





Análisis de Ethical Hacking

Jarvis

Noviembre 2021





	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada			Página 2 de 32

Derechos de uso:



El presente documento es propiedad de Mibanco – Banco de la Microempresa S.A. (en adelante, Mibanco), tiene carácter de uso confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático, ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y por escrito de Mibanco, titular del copyright .

El incumplimiento de las limitaciones señaladas será sancionado conforme a ley.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 3 de 32	

Contenido

1. INTRODUCCIÓN	4
1.1 Objetivo	4
1.2 Alcance	4
2. ANTECEDENTES	4
2.1 Resumen	4
3. CRITERIOS PARA LAS CALIFICACIONES DE RIESGO	5
4. CLASIFICACIÓN DE RIESGO	6
5. RESUMEN EJECUTIVO	7
5.1 Tabla de contenido	7
6. ANÁLISIS APLICATIVO JARVIS	8
6.1 Hallazgos	8
7. CONCLUSIONES	32
8. RECOMENDACIONES	32
9. NOMENCLATURA	32

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 4 de 32	

1. INTRODUCCIÓN

1.1 Objetivo

Identificar las brechas de seguridad existentes, con el objetivo de brindar o establecer controles de seguridad que permitan la mitigación de las vulnerabilidades encontradas basándose en las políticas de seguridad vigentes de **MiBanco**.



1.2 Alcance

Validación de posibles brechas de seguridad en el aplicativo móvil **Jarvis**.

2. ANTECEDENTES

2.1 Resumen

Solicita un Retest de Ethical Hacking del aplicativo Jarvis que se despliega en dispositivos Android. Se solicitaron dos usuarios de prueba con distintos tipos de roles para identificar vulnerabilidades en ambas cuentas.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 5 de 32	

3. CRITERIOS PARA LAS CALIFICACIONES DE RIESGO

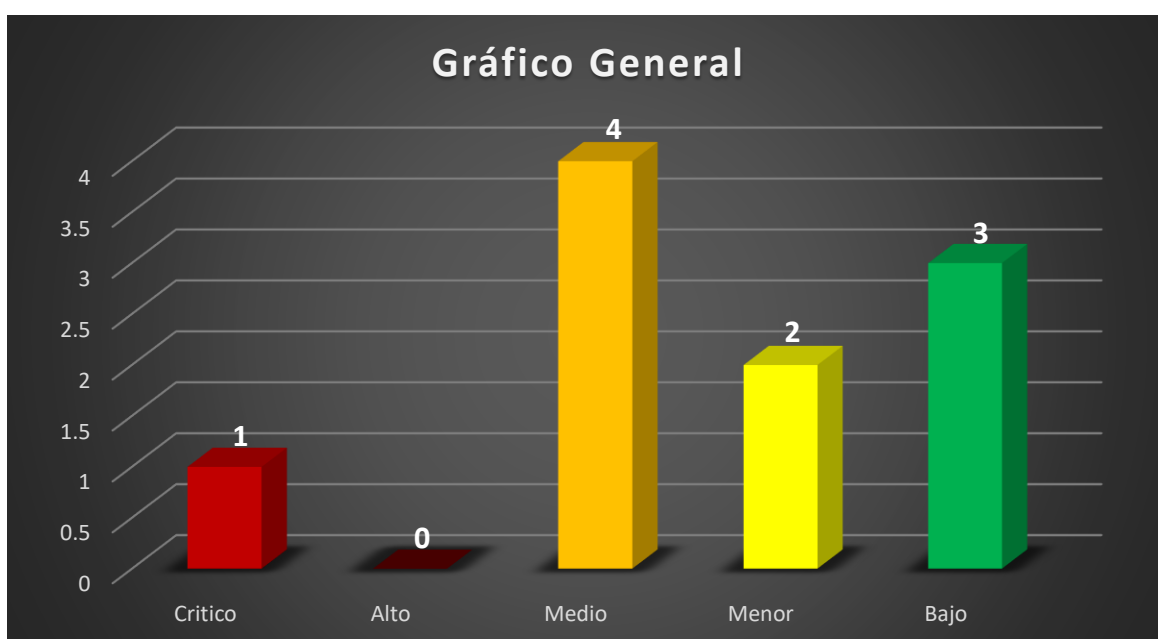
La siguiente tabla proporciona una clave de la denominación de riesgos y los colores utilizados en este informe para proporcionar un sistema de puntuación de riesgo.



#	Risk Rating	Descripción
1	CRITICO	Estos problemas pueden representar una amenaza de seguridad muy importante. Los problemas que tienen un impacto crítico suelen ser aquellos que permitirían a un atacante obtener acceso administrativo completo al dispositivo.
2	ALTO	Estos hallazgos identifican condiciones que podrían resultar directamente en el compromiso o acceso no autorizado de una red, sistema, aplicación o información. Los ejemplos de riesgos altos incluyen desbordamientos de búfer conocidos, contraseñas débiles o inexistentes, sin cifrado, lo que podría resultar en la denegación de servicio en sistemas o servicios críticos; Acceso no autorizado; y divulgación de información.
3	MEDIO	Estos hallazgos identifican condiciones que no resultan inmediata o directamente en el compromiso o acceso no autorizado de una red, sistema, aplicación o información, pero proporcionan una capacidad o información que podría, en combinación con otras capacidades o información, resultar en el compromiso o acceso no autorizado a una red, sistema, aplicación o información. Los ejemplos de riesgos medios incluyen sistemas, archivos y servicios desprotegidos que podrían resultar en la denegación de servicio en servicios o sistemas no críticos; y exposición de información de configuración y conocimiento de servicios o sistemas para explotarlos más.
4	MENOR	Estos problemas tienen limitaciones en el impacto directo que pueden causar. Por lo general, estos problemas incluirían problemas de fuga de información, problemas de denegación de servicio o aquellos que proporcionan un acceso significativamente limitado.
5	BAJO	Estos problemas representan una amenaza de seguridad de bajo nivel. Un problema típico implicaría la filtración de información que podría ser útil para un atacante, como una lista de usuarios o detalles de la versión.

