

# CONTACTAR COLOMBIA

---

ETHICAL HACKING  
APPS EXTERNAS

INFORME ETHICAL HACKING

Diciembre 17 de 2020

	<p align="center"><b>INFORME TECNICO</b></p>	
<p align="center">Versión 1</p>	<p align="center">Julio de 2020</p>	<p align="center">Página 1 de 19</p>

## **CONFIDENCIALIDAD**

Este documento incluye información confidencial de uso exclusivo de las partes interesadas en la investigación del asunto.

Toda información contenida en el presente documento debe ser mantenida en forma estrictamente confidencial y utilizada exclusivamente para el desarrollo del objetivo del presente documento.

Las dependencias y/o funcionarios involucrados(as) en la lectura, revisión y/o aprobación del presente documento se obligan a darle el uso estrictamente necesario para el cumplimiento de los objetivos trazados, de igual forma se compromete a tomar las medidas necesarias para que la información no llegue a manos de terceros bajo ninguna circunstancia.

**ESTE DOCUMENTO ES GENERADO EN FORMATO PDF CON  
PERMISOS PARA LECTURA EN PANTALLA UNICAMENTE.**



## CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCION CAMBIO	ELABORO
1.0	Diciembre 17 de 2020	Documento Inicial	Karina Padilla

	<b>INFORME TECNICO</b>	
Versión 1	Julio de 2020	Página 3 de 19

## TABLA DE CONTENIDO

.....	0
1. Generalidades.....	5
2. Objetivo .....	5
3. Alcance .....	5
4. Limitaciones .....	6
5. Resumen ejecutivo .....	6
6. Metodología .....	7
7. Analisis manual .....	7
8. Herramientas tecnicas utilizadas .....	8
9. Prueba Narrativa.....	9
9.1. Resultados.....	13
9.2. Vulnerabilidades identificadas.....	14
9.2.1. Versión de JQuery con Múltiples Vulnerabilidades .....	14
9.2.2. Uso de cifrados de robustez media en SSL.....	14
9.2.3. Enumeración de usuarios SSH .....	16
9.2.4. Protocolos de Cifrado no Seguros Habilitados – TLS 1.0 y TLS 1.1 .....	17
9.2.5. Divulgación de versión .....	18
10. Conclusiones .....	19
11. Recomendaciones .....	19

## TABLA DE ILUSTRACIONES

<i>Ilustración 1 Pruebas de verificación de protocolos y algoritmos de cifrados formiik.....</i>	<i>9</i>
<i>Ilustración 2 Descubrimiento de servicios ip servidor .....</i>	<i>10</i>
<i>Ilustración 3 Descubrimiento de servicios formiik .....</i>	<i>10</i>
<i>Ilustración 4 Análisis de vulnerabilidades ip servidor .....</i>	<i>11</i>
<i>Ilustración 5 Análisis de vulnerabilidades formiik .....</i>	<i>11</i>
<i>Ilustración 6 Análisis de vulnerabilidades web.....</i>	<i>12</i>
<i>Ilustración 7 Enumeracion de usuarios SSH .....</i>	<i>12</i>
<i>Ilustración 8 Versión JQuery.....</i>	<i>14</i>
<i>Ilustración 9 Cifrados soportados .....</i>	<i>15</i>
<i>Ilustración 10 Enumeración de usuarios.....</i>	<i>16</i>
<i>Ilustración 11 Cifrados soportados.....</i>	<i>17</i>
<i>Ilustración 12 Versión del servicio SSH.....</i>	<i>18</i>

	<b>INFORME TECNICO</b>	
Versión 1	Julio de 2020	Página 5 de 19

## 1. Generalidades

<b>Empresa Solicitante</b>	Contactar Colombia
<b>Equipo</b>	Karina Padilla – Pentester , CEH, CPTe
<b>Sistemas Auditados</b>	Aplicaciones externas

## 2. Objetivo

- Realizar pruebas de Ethical Hacking a las aplicaciones de Contactar Colombia.
- Determinar si es posible y cómo un usuario malintencionado puede llegar a obtener mayores privilegios de los otorgados.

