



Bogotá, D.C, 19 de marzo de 2020.

Señores:

**PAR SERVICIOS**

Asunto: **Informe de Resultados Re Test Ethical Hacking – Caja Blanca**

Cordial saludo.

En el presente documento encontrará el **Informe de Resultados del Re Test Ethical Hacking – Caja blanca** realizado a un sitio web con acceso por medio de las siguientes url's:

- <https://app.mproveedor.com/Par/public>
- <https://app.mproveedor.com/GrupoTransporte/public/login>

Quedo atento a cualquier duda o inquietud que tengan respecto a la información contenida en el presente documento.

Cordialmente,

**LUIS ALEJANDRO SAINEA ROJAS**

Ingeniero de Sistemas – Especialista en Ingeniería de Software, ACE y CEH.

# Informe de Resultados del Re Test Ethical Hacking – Caja blanca

BEH0012020



BOGOTA MARZO 2020

CONFIDENCIAL

# APARTADO DE CONFIDENCIALIDAD

La privacidad y confidencialidad de la información son la base más importante de este reporte, es por ello que el contenido de este documento se clasifica con el carácter de confidencial aplicándole esta definición a todo tipo de medio y de tipo de información, protegiéndose además a todo lo que se involucre con la propiedad intelectual. Este documento solo debe ser utilizado para los fines pertinentes establecidos con el cliente.

En caso de que se lleve a cabo alguna violación de la privacidad y confidencialidad de la información, se aplicarán las sanciones y penas a que hay lugar en la ley Colombiana.

El presente documento cuenta con carácter confidencial de secreto profesional y/o “know how”. El cliente utilizará todos los medios que estén a su alcance para hacer extensiva la presente disposición a todas aquellas personas que de una u otra forma tengan conocimiento de la información aquí contenida.

*Todos los derechos reservados. Esta publicación no puede ser reproducida total ni parcialmente, ni registrada o transmitida por un sistema de recuperación de información, en ninguna forma ni por ningún medio, sea mecánico, fotoquímico, electrónico, magnético, electro-óptico, fotostático o por cualquier otro, sin el permiso previo escrito de **BITTIN S.A.S.***

**BITTIN S.A.S. Derechos reservados.**

## Tabla de Contenido

1. Introducción .....	5
2. Objetivos .....	5
3. Descripción de las pruebas .....	5
4. Glosario .....	6
5. Desarrollo de actividades.....	8
5.1 Definición de escenarios y objetivos .....	8
5.2 Escenario.....	8
5.3 Técnicas de Comprobación.....	8
5.4 URL's objetivos .....	9
5.5 Listado de Objetivos.....	9
5.6 Plataforma de Par Servicios – Resumen verificación vulnerabilidades.....	9
5.7 Detalle verificación vulnerabilidades .....	10
6. Scan de Vulnerabilidades adicionales.....	23
7. Plataforma de Par Servicios – Fortalezas.....	23
8. Conclusiones .....	24
Conclusión General .....	24
Conclusiones complementarias .....	24
9. Anexos.....	24

# GENERALIDADES

## 1. Introducción

El presente documento tiene por objeto demostrar las actividades ejecutadas y los resultados obtenidos durante las pruebas de Re Test del Ethical Hacking – Caja blanca que fue desarrollado en el mes de enero de 2020 para la empresa PAR SERVICIOS.

## 2. Objetivos

- Validar las actividades de remediación realizadas por el equipo de tecnología de Par Servicios, sobre las vulnerabilidades reportadas en el informe de Ethical Hacking entregado el día 28 de Enero de 2020.
- Exponer las vulnerabilidades persistentes y las nuevas si es el caso.

## 3. Descripción de las pruebas

Este tipo de pruebas busca determinar aquellas vulnerabilidades que pueden aun persistir en la aplicación después de las actividades de remediación realizadas por el equipo de tecnología de Par Servicios. La metodología de análisis incluye principalmente los siguientes aspectos:

- Re Test de vulnerabilidades
- Escaneo e identificación de puertos

## 4. Glosario

- **Ataque:** Acción realizada por una tercera parte, distinta del emisor y del receptor de la información protegida, para intentar contrarrestar esta protección.
- **Certificado digital:** Archivo con carácter de documento emitido por una autoridad de certificación que asocia una entidad con una clave pública. Garantiza la confidencialidad de la comunicación llevada a cabo entre la misma y los usuarios. Es utilizado, entre otras cosas, en los sitios web que utilizan el protocolo HTTPS.
- **Cifrado:** Transformación de un texto en claro, mediante un algoritmo que tiene como parámetro una clave, en un texto cifrado no legible para quien no conozca la clave de descifrado.
- **Descifrado/ Desencriptar:** Transformación inversa al cifrado para obtener el texto en claro a partir del texto cifrado y la clave de descifrado.
- **DNS:** Sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o una red privada, del inglés Domain Name System.
- **Exploit:** (Del inglés to exploit, 'explotar' o 'aprovechar') Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
- **Firewall:** Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.
- **FTP File Transfer Protocol.** Protocolo de transferencia de archivos. Por medio de programas que usan este protocolo, se permite la conexión entre dos computadoras y se pueden cargar y descargar archivos entre el cliente y el host (servidor).
- **Hacker:** Persona apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".
- **Hacking ético:** es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y

encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

- **Host:** Se refiere a cada una de las computadoras conectadas a una red que proveen o utilizan servicios de ella.
- **HTTP:** Es el protocolo utilizado en cada transacción de la World Wide Web, del inglés Hyper Text Transfer Protocol.
- **HTML:** (del inglés Hyper Text Markup Language, lenguaje de marcas de hipertexto) es el lenguaje de programación en el que se escriben las páginas Web.
- **IP:** Es un protocolo no orientado a conexión, usado por el origen y el destino para comunicación de datos a través de una red de paquetes conmutados, del inglés "Internet Protocol".
- **Intrusiones:** Penetraciones que se hacen en los sistemas sin permisos o derechos.
- **Log:** Registro de eventos que se producen durante un rango de tiempo en particular.
- **Malware:** Tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento del propietario.
- **Parche:** Cambios que se aplican a un problema para solucionar errores o actualizaciones.
- **Parche de seguridad:** Actualización que se aplica a un software para resolver vulnerabilidades. Por lo general, no modifica la funcionalidad, sino que corrige problemas de seguridad.
- **Payload:** Se refiere a los efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos secundarios de dicha infección (cambios en la configuración).
- **SSL:** Acrónimo en inglés de Secure Socket Layer. Protocolo creado por Netscape con el fin de hacer posible la transmisión encriptada y por ende segura, de información a través de la red donde sólo el servidor y el cliente podrán entender un determinado texto.
- **Vulnerabilidad:** Hace referencia a cualquier fallo en una determinada aplicación

## 5. Desarrollo de actividades

### 5.1 Definición de escenarios y objetivos

Se realizan las pruebas de ReTest de Hacking ético Caja blanca, tomando como base el listado de vulnerabilidades reportadas en el informe de Ethical Hacking entregado el día 28 de Enero de 2020 sobre la aplicación web. Se realizará un análisis de vulnerabilidades web para la plataforma que tiene como punto de acceso las siguientes url's:

- <https://app.mproveedor.com/Par/public>
- <https://app.mproveedor.com/GrupoTransporte/public/login>

Para las pruebas de intruso interno, se ejecutarán pruebas desde dos perfiles que intervienen en la plataforma con los siguientes privilegios:

#### **Plataforma Producción**

- Root
- Estandar
- Proveedor

#### **Plataforma Clientes**

- Todos los permisos Activos
- Usuario Limitado

### 5.2 Escenario

El consultor se encuentra ubicado fuera de las instalaciones de PAR SERVICIOS, ya que la aplicación esta expuesta a internet y las pruebas se pueden realizar de forma remota. Se utilizaron herramientas para el Hacking ético en distintas plataformas: Windows y Linux.