4. CLASIFICACIÓN DE RIESGO

El nivel de riesgo es producto del impacto **(de negocio o técnico)** por la probabilidad de ocurrencia. La probabilidad de ocurrencia de explotación de vulnerabilidades es inversamente proporcional a la complejidad del ataque. Por lo tanto, se ha determinado el riesgo en función al impacto y a la complejidad de ataque de la siguiente manera:

Niveles de Riesgo Ethical Hacking						
Impacto	Crítico					1
	Alto					
	Medio			6,7,8		
	Menor	13	11,12	9		
	Bajo			15,16		
		Muy Raro	Raro	Eventual	Frecuente	Muy Frecuente
		Probabilidad				





	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada			Página 7 de 32

5. RESUMEN EJECUTIVO

5.1 Tabla de contenido

Código	Título de la Incidencia	Riesgo	Estado
Vuln01	Bypass Root Detection	Crítico	X
Vuln02	Bypass SSL Pinning	Crítico	✓
Vuln03	Fuzzer - Ataques automatizados	Alto	✓
Vuln04	Fuera de sesión - Autenticación Mutua	Alto	✓
Vuln05	Suplantación de Identidad	Alto	✓
Vuln06	Validación de dominios	Medio	X
Vuln07	Autenticación y Administración de identidades	Medio	X
Vuln08	Ejecución de APK en Emulador	Medio	X
Vuln09	Brute Force	Medio	X
Vuln10	Cifrados inseguros implementados	Menor	✓
Vuln11	Ausencia de WAF	Menor	X
Vuln12	Detección de IP	Menor	X
Vuln13	Enumeración de usuarios	Bajo	X
Vuln14	JavaScript dependency	Bajo	✓
Vuln15	Errores genéricos	Bajo	X
Vuln16	Mensajes genéricos	Bajo	X
Vuln17	Use of a Broken or Risky Cryptographic Algorithm	Bajo	✓

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 8 de 32	

6. ANÁLISIS APLICATIVO JARVIS

6.1 Hallazgos

Vulnerabilidad	Bypass Root Detection		
Código ID	Vuln 01	Riesgo	Crítico
Target	APP JARVIS		

Resultados de Evaluación



Se valida que la aplicación no cuenta con mecanismos que detecten si algún software de terceros está validando el tráfico de la aplicación y las funciones de llamada al sistema operativo con el fin de modificar su resultado.
Un potencial atacante puede modificar el binario original de la aplicación y generar una aplicación alterna con funcionalidades maliciosas y con los controles de seguridad eliminados.

Aplicación Formiik Mobile

- a) Se identifica que el aplicativo no se apertura en dispositivos rooteados y da como resultado un banner de alerta.



Imagen 01.- Acceso no permitido.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 9 de 32	

b) Al realizar la decompilación del aplicativo se visualiza la detección del modo Root.

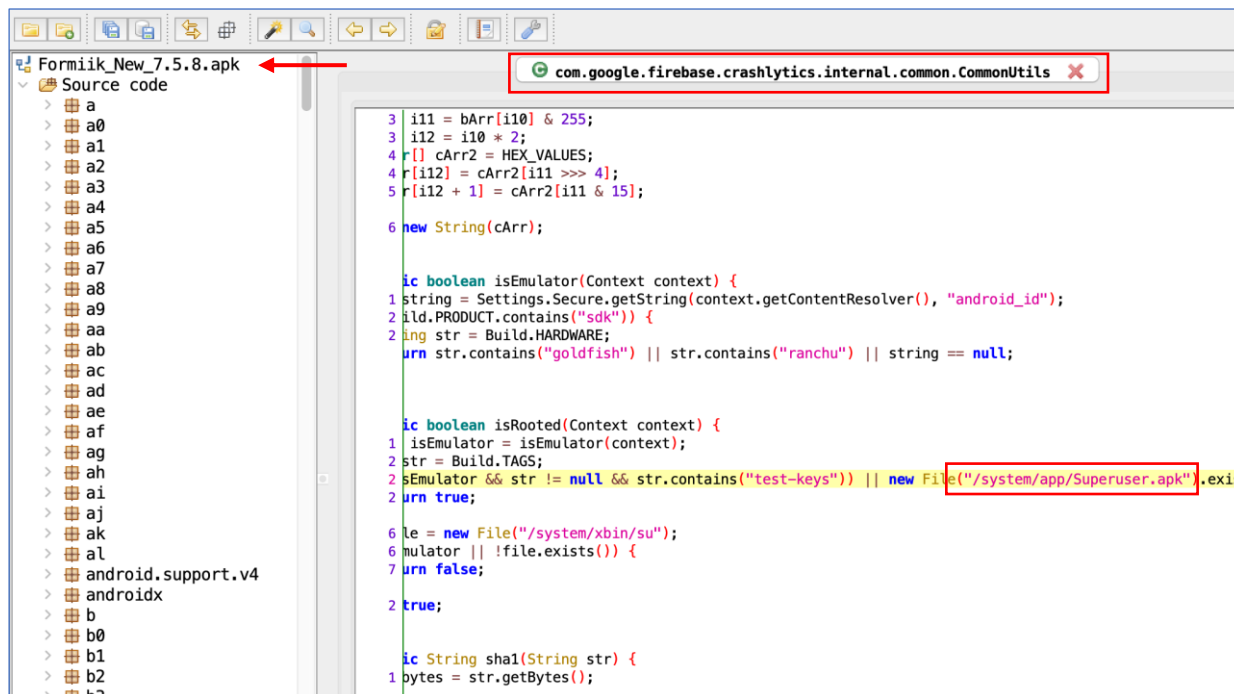


Imagen 02.- Ruta de evidencia.

c) El dispositivo celular donde se realizarán las pruebas tiene privilegios root.