## 3. Alcance

A fin de conocer vectores de riesgo relacionado con las aplicaciones, se realizan auditorias sobre las siguientes aplicaciones:

NOMBRE DE LA APLICACION	URL/IP	TIPO
formiik	<a href="https://app.formiik.com/">https://app.formiik.com/</a>	WEB
Servidor	45.167.250.106	IP

## 4. Limitaciones

Para las pruebas se proporcionó un solo usuario con rol auditor, no teníamos conocimientos de las actividades que puede hacer un usuario con mayores privilegios.

## 5. Resumen ejecutivo

Para presentar los resultados de este análisis se establecen los siguientes niveles de riesgo en la evaluación de las vulnerabilidades encontradas:

Nivel de riesgo Alto: Fallas de seguridad que proporcionan información clara para acceder al sistema, o permiten el acceso directo al mismo.

Nivel de riesgo Medio: Fallas de seguridad que proporcionan información del sistema que podrían facilitar el acceso al mismo, utilizando técnicas de explotación y convirtiendo la falla en una de nivel de riesgo alto.

Nivel de riesgo Bajo: Fallas de seguridad que por sí solas no comprometen la seguridad del sistema analizado, pero combinado con otras fallas y utilizando técnicas de explotación podría aumentar el nivel de riesgo a medio o alto.

Las vulnerabilidades totales identificadas corresponden a la siguiente distribución:

Nivel de riesgo	Total
Alto	0
Medio	4
Bajo	1
Total encontrado	5

	<p align="center"><b>INFORME TECNICO</b></p>	
<p align="center">Versión 1</p>	<p align="center">Julio de 2020</p>	<p align="center">Página 7 de 19</p>

## 6. Metodología

Para la realización de las pruebas se usa como base la metodología de pruebas de penetración de IT SECURITY SERVICES, la guía de pruebas de penetración de PCI (Penetration Testing Guidance), teniendo en cuenta las siguientes fases:

- Recopilación de información / gestión de configuración.
- Test de Autenticación.
- Test de Autorización.
- Pruebas de gestión de sesión.
- Pruebas lógicas.
- Pruebas de manejo de errores.
- Validación de Data.
- Pruebas de almacenamiento con cifrado inseguro.
- Pruebas de comunicaciones inseguras.

Se realizaron pruebas manuales de inspección de código, y validación de data input, así como la verificación de usuarios por defecto, usuarios en blanco, contraseñas débiles, entre otras.

## 7. Analisis manual

En este caso se realiza la verificación del código en busca de funciones, procedimientos mal formados o variables flotantes que puedan exponer data sensible. Adicionalmente, se revisan los hallazgos arrojados por las herramientas de escaneo, corroborando la no existencia de falsos positivos en dichos resultados, esta comprobación se realiza revisando manualmente las peticiones que permitan explotar las vulnerabilidades asociadas a:

- Errores de inyección (SQLi, comandos de SO, LDAP, XPATH, entre otros). (6.5.1)
- Buffer overflow. (6.5.2)
- Almacenamiento y comunicaciones inseguras (no cifradas). (6.5.3 – 6.5.4)
- Manejo inadecuado de errores. (6.5.5)
- Cross site scripting (XSS). (6.5.7)
- Acceso no controlado a archivos y carpetas. (6.5.8)
- Cross Site Request Forgery (CSRF). (6.5.9)
- Session hijacking / Session fixation. (6.5.10)

Para dicha actividad se utilizan diferentes herramientas que están contenidas en la SUITE de Kali Linux, así como algunas herramientas de Windows. Una vez explotadas las vulnerabilidades, se extraen las evidencias correspondientes descartando los falsos positivos.



	<b>INFORME TECNICO</b>	
Versión 1	Julio de 2020	Página 8 de 19

Por otro lado, se revisan las vulnerabilidades de alto riesgo detectadas en el proceso de identificación de vulnerabilidades llevado a cabo por la organización para cada una de las IPs asociadas a las diferentes aplicaciones. En este proceso se ejecutan pruebas que permitan identificar si dichos fallos son falsos positivos o riesgos explotables que puedan comprometer la seguridad de los activos y/o aplicación.

Para las aplicaciones cliente servidor se realizan pruebas manuales de inserción de código, en donde existan campos de input data, adicionalmente se realizan intentos de acceso no autorizado sobre archivos y carpetas, pruebas de almacenamiento, comunicaciones inseguras y manejo inadecuado de errores.