### 5.3 Técnicas de Comprobación

Para el ejercicio de re test realizado sobre la aplicación de PAR SERVICIOS, se utilizan las siguientes técnicas de análisis:

- Inspecciones y Revisiones Manuales



- Modelado de Amenazas
- Pruebas de Intrusión

## 5.4 URL's objetivos

Tipo	URL
URL aplicación Web	https://app.miproveedor.com/Par/public
	https://app.miproveedor.com/GrupoTransporte/public/login

## 5.5 Listado de Objetivos

DIRECCION IP IDENTIFICADA PRUEBAS RETEST	
IP	Nombre Servidor
3.17.38.98	amazonaws

3.17.38.98

FIND









IP address	3.17.38.98
Latitude	39.9653
Longitude	-83.0235
Country	United States
Region	Ohio
City	Columbus
Organization	Amazon.com

Gráfico 1. Dirección IP.

El servidor en el cual se encuentra desplegada la aplicación de **PAR SERVICIOS** esta soportado por un sistema operativo Linux, servidor de aplicaciones Apache 2.4.6 y lenguaje de programación PHP 7.0.33.

## 5.6 Plataforma de Par Servicios – Resumen verificación vulnerabilidades

El resumen de las pruebas de ReTest ejecutado sobre las 8 vulnerabilidades reportadas en el ejercicio Inicial, se presenta a continuación:

ID	Vulnerabilidad	Criticidad	Resultado RETEST
1	File upload		Corregido
2	Visibilidad servidor		Corregido
3	Login page password-guessing attack		Corregido
4	Failure to Restrict URL Access		Corregido
5	Password field with auto-complete		Corregido
6	Missing 'Strict-Transport-Security' header		Corregido
7	PHP version without support		Corregido
8	Cross-site Scripting en sitios web (parcial)		Corregido

**Tabla 2.** Resumen ReTest Vulnerabilidades identificadas en el Análisis aplicación Par Servicios

## 5.7 Detalle verificación vulnerabilidades

Se presenta el detalle de las verificaciones realizadas sobre las 8 vulnerabilidades existentes:

### 5.7.1 File upload

- **Descripción:** Para la validación se utiliza la imagen **papaNoel.php.jpg** del ejercicio inicial, al que se inyecto un código malicioso php.

Creamos un nuevo cliente en la plataforma <https://app.mproveedor.com/Par/public> por medio de la opción inscripción y le adjuntamos la imagen infectada:

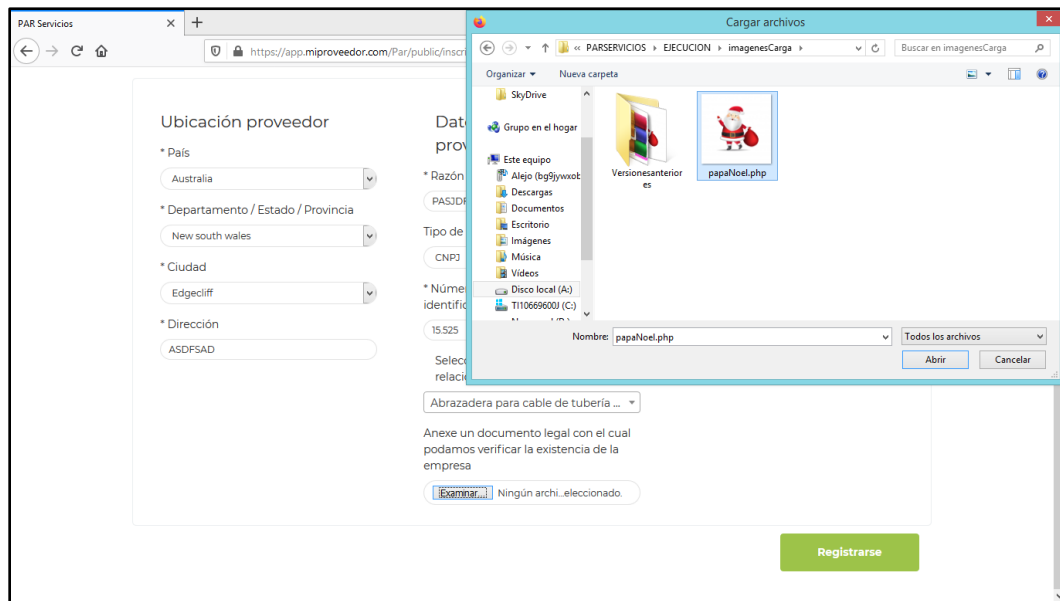


Gráfico 2. Se realiza una nueva inscripción.

Se observa que el sistema no permite crear el cliente y almacenar la imagen en la aplicación ya que tiene el control sobre la extensión.

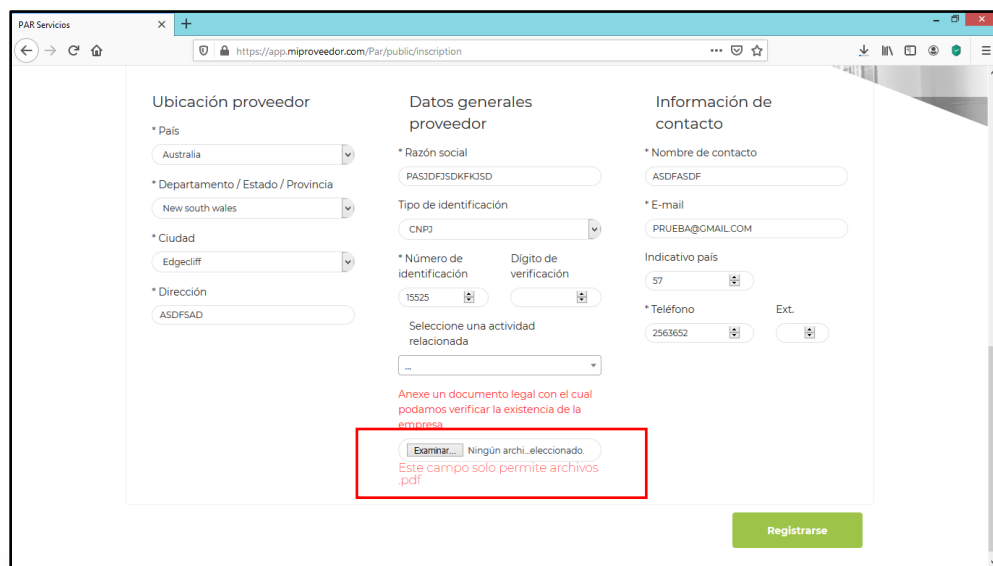


Gráfico 3. Se observa el control de archivos con extensión no permitida.