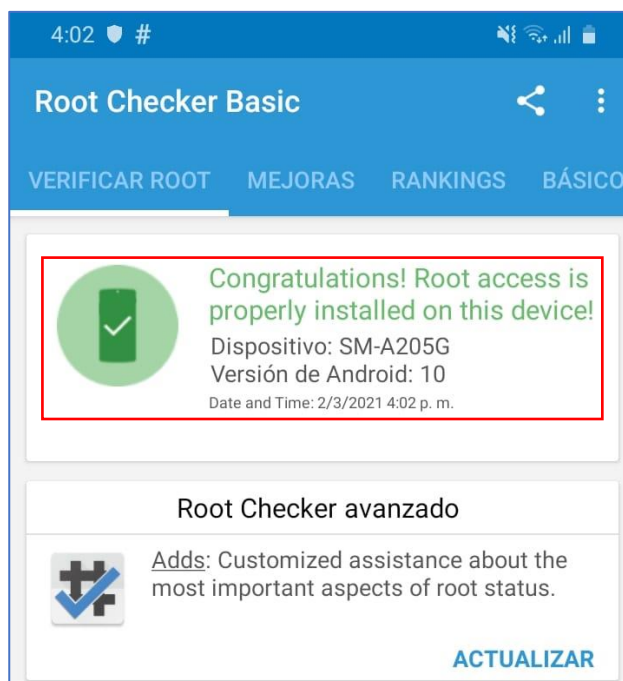




Imagen 03.- Dispositivo rooteado.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 10 de 32	

PID	Name
7326	Formiik New
7029	Google Play Store
2930	Lite
1713	adbd
2404	android.ext.services
2506	android.process.acore
1851	audioserver
1852	cameraserver
3839	com.android.defcontainer
2440	com.android.keychain
2287	com.android.phone
2232	com.android.systemui
6811	com.android.vending:background
6447	com.google.android.gms
6092	com.google.android.gms.feedback
5608	com.google.android.gms.persistent
6209	com.google.android.gms.ui
6862	com.google.android.instantapps.supervisor
2643	com.google.process.gapps
5684	com.vphone.launcher
1663	debuggerd
1670	debuggerd:signaller
1779	drmserver
6997	frida-server
1716	gatekeeperd

Imagen 04.- Se ubica el proceso donde se ejecuta.

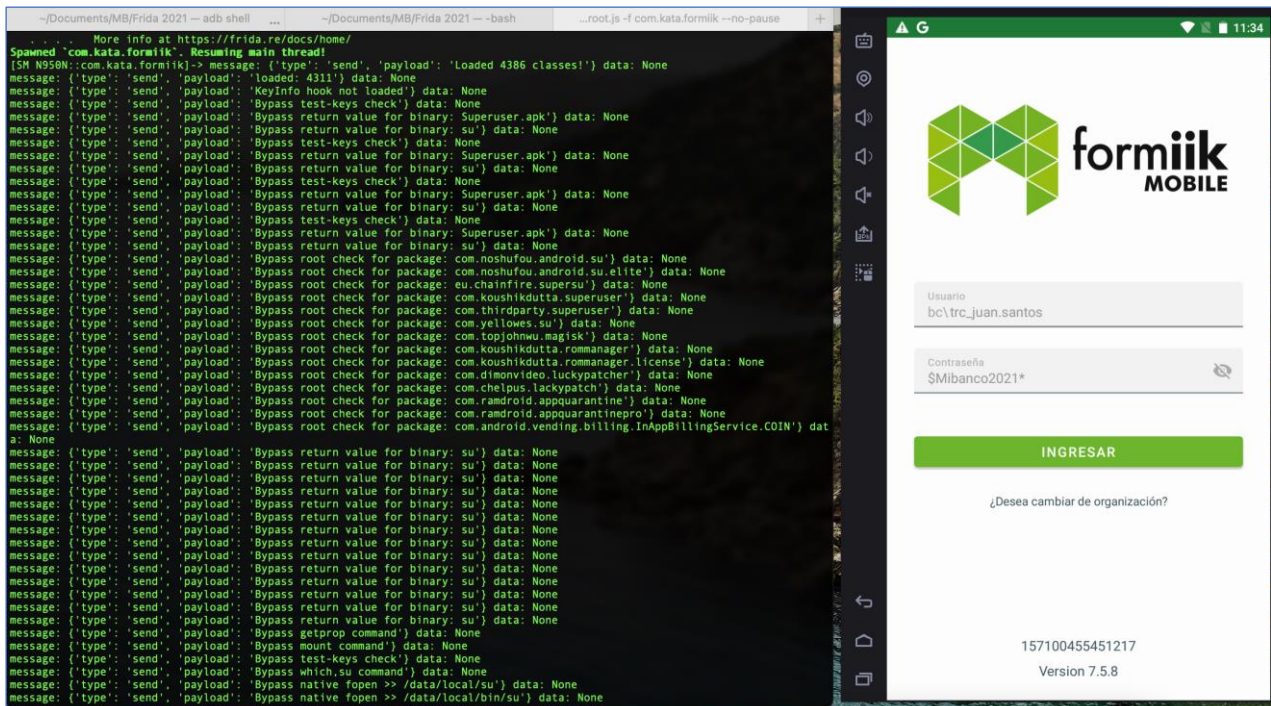




Imagen 05.- Ejecución de la aplicación dentro de un dispositivo rootado.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 11 de 32	