## 8. Herramientas tecnicas utilizadas

Para el desarrollo de las pruebas sobre aplicación interna, se emplearon un conjunto de herramientas especializadas.

A continuación, se mencionan algunos de los aplicativos más utilizados en el proceso:

HERRAMIENTA	DESCRIPCIÓN
Python	Interprete para scripting del mismo lenguaje
Burp suite	Proxy HTTP
SQLMap	Herramienta de automatización de inyección SQL
Dirsearch	Herramienta de automatización de enumeración web

	<p align="center"><b>INFORME TECNICO</b></p>	
<p align="center">Versión 1</p>	<p align="center">Julio de 2020</p>	<p align="center">Página 9 de 19</p>

## 9. Prueba Narrativa

El objetivo de las pruebas realizadas, era diagnosticar el estado de seguridad de los activos de información establecidos en el alcance de este documento y si de alguna u otra manera se podía llegar a verse comprometidos.

Se realizó el análisis manualmente, validando los servicios disponibles dentro del perfil del usuario dado.

Se anexan las evidencias de los análisis correspondientes con las vulnerabilidades encontradas dentro de la validación de las pruebas:

```

OpenSSL 1.0.2-chacha (1.0.2g-dev)
Connected to 70.37.48.30
Testing SSL server app.formiik.com on port 443 using SNI name app.formiik.com

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.formiik.com
AltNames: DNS:*.formiik.com, DNS=formiik.com
Issuer: USERTrust RSA Organization Validation Secure Server CA

Not valid before: May 8 00:00:00 2020 GMT
Not valid after: Aug 10 00:00:00 2022 GMT

```

*Ilustración 1 Pruebas de verificación de protocolos y algoritmos de cifrados formiik*

```
Nmap scan report for 45.167.250.106
Host is up (0.037s latency).
Not shown: 1980 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
6129/tcp  filtered unknown
53/udp    open|filtered domain
67/udp    open|filtered dhcp
135/udp    open|filtered msrpc
136/udp    open|filtered profile
137/udp    open|filtered netbios-ns
138/udp    open|filtered netbios-dgm
139/udp    open|filtered netbios-ssn
161/udp    open|filtered snmp
445/udp    open|filtered microsoft-ds
500/udp    open     isakmp       StrongSwan ISAKMP
1029/udp   open|filtered solid-mux
1900/udp   open|filtered upnp
4500/udp   open     isakmp       StrongSwan ISAKMP
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

*Ilustración 2 Descubrimiento de servicios ip servidor*