Se realiza un escenario adicional por medio de la opción de carga de archivos para un perfil de usuario proveedor ya autenticado en la aplicación y utilizando el archivo **infprueba.pdf** de las pruebas iniciales, el cual se encuentra infectado con un Payload:

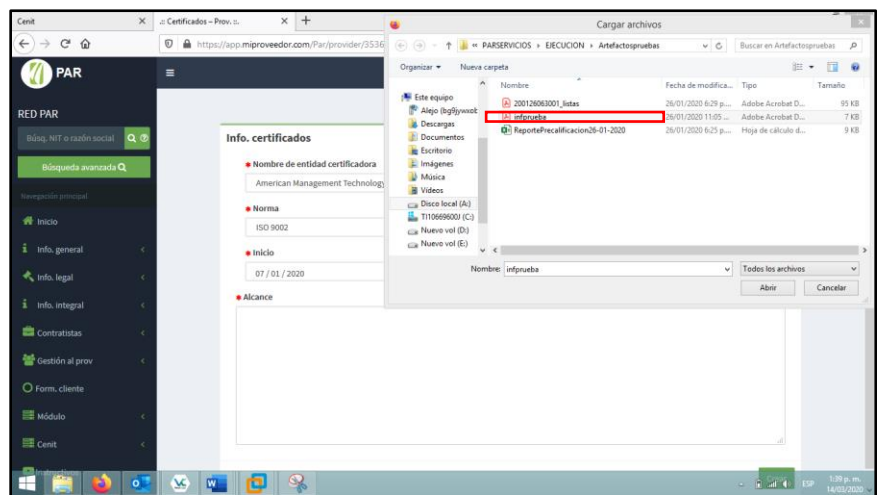


Gráfico 4. Se crea un nuevo certificado

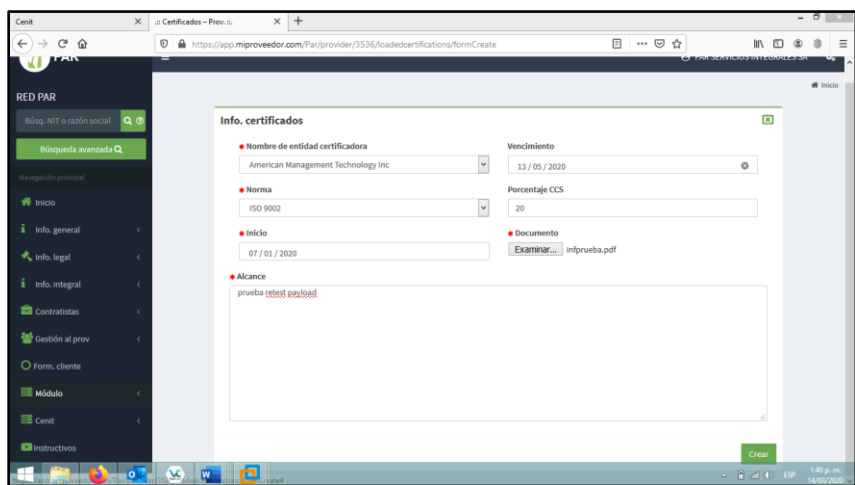


Gráfico 5. Se crea un nuevo certificado

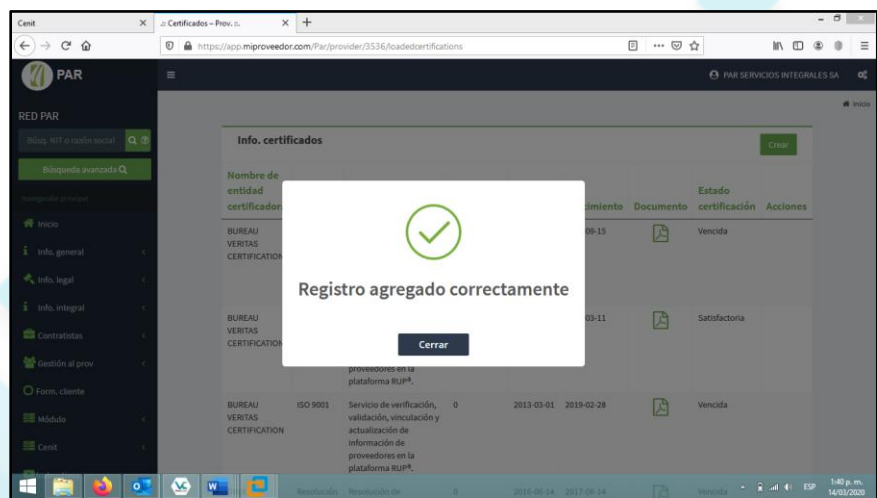


Gráfico 6. Se crea el certificado exitosamente.

Se observa que la aplicación permite la carga del archivo infectado.

La implementación en este momento de un control en la aplicación que permita detectar archivos PDF infectados al momento de la carga, presenta una restricción técnica relevante que impide el ajuste. Sin embargo, la compañía implementó como medida alterna para mitigar la vulnerabilidad, un apartado en los términos y condiciones de la aplicación por medio de la cual notifica al usuario de las siguientes prácticas para la descarga y apertura de los archivos PDF de la aplicación:

- Utilizar lectores de PDF con soporte tales como Adobe Acrobat reader
- Deshabilitar el Acrobat JavaScript y la ejecución automática de url's en las opciones de administración del lector de PDF si este lo permite.
- Mantener actualizado a su última versión los programas lectores de PDF y navegadores web
- Mantener actualizado el antivirus del equipo.
- Realizar una configuración adecuada del Firewall para bloquear la ejecución de links externos sospechosos desde los equipos de la organización.

En las siguientes imágenes se evidencia la implementación de esta medida alterna:

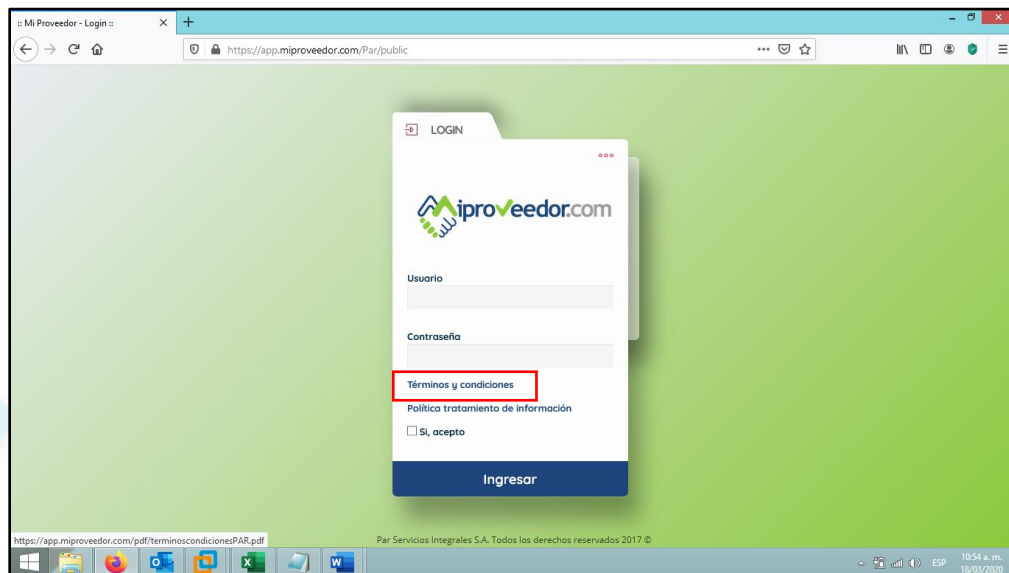


Gráfico 7. Se crea el certificado exitosamente.