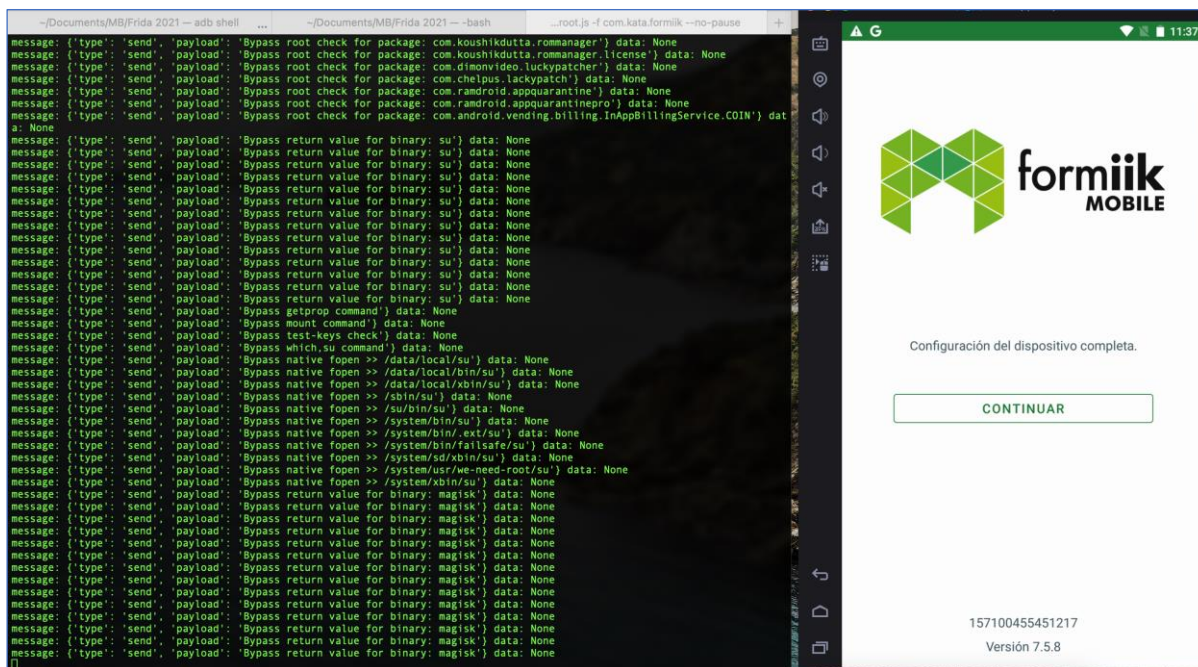


Imagen 06.- Configuración exitosa.



Recomendación

Se recomienda implementar verificaciones de integridad que comprueben que el binario y sus recursos no han sido modificados los cuales deben ser reforzados por mecanismos adicionales como los siguientes:

- Ofuscación robusta de código.
- Controles anti-debugging

Referencia

- <https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet#security-libraries>

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 12 de 32	

Vulnerabilidad	Bypass SSL Pinning		
Código ID	Vuln 02	Riesgo	-
Target	APP JARVIS		

Resultados de Evaluación

Se valida la correcta solución del bypass del SSL Pinning donde no se permite realizar una interceptación de las comunicaciones del APP.

Aplicación Formiik Mobile

- a) Se identifica un error al intentar realizar una comunicación TLS.

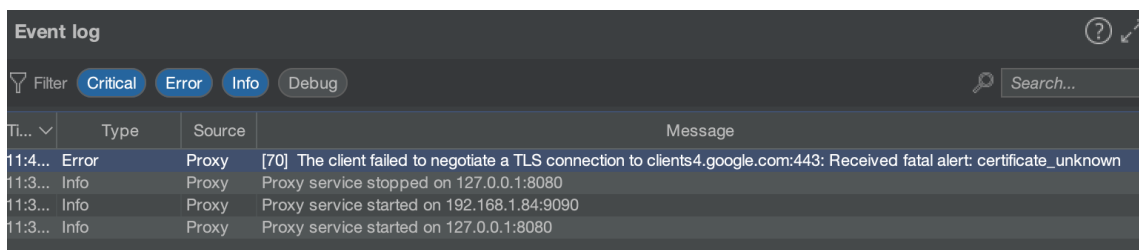


Imagen 01.- Acceso no permitido.

```

Spawned `com.kata.formiik`. Use %resume to let the main thread start executing!
[SM N950N::com.kata.formiik]-> %resume
[SM N950N::com.kata.formiik]->
=====
[#] Android Bypass for various Certificate Pinning methods [#]
=====
[-] OkHttpV3 {1} pinner not found
[-] OkHttpV3 {2} pinner not found
[-] OkHttpV3 {3} pinner not found
[-] OkHttpV3 {4} pinner not found
[-] Trustkit {1} pinner not found
[-] Trustkit {2} pinner not found
[-] Trustkit {3} pinner not found
[-] Appcelerator PinningTrustManager pinner not found
[-] OpenSSLEngineSocketImpl Conscrypt pinner not found
[-] OpenSSLSocketImpl Apache Harmony pinner not found
[-] PhoneGap sslCertificateChecker pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {1} pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {1} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {3} pinner not found

```



Imagen 02.- Ataque fallido.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 13 de 32	

Vulnerabilidad	Fuzzer - Ataques automatizados		
Código ID	Vuln 03	Riesgo	-
Target	APP JARVIS		

Resultados de Evaluación

Se valida la correcta solución del bypass del SSL Pinning donde no se permite realizar una interceptación de las comunicaciones del APP.