```
Nmap scan report for app.formiik.com (40.113.232.207)
Host is up (0.15s latency).
Not shown: 65521 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http
443/tcp    open  https
3020/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3021/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3022/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3030/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3031/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3032/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3034/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8043/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8081/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8082/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8084/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8088/tcp   open  http         Microsoft IIS httpd 10.0
8089/tcp   open  ssl/http     Microsoft IIS httpd 10.0
```

*Ilustración 3 Descubrimiento de servicios formiik*

**TABLE OF CONTENTS**
**Vulnerabilities by Host**

- 45.167.250.106

## Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)
**45.167.250.106**

**Scan Information**

Start time: Thu Dec 10 09:07:39 2020  
 End time: Thu Dec 10 09:13:12 2020

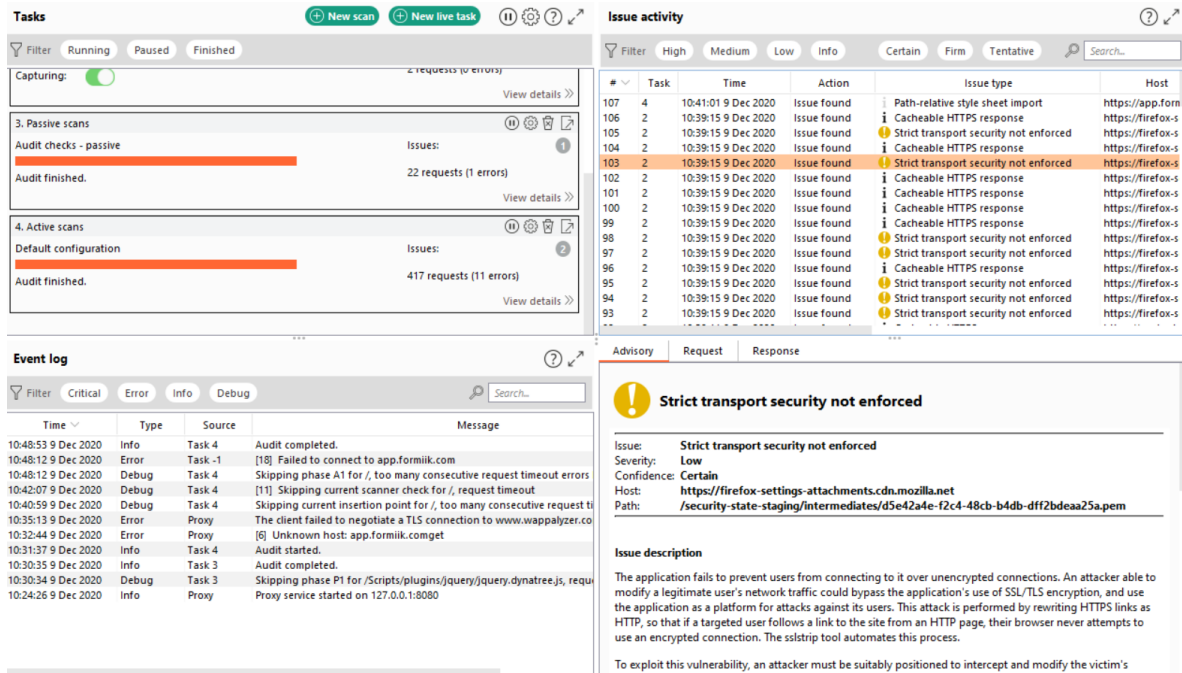
*Ilustración 4 Análisis de vulnerabilidades ip servidor*
**TABLE OF CONTENTS**
**Vulnerabilities by Host**

- app.formiik.com

## Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)
**app.formiik.com**

*Ilustración 5 Análisis de vulnerabilidades formiik*



The screenshot displays the Burp Suite interface during a scan. The 'Issues' tab shows a list of findings, with 'Strict transport security not enforced' highlighted. The 'Event log' shows the scan progress, including 'Audit finished' and '417 requests (11 errors)'. The detailed view of the issue shows the following information:

- Issue:** Strict transport security not enforced
- Severity:** Low
- Confidence:** Certain
- Host:** <https://firefox-settings-attachments.cdn.mozilla.net>
- Path:** <https://firefox-settings-attachments.cdn.mozilla.net/security-state-staging/intermediates/d5e42a4e-f2c4-48cb-b4db-dff2bdea25a.pem>

The issue description states: "The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process."

Ilustración 6 Análisis de vulnerabilidades web

