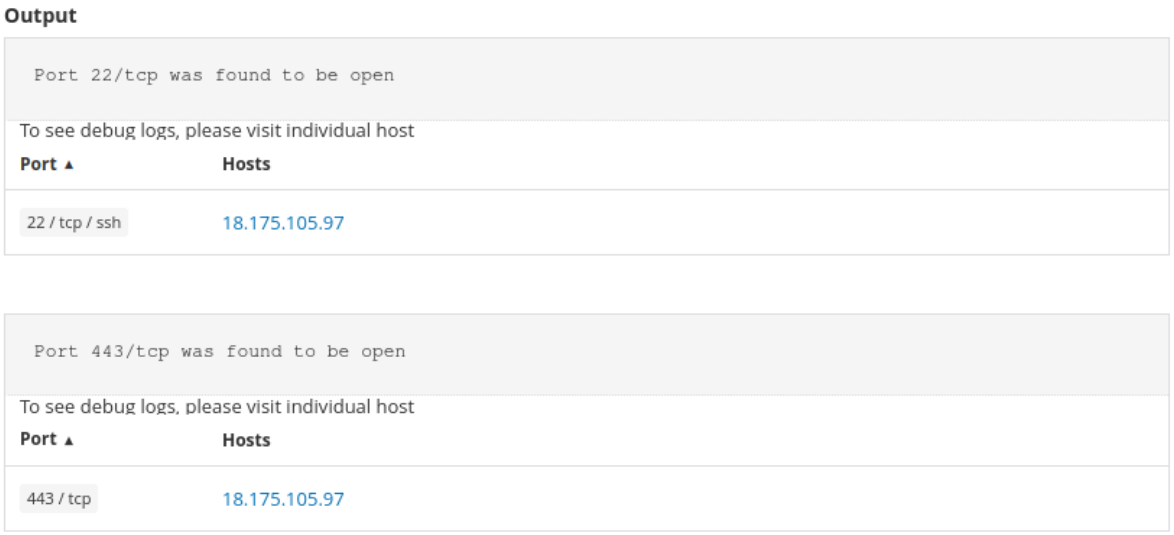


Imagen 3.3.8 Puertos abiertos

3.4. RESULTADOS OBTENIDOS

Una vez efectuadas las pruebas se identificaron 1 vulnerabilidades de riesgos medios y 4 vulnerabilidades de tipo de riesgo informacional. En la Tabla 3.4.1 se especifican las vulnerabilidades encontradas y se clasifican de acuerdo al riesgo que estás representa.

Tabla 3.4.1 Vulnerabilidad por clasificación de riesgo

Vulnerabilidades contabilizadas por clasificación de riesgo			
Hallazgos	Medio	Bajo	Info
Puertos abiertos			1

4. PRUEBAS NO REALIZADAS

Ciertas pruebas de riesgo o potencialmente perturbadores no se llevaron a cabo, en concreto:

- Denegación de servicio, inundación o ataques tipo "bombardeo".
- Ataques de tipo de manipulación del protocolo TCP, RIP y ARP (incluido el análisis de fragmentación). Es muy probable que estos tipos de ataques causen interrupciones en las aplicaciones.
- Intentos de inicio de sesión de fuerza bruta (excepto en cuentas designadas) y ataques de compromiso de cuenta. Esto puede llevar a que las cuentas de usuario se bloqueen y, por lo tanto, pueden funcionar eficazmente como un ataque de denegación de servicio.

5. POLÍTICAS DE SEGURIDAD

Esta sección aborda problemas que no son específicamente técnicos, pero que sin embargo podría causar que la aplicación sea vulnerable a un atacante.

5.1. CALIDAD DE LA CONTRASEÑA

Si los requisitos de complejidad de contraseñas de la aplicación son demasiado bajos. Puede que sea posible, la adivinación de contraseñas o llevar a cabo un ataque de fuerza bruta sobre ellas.

Las contraseñas deben tener al menos 8 caracteres de longitud e idealmente deberían estar obligados a contener una mezcla de letras mayúsculas, letras minúsculas, números y caracteres especiales.

5.2. BLOQUEO DE CUENTAS

De acuerdo con las con las buenas prácticas de seguridad, las cuentas deben bloquearse después de un número razonable de intentos con contraseña incorrecta.

6. CONCLUSIONES Y RECOMENDACIONES

Hecha las pruebas de Penetración o Ethical Hacking, sobre la aplicación de LaborOffice podemos concluir que:

- La aplicación no presenta vulnerabilidades críticas que comprometan su seguridad en lo inmediato.
- Las medidas de contingencia y seguridad tomadas para LaborOffice aseguran la protección en ataques de alto riesgo y cumplen con las exigencias de la Dirección del Trabajo para su certificación.

Recomendaciones

- Se recomienda evaluar a futuro:
  1. La implementación de sistemas de monitoreo ante intrusiones no deseadas.
  2. Repetición anual de pruebas de Ethical hacking para mantener los estándares actuales de seguridad.

Víctor Hernández M.
Técnico de Nivel Superior en Informática
Profesional Certificador