Aplicación Formiik Mobile

```

Spawned `com.kata.formiik`. Use %resume to let the main thread start executing!
[SM N950N::com.kata.formiik]-> %resume
[SM N950N::com.kata.formiik]->
=====
[#] Android Bypass for various Certificate Pinning methods [#]
=====
[-] OkHTTPv3 {1} pinner not found
[-] OkHTTPv3 {2} pinner not found
[-] OkHTTPv3 {3} pinner not found
[-] OkHTTPv3 {4} pinner not found
[-] Trustkit {1} pinner not found
[-] Trustkit {2} pinner not found
[-] Trustkit {3} pinner not found
[-] Appcelerator PinningTrustManager pinner not found
[-] OpenSSLEngineSocketImpl Conscrypt pinner not found
[-] OpenSSLSocketImpl Apache Harmony pinner not found
[-] PhoneGap sslCertificateChecker pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {1} pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {1} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {3} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {4} pinner not found
[-] CWAC-Netsecurity CertPinManager pinner not found
[-] Worklight Androidgap WLCertificatePinningPlugin pinner not found
[-] Netty FingerprintTrustManagerFactory pinner not found
[-] Squareup CertificatePinner {1} pinner not found
[-] Squareup CertificatePinner {2} pinner not found
[-] Squareup OkHostnameVerifier pinner not found
[-] Squareup OkHostnameVerifier pinner not found
[-] Android WebViewClient {2} pinner not found
[-] Apache Cordova WebViewClient pinner not found
[-] Boye AbstractVerifier pinner not found
[+] Bypassing Trustmanager (Android < 7) request
[+] Bypassing Trustmanager (Android < 7) request
[+] Bypassing Trustmanager (Android < 7) request

```



Imagen 01.- Ataque fallido.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 14 de 32	

Vulnerabilidad	Fuera de sesión - Autenticación Mutua		
Código ID	Vuln 04	Riesgo	-
Target	https://app.formiik.com:3034/SecurityPipeRest.svc https://app.formiik.com:3034/MiddlewareRest.svc?xsd=xsd2		

Resultados de Evaluación

Se valida la correcta solución de la vulnerabilidad detectada en un primer informe de Ethical Hacking.

Aplicación Formiik

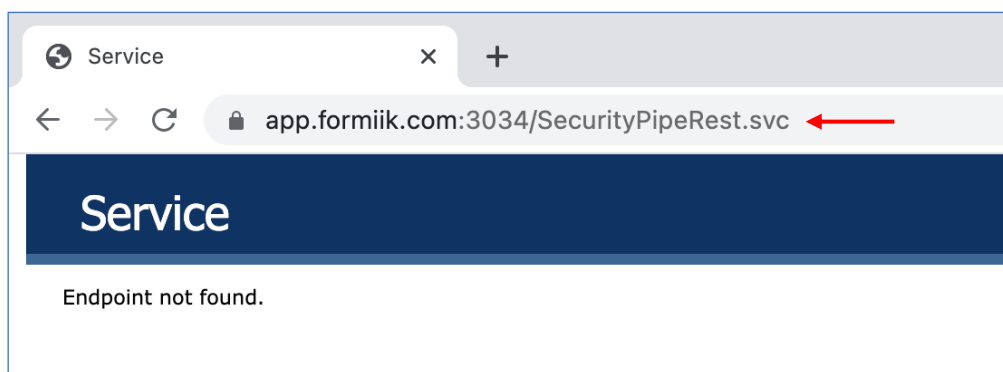


Imagen 01.- Evidencia.

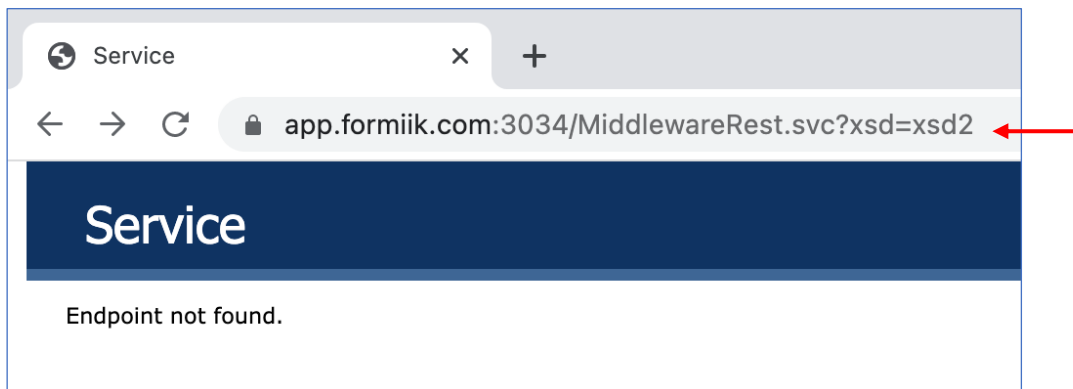




Imagen 02.- Evidencia.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 15 de 32	

Vulnerabilidad	Suplantación de Identidad		
Código ID	Vuln 05	Riesgo	-
Target	https://app.formiik.com:3034		

Resultados de Evaluación

Se valida la correcta solución de la vulnerabilidad detectada en un primer informe de Ethical Hacking.

Aplicación

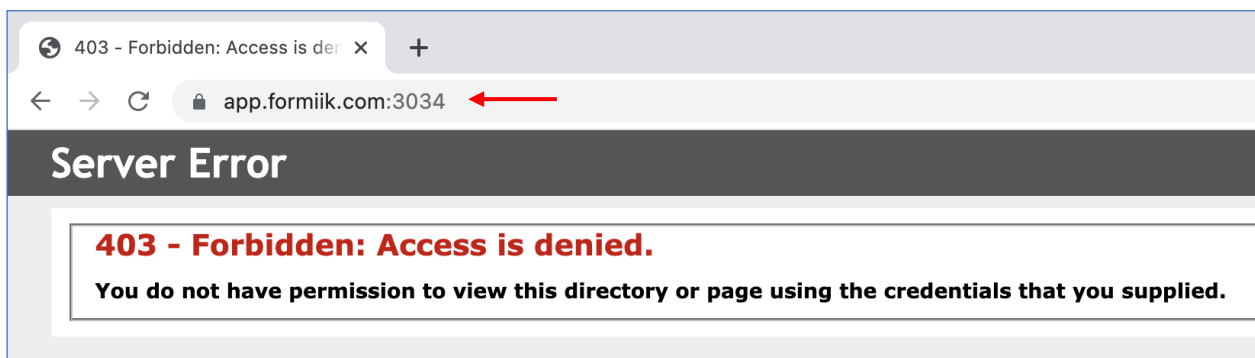




Imagen 01.- Evidencia.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 16 de 32	