```
msf5 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 45.167.250.106:22 - SSH - Using malformed packet technique
[*] 45.167.250.106:22 - SSH - Starting scan
[*] 45.167.250.106:22 - SSH - User 'root' found
[*] 45.167.250.106:22 - SSH - User 'www-data' found
[*] 45.167.250.106:22 - SSH - User 'sys' found
[*] 45.167.250.106:22 - SSH - User 'sshd' found
[*] 45.167.250.106:22 - SSH - User 'nobody' found
[*] 45.167.250.106:22 - SSH - User 'mail' found
[*] 45.167.250.106:22 - SSH - User 'games' found
[*] 45.167.250.106:22 - SSH - User 'daemon' found
[*] 45.167.250.106:22 - SSH - User 'backup' found
[*] 45.167.250.106:22 - SSH - User 'uucp' found
[*] 45.167.250.106:22 - SSH - User 'man' found
[-] 45.167.250.106:22 - SSH - User 'maintain' not found
[-] 45.167.250.106:22 - SSH - User 'maint' not found
[-] 45.167.250.106:22 - SSH - User 'm1122' not found
[-] 45.167.250.106:22 - SSH - User 'lynx' not found
[-] 45.167.250.106:22 - SSH - User 'lucy99' not found
[-] 45.167.250.106:22 - SSH - User 'lucenttech2' not found
[-] 45.167.250.106:22 - SSH - User 'lucenttech1' not found
[-] 45.167.250.106:22 - SSH - User 'LR-ISDN' not found
[-] 45.167.250.106:22 - SSH - User 'lpadm' not found
[*] 45.167.250.106:22 - SSH - User 'lp' found
```

Ilustración 7 Enumeración de usuarios SSH

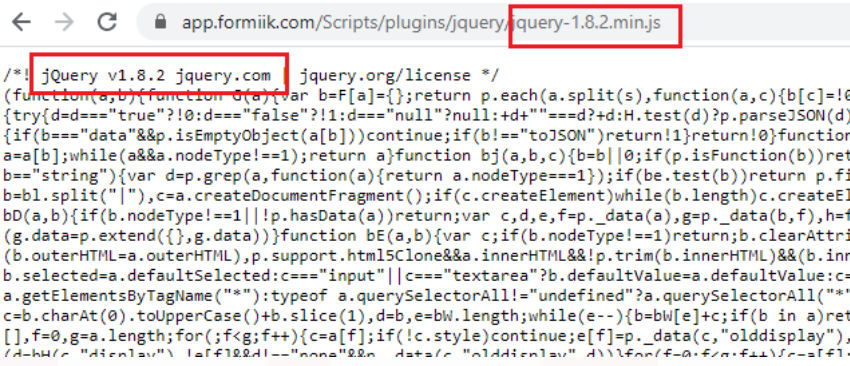
	<b>INFORME TECNICO</b>	
Versión 1	Julio de 2020	Página 13 de 19

### 9.1. Resultados

Luego de las diferentes pruebas realizadas, se establecen los siguientes resultados

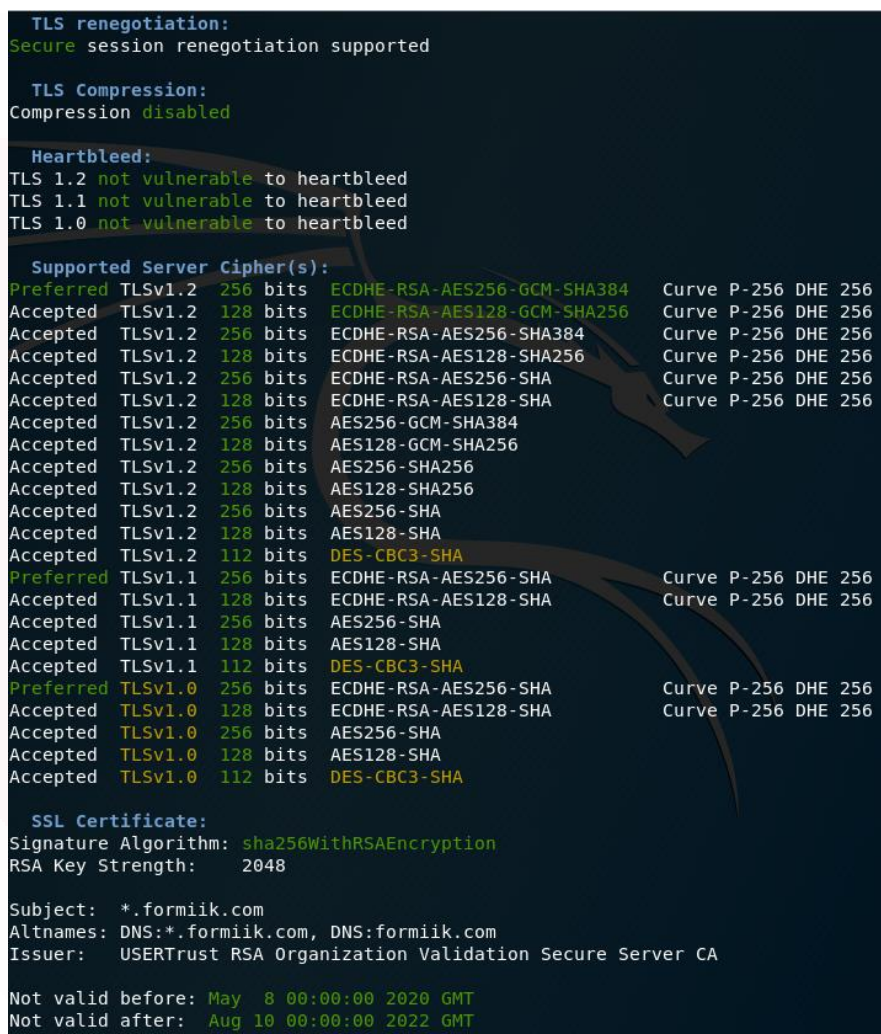
VULNERABILIDAD	TESTEADO	RESULTADO
Errores de inyección (SQLi, comandos de SO, LDAP, XPATH, entre otros). (6.5.1)	SI	No se encontró una vulnerabilidad asociada
Buffer overflow. (6.5.2)	SI	No se encontró una vulnerabilidad asociada
Almacenamiento y comunicaciones inseguras (no cifradas). (6.5.3 – 6.5.4)	SI	No se encontró una vulnerabilidad asociada
Manejo inadecuado de errores. (6.5.5)	SI	No se encontró una vulnerabilidad asociada
Cross site scripting (XSS). (6.5.7)	SI	No se encontró una vulnerabilidad asociada
Acceso no controlado a archivos y carpetas. (6.5.8)	SI	Se encontró una vulnerabilidad asociada