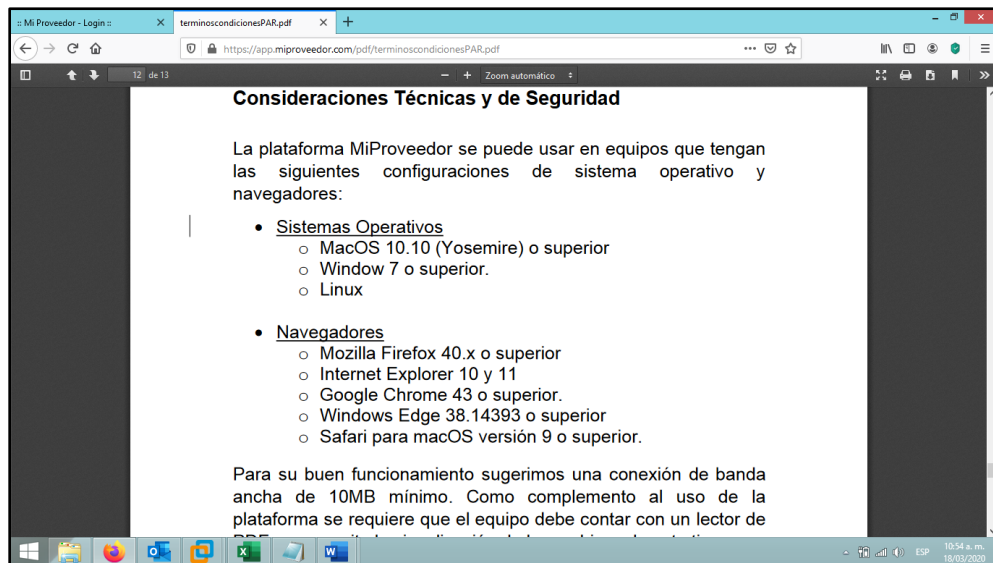


Gráfico 8. Sección con las recomendaciones técnicas y de seguridad.

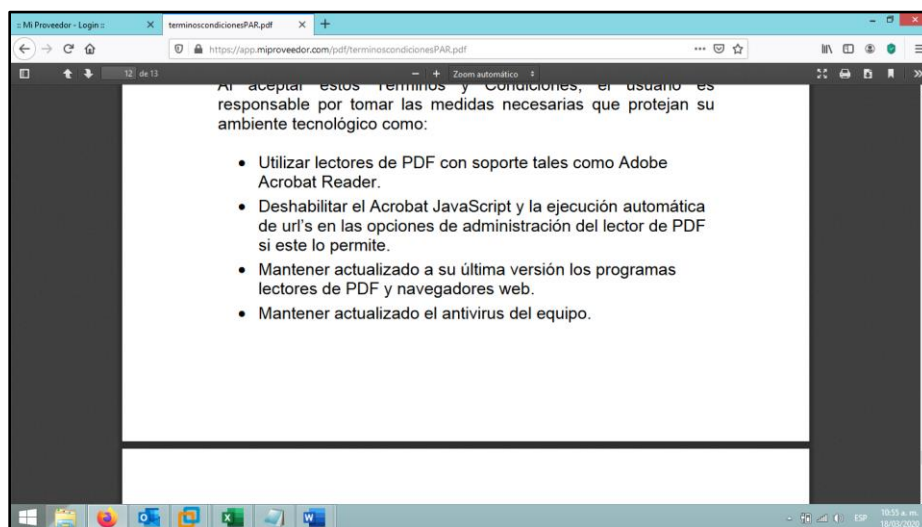


Gráfico 9. Recomendaciones agregadas.



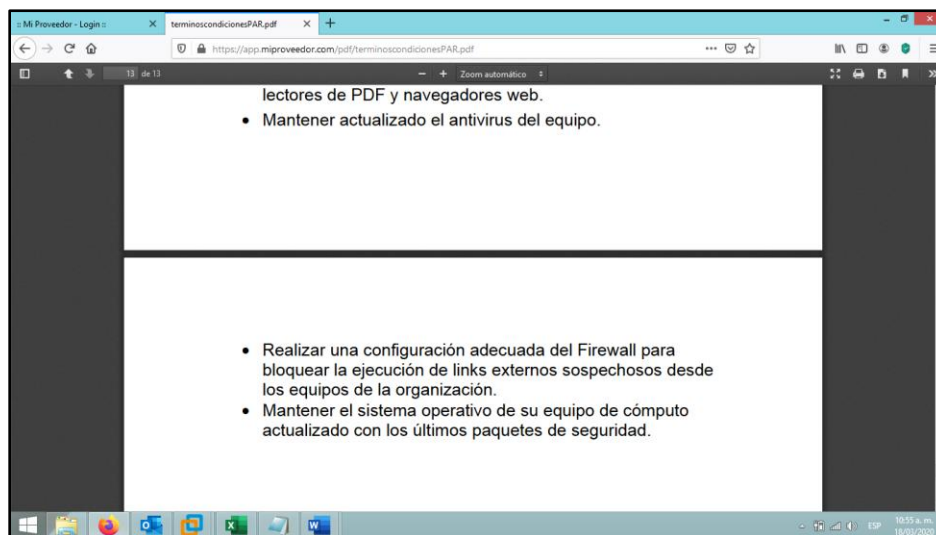


Gráfico 10. Recomendaciones agregadas.

## 5.7.2 Visibilidad servidor

- **Descripción:** La fase de reconocimiento del objetivo se realizó en dos escenarios, el primero realizando un escaneo desde una dirección IP no autorizada por el proveedor de hosting y un segundo escenario con la dirección IP autorizada.

A continuación, se presenta el resultado del nivel de visibilidad del servidor del ejercicio inicial:

PUERTOS IDENTIFICADOS EJERCICIO INICIAL					
SIN AUTORIZACIÓN			AUTORIZADA		
PORT	STATE	SERVICE	PORT	STATE	SERVICE
21	open	ftp vsftpd 2.0.8	22	open	ssh OpenSSH 7.4 (protocol 2.0)
443	open	ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33)	443	open	ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33)
80	open	http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33)	80	open	http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33)
8008	open	http	21	open	ftp vsftpd 2.0.8
2000	open	cisco-sccp?			
5060	open	Sip?			