Vulnerabilidad	Validación de dominios		
Código ID	Vuln 06	Riesgo	Medio
Target	https://app.formiik.com		

Resultados de Evaluación

Se realiza un ataque de fuerza bruta para identificar que otro tipo de empresas trabajan con la plataforma Formiik y con ello realizar algún tipo de vector de ataque de recolección de información.

Aplicación Formiik

- a) Se procede a seleccionar el parámetro de realizar el fuzzer.

```

1 POST /Login/bf HTTP/2
2 Host: app.formiik.com
3 Cookie: ai_user=K+VNw+1JgKZPdSBioFt50I|2021-11-05T02:44:28.568Z; ai_sessio
4 Content-Length: 59
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "macOS"
9 Upgrade-Insecure-Requests: 1
10 Origin: null
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Accept-Encoding: gzip, deflate
19 Accept-Language: es-419,es;q=0.9
20
21 client=b$fs&differenceTimespan=-5&userName=test&password=test

```

Imagen 01.- Parámetro client.

- b) Creación de una lista de palabras a inyectar.

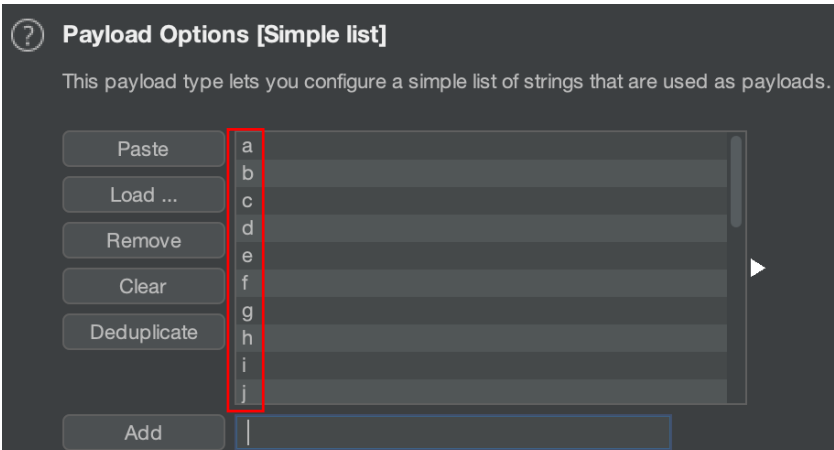




Imagen 02.- Ruta de evidencia.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 17 de 32	

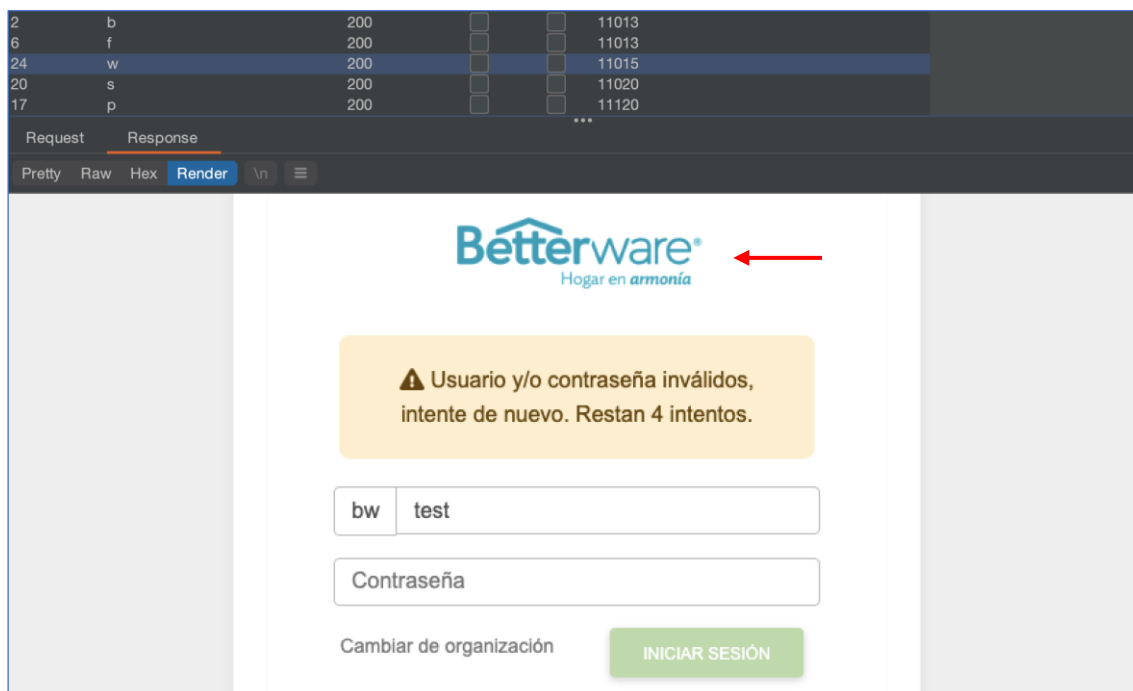


Imagen 03.- Evidencia.