Cross Site Request Forgery (CSRF). (6.5.9)	SI	No se encontró una vulnerabilidad asociada
Session hijacking / Session fixation. (6.5.10)	SI	No se encontró una vulnerabilidad asociada

## 9.2. Vulnerabilidades identificadas

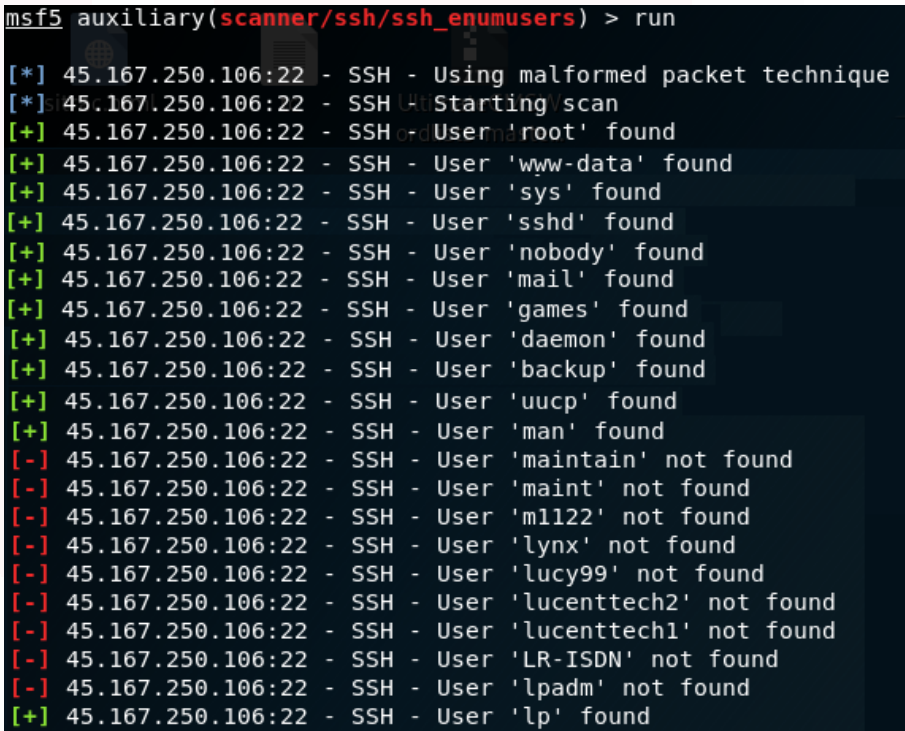
ID	CC-2020-CONTACTAR-001	Nivel	Media
CVSS	5.0 V:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		
Descripción del hallazgo	<b>9.2.1. Versión de JQuery con Múltiples Vulnerabilidades</b>  Se ha identificado la versión 1.8.2 de JQuery. Esta versión es vulnerable a XSS y denegación de servicio. Sin embargo, no ha sido posible verificar la presencia de esta vulnerabilidad porque se desconoce si se hace uso de los atributos vulnerables y en que componente(s) se usan.		
Evidencia	<p><a href="https://app.formiik.com/Scripts/plugins/jquery/jquery-1.8.2.min.js">https://app.formiik.com/Scripts/plugins/jquery/jquery-1.8.2.min.js</a></p>  <p><i>Ilustración 8 Versión JQuery</i></p>		
Recomendación	Se recomienda actualizar JQuery a la última versión estable, que a la fecha de elaboración de este informe es la 3.5.0		
Referencias	CVE-2020-11022, CVE-2020-11023		

ID	CC-2020-CONTACTAR-002	Nivel	Media
CVSS	5.0 V:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		
Descripción del hallazgo	<b>9.2.2. Uso de cifrados de robustez media en SSL</b>  Los servicios afectados permiten el uso de suites SSL que ofrecen un cifrado de robustez media. Se categoriza como cifrado medio cualquiera que utilice longitudes de clave de al menos 64 bits y menores que 112 bits, o que usen la suite de cifrado 3DES. Un atacante podría		



	eludir más fácilmente un cifrado de este tipo si se encuentra en la misma red.
Evidencia	<p>https://app.formiik.com:8089/</p>  <p><i>Ilustración 9 Cifrados soportados</i></p>
Recomendación	Se recomienda reconfigurar la aplicación afectada, si es posible, para evitar el uso de cifrados de robustez media tales como DES, CBC3 y SHA
Referencias	<a href="https://www.openssl.org/blog/blog/2016/08/24/sweet32">https://www.openssl.org/blog/blog/2016/08/24/sweet32</a>

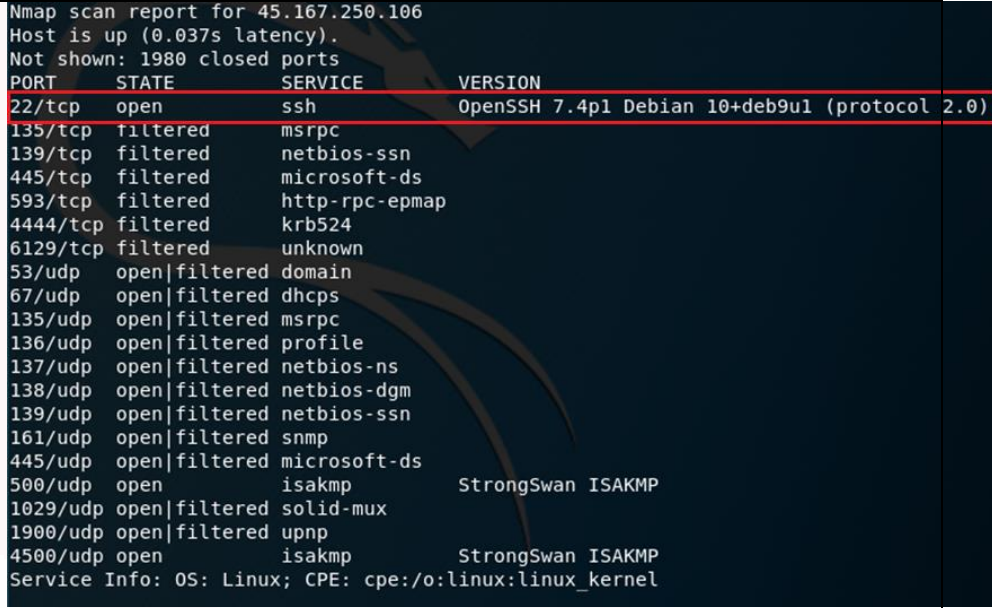


<b>ID</b>	CC-2020-CONTACTAR-003	<b>Nivel</b>	Media