Tabla 3. Resultado de Escaneo de reconocimiento

En la siguiente tabla se presentan los resultados del scan de retest:

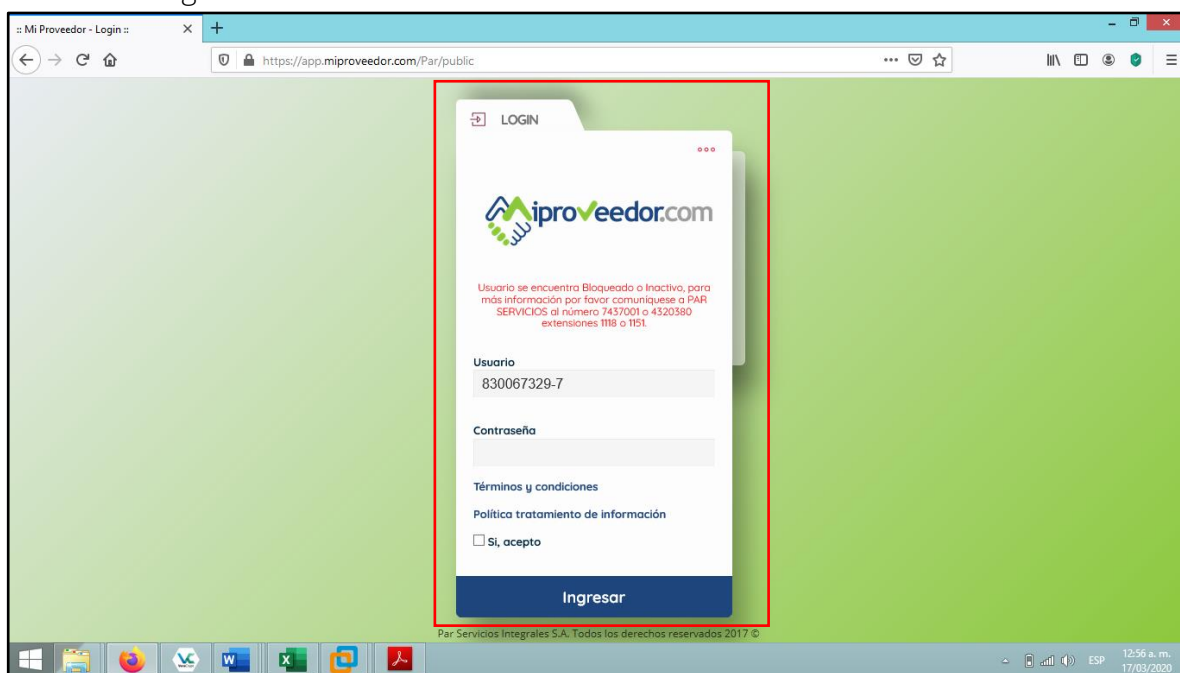
PUERTOS IDENTIFICADOS EJERCICIO RE TEST					
SIN AUTORIZACIÓN			AUTORIZADA		
PORT	STATE	SERVICE	PORT	STATE	SERVICE
25	open	smtp?	22	open	ssh OpenSSH 7.4 (protocol 2.0)
443	open	ssl/http Apache httpd	443	open	ssl/http Apache httpd
80	open	http Apache	80	open	http Apache httpd
			21	open	ftp vsftpd 2.0.8

**Tabla 4.** Resultado de Escaneo de reconocimiento – re test

Se evidencia la implementación de controles de visibilidad sobre los puertos del servidor, principalmente para aquellos scan desde IP's no autorizadas reduciendo la información técnica expuesta.

### 5.7.3 Login page password-guessing attack

- **Descripción:** Se realizaron 10 pruebas manuales de ingreso de password errado sobre las dos URL's de la aplicación, identificando que para la URL <https://app.miproveedor.com/Par/public>, se implementó un control de bloqueo de usuario al realizar múltiples ingresos fallidos como se muestra en la siguiente imagen:



**Gráfico 11.** Bloqueo usuario por ingresos fallidos.

Al realizar el mismo escenario para la URL <https://app.miproveedor.com/GrupoTransporte/public/login>, se encontró que se implementó un control de bloqueo de usuario al realizar los múltiples ingresos fallidos como se muestra en la siguiente imagen:



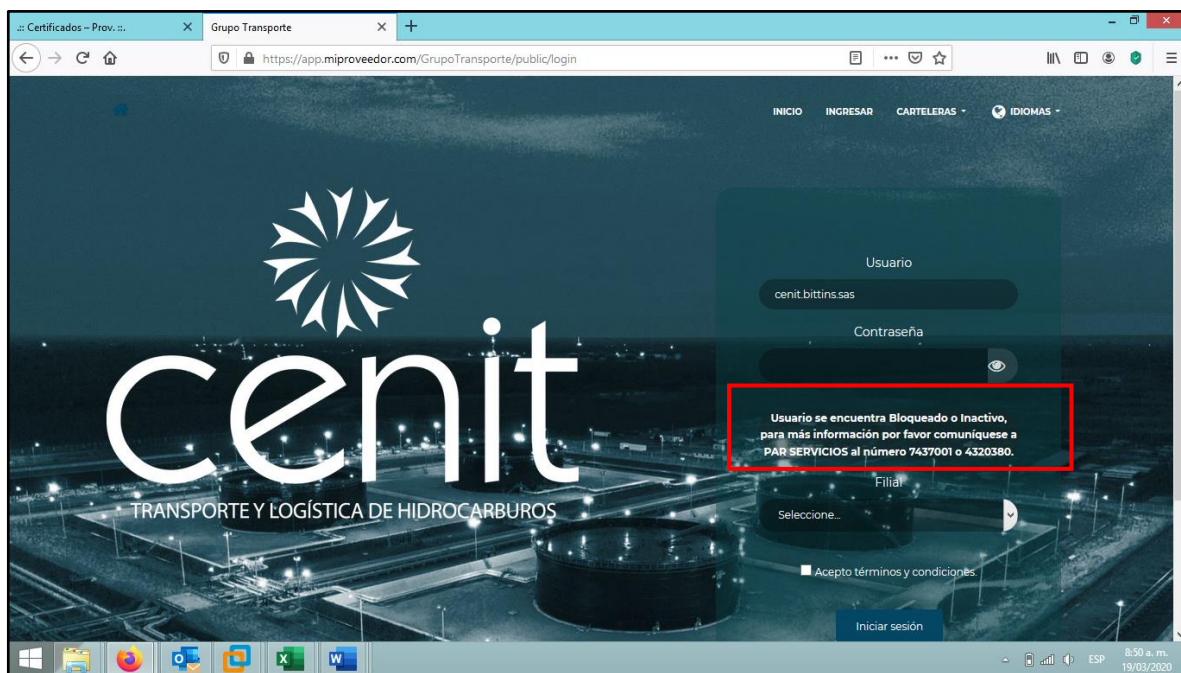
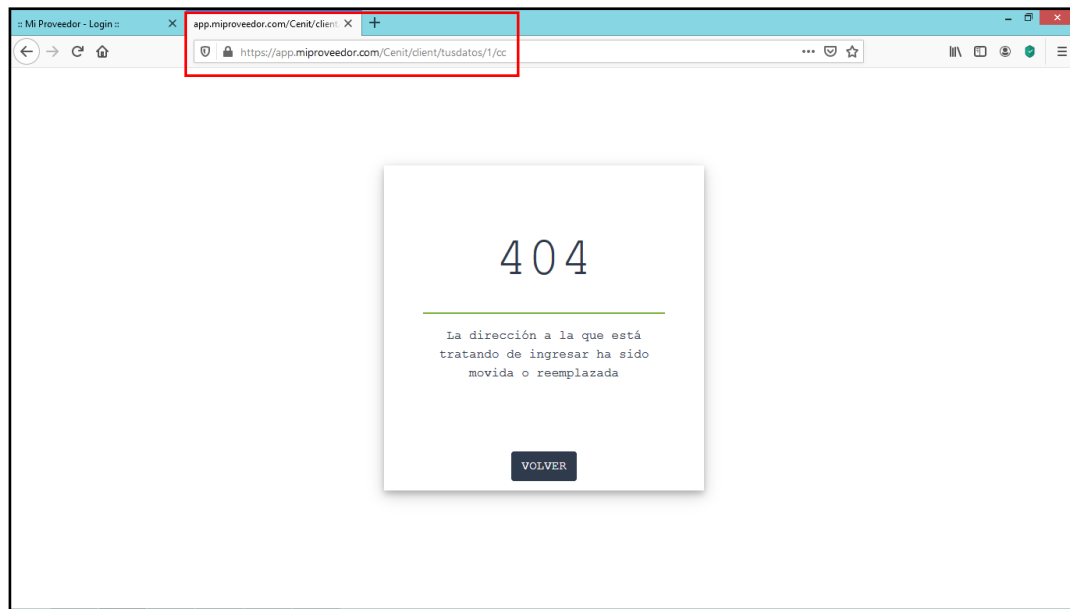