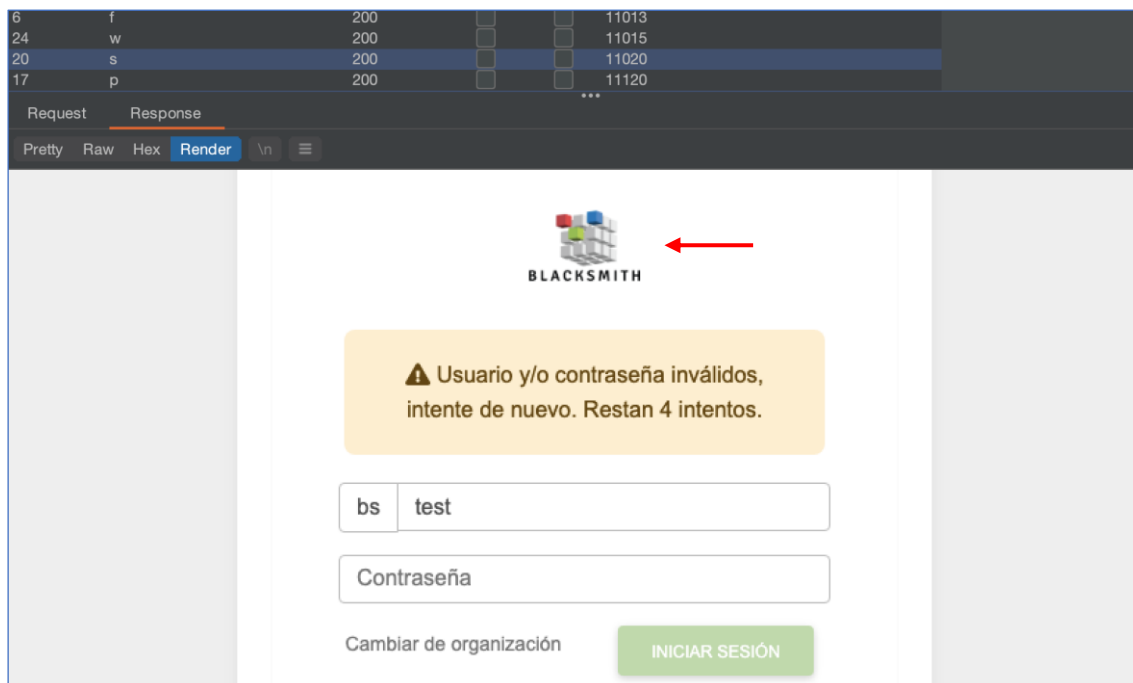


Imagen 04.- Evidencia.

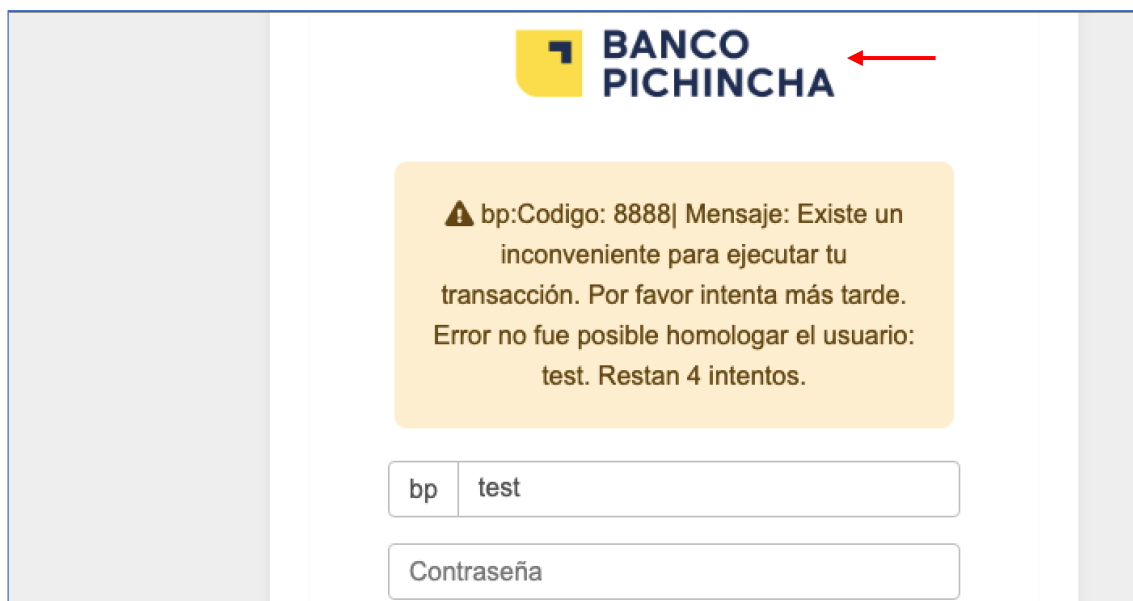


Imagen 05.- Evidencia.