<b>CVSS</b>	5.0 V:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		
<b>Descripción del hallazgo</b>	<b>9.2.3. Enumeración de usuarios SSH</b>  OpenSSH hasta la versión 7.7 está afectado por una vulnerabilidad de enumeración de usuarios debido a no retrasar la respuesta para un usuario de autenticación no válida hasta después de que el paquete que contiene la solicitud haya sido completamente analizado.		
<b>Evidencia</b>	 <p style="text-align: center;"><i>Ilustración 10 Enumeración de usuarios</i></p>		
<b>Recomendación</b>	Se recomienda aplicar los parches de seguridad apropiados para OpenBSD y OpenSSH (6.7p1-1, 7.7p1-1).		
<b>Referencias</b>	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473</a> <a href="http://www.openwall.com/lists/oss-security/2018/08/15/5">http://www.openwall.com/lists/oss-security/2018/08/15/5</a>		

ID	CC-2020-CONTACTAR-004	Nivel	Media
CVSS	5.0 V:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		
Descripción del hallazgo	<p><b>9.2.4. Protocolos de Cifrado no Seguros Habilitados – TLS 1.0 y TLS 1.1</b></p> <p>El servicio web acepta el cifrado de conexiones mediante TLS 1.0 y 1.1. El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago o PCI DSS establece que, a partir del 30 de junio de 2018, TLS 1.0 debe ser deshabilitado excepto en terminales POS POI, en los cuales se ha verificado que no se encuentran afectados por ninguna vulnerabilidad pública. Adicionalmente, PCI DSS sugiere deshabilitar TLS 1.1.</p>		
Evidencia	<p><a href="https://app.formiik.com:8089/">https://app.formiik.com:8089/</a></p>  <p><i>Ilustración 11 Cifrados soportados</i></p>		
Recomendación	Se recomienda deshabilitar los protocolos TLS 1.0 y 1.1.		

 <b>IT-SS</b> Expertos en S.I & Ciberseguridad	<b>INFORME TECNICO</b>	 <b>Contactar</b> Microfinanciera
Versión 1	Julio de 2020	Página 18 de 19

Referencias	<a href="https://www.blai.blog/2019/11/deshabilitar-tls-10-y-tls-11-en-iis.html">https://www.blai.blog/2019/11/deshabilitar-tls-10-y-tls-11-en-iis.html</a>
-------------	---

ID	CC-2020-CONTACTAR-005	Nivel	Baja
CVSS	<a href="#">AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N</a>		