Gráfico12. Se realizan 10 intentos fallidos de password.

- **Recomendación:** Se sugiere complementar el control agregando un mensaje con el número de intentos faltantes para que el usuario sea bloqueado

#### 5.7.4 Failure to Restrict URL Access

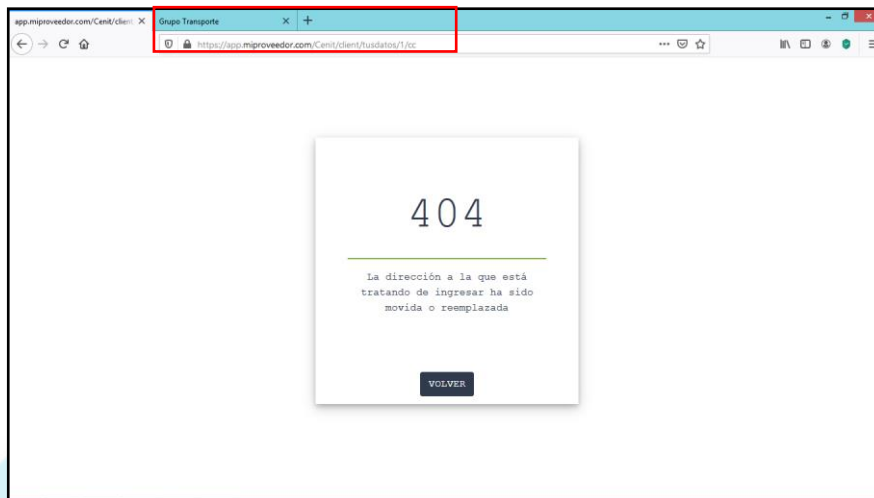
- **Descripción:** Se realiza el re test en la aplicación <https://app.mproveedor.com/Par/public> con el usuario estándar bit.luis.sainea, validando si es posible acceder a la página Cenit/client/tusdatos/1/cc que es de acceso restringido para el perfil cenit.bittins.sas:



**Gráfico 13.** Se presenta la restricción de acceso a la sección restringida para ese perfil.

Se observa que la aplicación presenta el control de acceso a la pantalla.

Se realiza la validación del escenario en el que se retorna la pantalla de error con la información técnica de la aplicación. Para esto se utiliza el usuario proveedor 830067329-7 como se muestra a continuación:



**Gráfico 14.** Se restringe el acceso a la pantalla con el error técnico.

Se observa que la aplicación presenta el control que ya no permite visualizar la pantalla con el error técnico.

### 5.7.5 Password field with auto-complete

- **Descripción:** Tomando como base que la funcionalidad del administrador de contraseñas de los navegadores web no puede ser suprimido desde la aplicación, el cliente inhabilita la función de autocompletar de los campos de usuario de las dos url objetivo con el objetivo de mitigar la vulnerabilidad. Esta implementación busca que el usuario digite siempre de cero los datos de autenticación en la aplicación y no que sea el navegador el que sugiera los usuarios ingresados los cuales al ser seleccionados ejecutan el administrador de contraseñas:

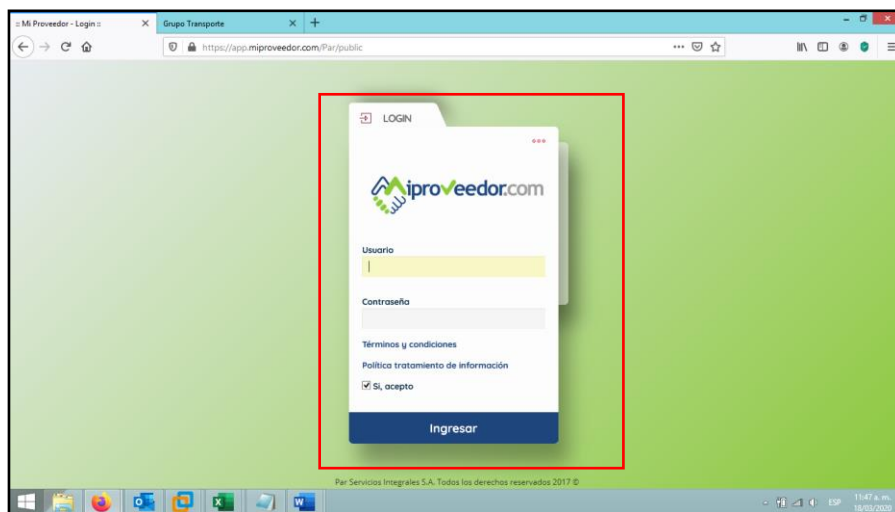


Gráfico 15. La aplicación ya no sugiere los usuarios ingresados.