Descripción del hallazgo	<b>9.2.5. Divulgación de versión</b> Se identificó que el protocolo SSH divulga la versión instalada.		
Evidencia	 <p>Nmap scan report for 45.167.250.106          Host is up (0.037s latency).          Not shown: 1980 closed ports          PORT STATE SERVICE VERSION          22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)          135/tcp filtered msrpc          139/tcp filtered netbios-ssn          445/tcp filtered microsoft-ds          593/tcp filtered http-rpc-epmap          4444/tcp filtered krb524          6129/tcp filtered unknown          53/udp open filtered domain          67/udp open filtered dhcpc          135/udp open filtered msrpc          136/udp open filtered profile          137/udp open filtered netbios-ns          138/udp open filtered netbios-dgm          139/udp open filtered netbios-ssn          161/udp open filtered snmp          445/udp open filtered microsoft-ds          500/udp open isakmp StrongSwan ISAKMP          1029/udp open filtered solid-mux          1900/udp open filtered upnp          4500/udp open isakmp StrongSwan ISAKMP          Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel</p> <p><i>Ilustración 12 Versión del servicio SSH</i></p>		
Recomendación	● Realizar un hardening al servicio SSH para ocultar la información de la versión instalada.		
Referencias	<a href="http://kb.ictbanking.net/article.php?id=666">http://kb.ictbanking.net/article.php?id=666</a> <a href="https://cwe.mitre.org/data/definitions/200.html">https://cwe.mitre.org/data/definitions/200.html</a>		

	<p align="center"><b>INFORME TECNICO</b></p>	
<p align="center">Versión 1</p>	<p align="center">Julio de 2020</p>	<p align="center">Página 19 de 19</p>

## 10. Conclusiones

Basado en el estudio de las pruebas realizadas,

- Se evidencia que la aplicación cuenta con las buenas prácticas de seguridad en desarrollo de código seguro.

## 11. Recomendaciones

- Se recomienda hardening del servicio SSH para evitar la divulgación de información y la enumeración de usuarios.
- Se recomienda el uso de cifrados fuertes para las comunicaciones.
- Se recomienda la actualización del servicio SSH y la librería de Jquery a la última versión estable.