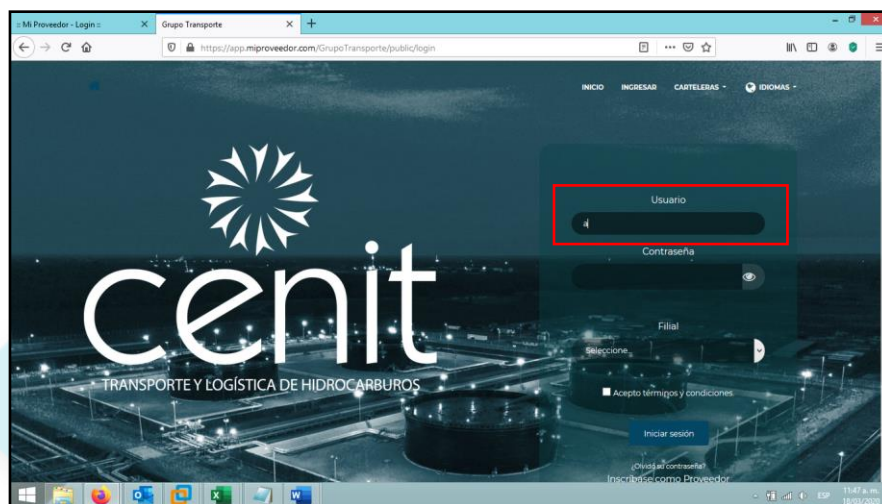


Gráfico 16. La aplicación ya no sugiere los usuarios ingresados.

Se observa que aún se presenta la vulnerabilidad en las dos url's.

- **Recomendación:** Se debe asegurar de que no se almacenen credenciales en texto claro o que sean fácilmente recuperables en cookie.
- **Referencia:**  
[https://www.owasp.org/index.php/Testing\\_for\\_Vulnerable\\_Remember\\_Password\\_\(OTG-AUTHN-005\)](https://www.owasp.org/index.php/Testing_for_Vulnerable_Remember_Password_(OTG-AUTHN-005))

### 5.7.6 Missing 'Strict-Transport-Security' header

- **Descripción:** Se realiza la validación de la vulnerabilidad sobre la URL <https://app.miproveedor.com/GrupoTransporte/public/login> como se muestra a continuación:

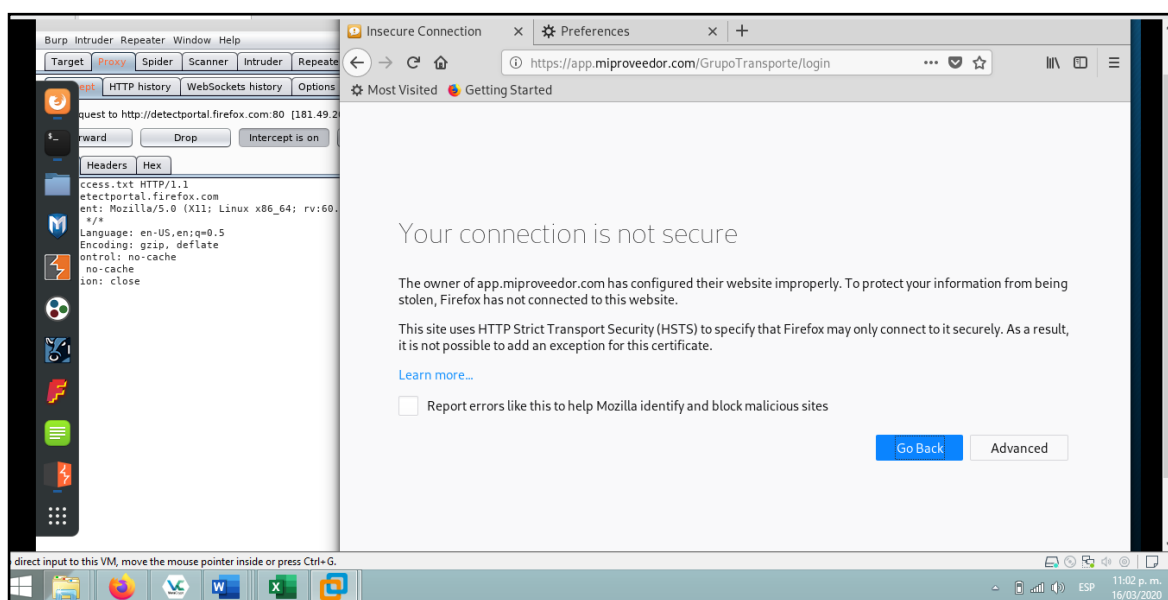


Gráfico 17. Intercepción tráfico aplicación pantalla autenticación.

Se observa que la aplicación ya cuenta con la implementación del encabezado HTTP Strict Transport Security (HSTS).

### 5.7.7 PHP version without support

- **Descripción:** En el ejercicio inicial por medio del scan de puertos, se identificó que la versión de PHP utilizada en el sitio web era PHP/7.0.33, la cual finalizo su periodo de soporte en enero del 2019. En el ejercicio de re test la aplicación ya no expone la versión de PHP utilizada, evitando que un atacante conozca fácilmente la vulnerabilidad de versión fuera de soporte.

### 5.7.8 Cross-site Scripting en sitios web (parcial)

- **Descripción:** Se realiza la validación insertando la sentencia `<script>alert('prueba')</script>` al momento de crear un nuevo certificado en la aplicación como se muestra en la siguiente imagen:

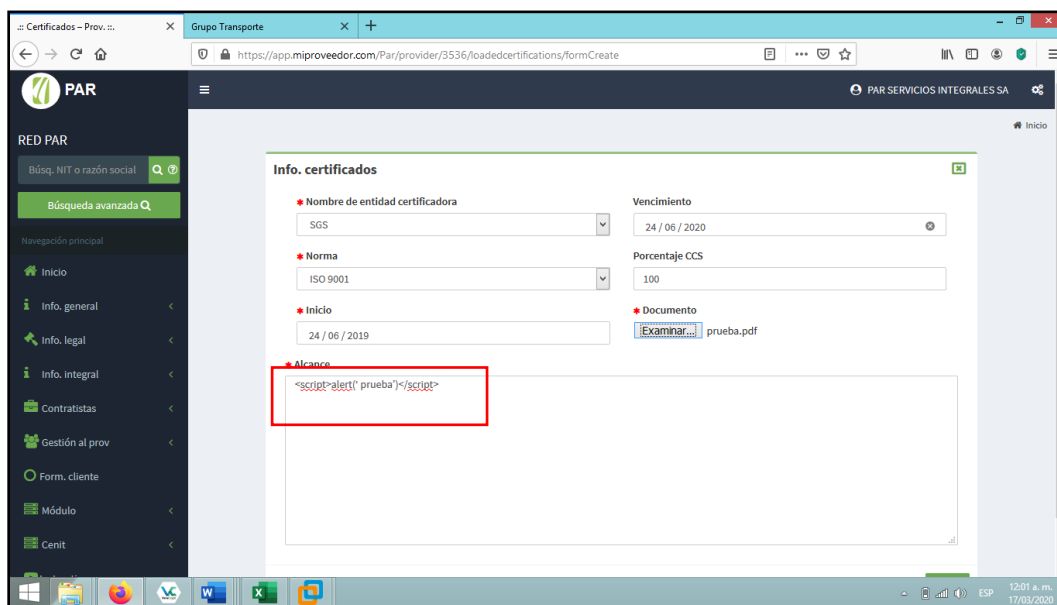


Gráfico 18. Se coloca sentencia XSS.

Se observa que el nuevo certificado se creó de manera exitosa:

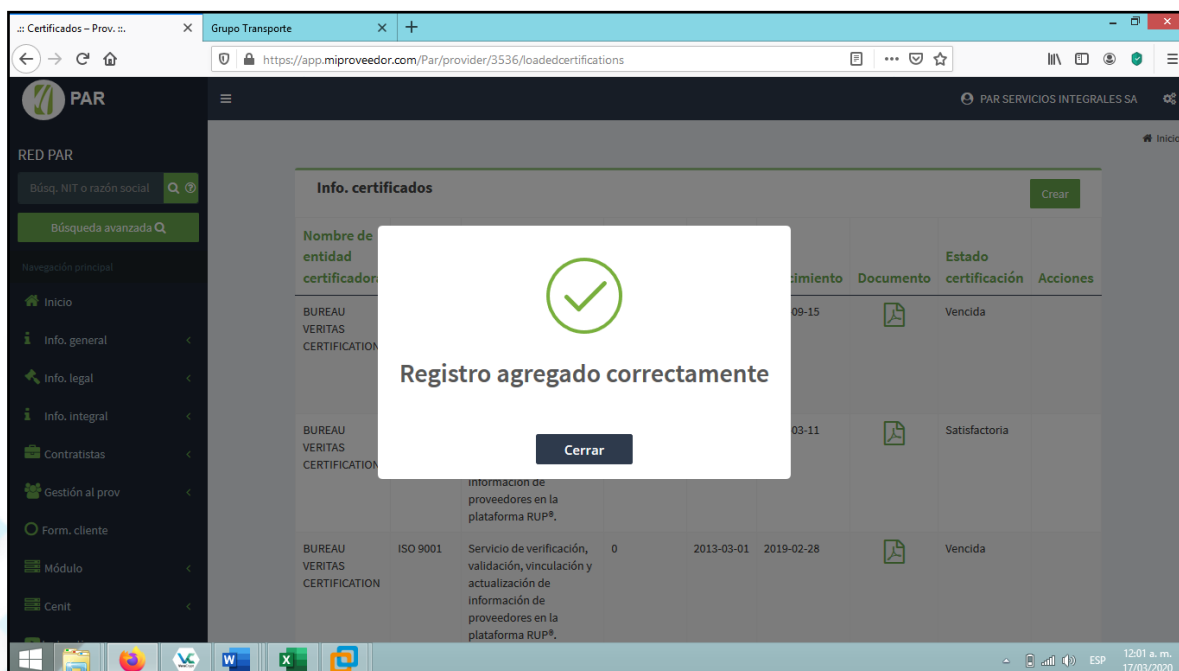


Gráfico 19. Se crea el certificado de manera exitosa

Entidad	Norma	Descripción	Puntaje	Fecha de inicio	Fecha de vencimiento	Estado	Acciones
VERITAS CERTIFICATION		verificación, validación, vinculación y actualización de información de proveedores en la plataforma RUP®.					
BUREAU VERITAS CERTIFICATION	OHSAS 18001	Servicio de verificación, validación, vinculación y actualización de información de proveedores en la plataforma RUP®.	0	2018-04-30	2021-03-11	Satisfactoria	
BUREAU VERITAS CERTIFICATION	ISO 9001	Servicio de verificación, validación, vinculación y actualización de información de proveedores en la plataforma RUP®.	0	2013-03-01	2019-02-28	Vencida	
DIAN	Resolución	Resolución de facturación	0	2016-06-14	2017-06-14	Vencida	
American Management Technology Inc.	ISO 9002	prueba retest payload	20	2020-01-07	2020-05-13		
SGS	ISO 9001	<script>alert(' prueba')</script>	100	2019-06-24	2020-06-24		

Gráfico 20. Se genera el registro exitosamente.

**Info. certificados**

Nombre de entidad certificadora: SGS

Vencimiento: 24 / 06 / 2020

Norma: ISO 9001

Porcentaje CCS: 100

Inicio: 24 / 06 / 2019

Documento: Examinar... Ningún archivo seleccionado.

Alcance: <script>alert(' prueba')</script>

Gráfico 21. Se ingresa al registro pero no se ejecuta el código ingresado

Como se observa, el sistema permite crear el registro y almacenar la sentencia en la aplicación, sin embargo, al ingresar nuevamente al registro la aplicación suprime la ejecución del código previamente insertado.



Dado que la aplicación mantiene el control de ejecución del código insertado en el campos de texto mitigando la vulnerabilidad, se deja como recomendación que para fortalecer el control se implemente un proceso de validación de meta caracteres sobre los datos ingresados en los formularios de la aplicación, teniendo en cuenta que cada dato debe ser validado cuando se recibe para asegurar que es del tipo correcto, o rechazado si no pasa ese proceso de validación.

## 6. Scan de Vulnerabilidades adicionales

Como valor agregado se realiza un escaneo de vulnerabilidades externo a la aplicación para identificar posibles nuevas vulnerabilidades después de la remediación. Los informes resultado se adjuntan al presente informe realizando la aclaración de que al ser una actividad de escaneo de vulnerabilidades, los hallazgos identificados no se les realiza proceso de validación y explotación.

## 7. Plataforma de Par Servicios – Fortalezas

Del conjunto de pruebas realizadas a la plataforma en el ReTest, se establecen las siguientes fortalezas:

FORTALEZA	DESCRIPCIÓN DE LA FORTALEZA
File upload	La aplicación cuenta con controles para evitar la carga de archivos adjuntos infectados que puedan materializar ataques de modificación, borrado o extracción de información.
Inyección	La aplicación controla la inyección de código o sentencias SQL maliciosas, las cuales están orientadas a extraer información técnica de como esta hecha la aplicación, o información sensible almacenada en el motor de base de datos.
Seguridad Perimetral	Los controles perimetrales con los que cuenta la aplicación evitan actividades de reconocimiento, en los que se recolectan datos técnicos sensibles.
Missing 'Strict-Transport-Security' header	La aplicación cuenta con el control 'Strict-Transport-Security' para evitar la materialización de ataques de hombre en el medio MITM.
Login page password-guessing attack	La aplicación cuenta con el control de ingreso errado de contraseña el cual evita ataques de fuerza bruta.

Tabla 5. Fortalezas aplicación

## 8. Conclusiones

### Conclusión General

8.1 En el ReTest realizado a la aplicación de **PAR SERVICIOS**, se identificó que se implementaron controles en la aplicación orientados a mitigar las siguientes vulnerabilidades:

- Protección ante la carga de archivos adjuntos maliciosos
- Seguridad perimetral reduciendo la cantidad de información técnica expuesta del servidor en el que está desplegada la aplicación.
- Protección ante ataques de hombre en el medio (MITM).
- Control en acceso a secciones de uso exclusivo del administrador.

### Conclusiones complementarias

- 8.2 Se debe generar un plan de remediación sobre las vulnerabilidades restantes.
- 8.3 Se debe establecer una acción correctiva para evitar el almacenamiento de contraseñas de login en el navegador a fin de mitigar el riesgo de fuga de información confidencial de la compañía.

## 9. Anexos

A continuación, se presenta una lista de documentos anexos a este informe:

- Información de los scan de puertos con y sin autorización del re test.
- Informe nuevo scan de vulnerabilidades.