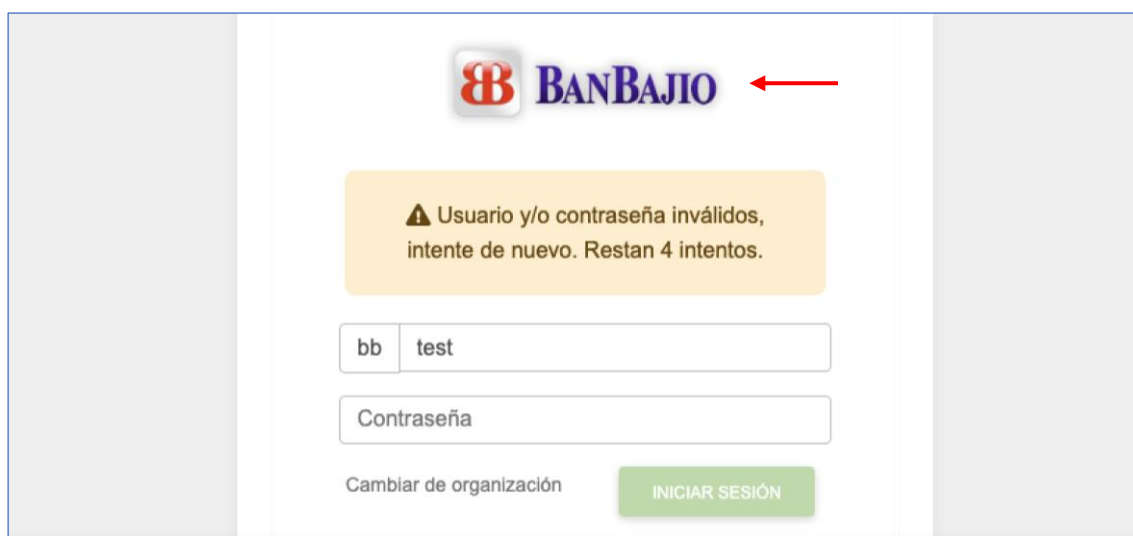




Imagen 06.- Evidencia.

Recomendación

- Implementar un reCaptcha para evitar múltiples intentos de validación de dominios.
- Emplear consultas POST.

Referencia

- <https://developer.android.com/training/safetynet/recaptcha?hl=es-419>

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 19 de 32	

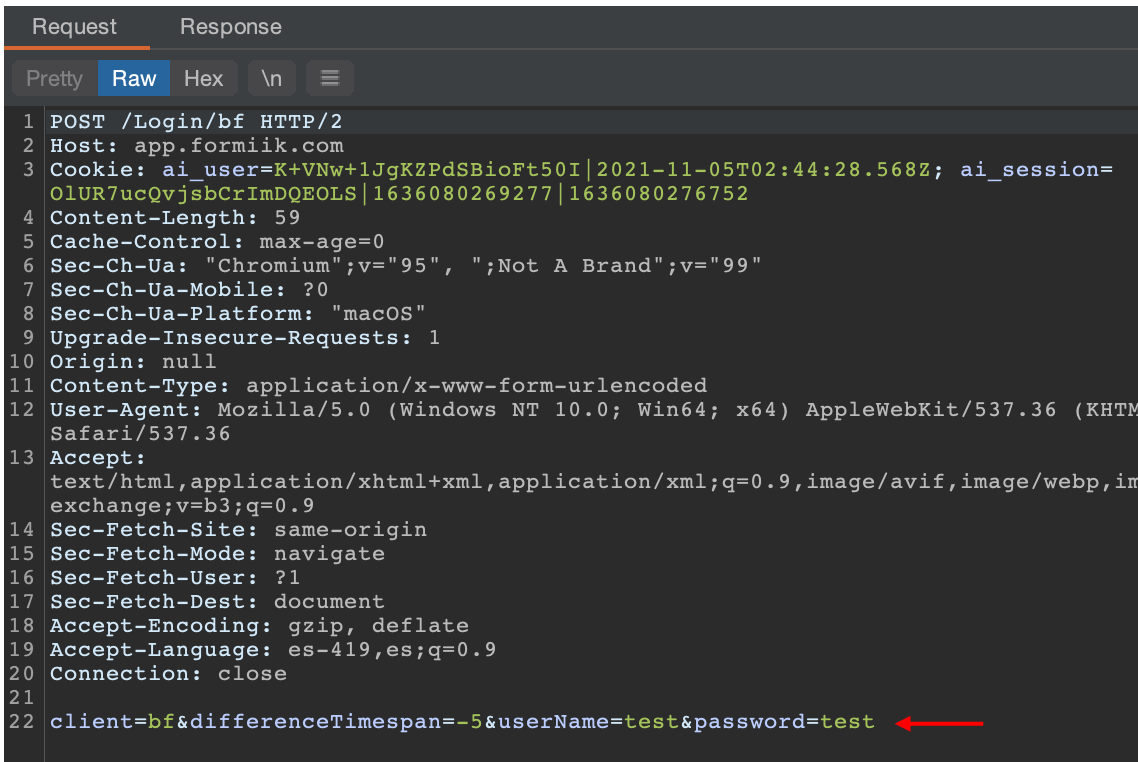
Vulnerabilidad	Autenticación y Administración de identidades		
Código ID	Vuln 07	Riesgo	Medio
Target	https://app.formiik.com		

Resultados de Evaluación

Se valida que el login de la aplicación web a diferencia del APP mobile, no presenta algún tipo de control que evite la visualización del parámetro **password** en texto cifrado o ilegible para un atacante.

Aplicación Formiik

- a) Captura de solicitud en el login del aplicativo Formiik.



```

Request      Response
Pretty  Raw  Hex  \n  ≡
1 POST /Login/bf HTTP/2
2 Host: app.formiik.com
3 Cookie: ai_user=K+VNw+1JgKZPdSBioFt50I|2021-11-05T02:44:28.568Z; ai_session=
  OlUR7ucQvjSbCrImDQEOLS|1636080269277|1636080276752
4 Content-Length: 59
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "macOS"
9 Upgrade-Insecure-Requests: 1
10 Origin: null
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
  Safari/537.36
13 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
  exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Accept-Encoding: gzip, deflate
19 Accept-Language: es-419,es;q=0.9
20 Connection: close
21
22 client=bf&differenceTimespan=-5&userName=test&password=test ←

```



Imagen 01.- Evidencia.

Recomendación

- Implementar métodos de envío de credenciales a través de ofuscación o codificación.

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 20 de 32	

Vulnerabilidad	Ejecución de APK en Emulador		
Código ID	Vuln 08	Riesgo	Medio
Target	APP JARVIS		

Resultados de Evaluación

Se detecta que el aplicativo es posible ejecutarlo en emuladores de Android. Con ello un atacante podría automatizar los ataques y pruebas desde el mismo ordenador con el objetivo de una intrusión exitosa.

Aplicación Formiik Mobile

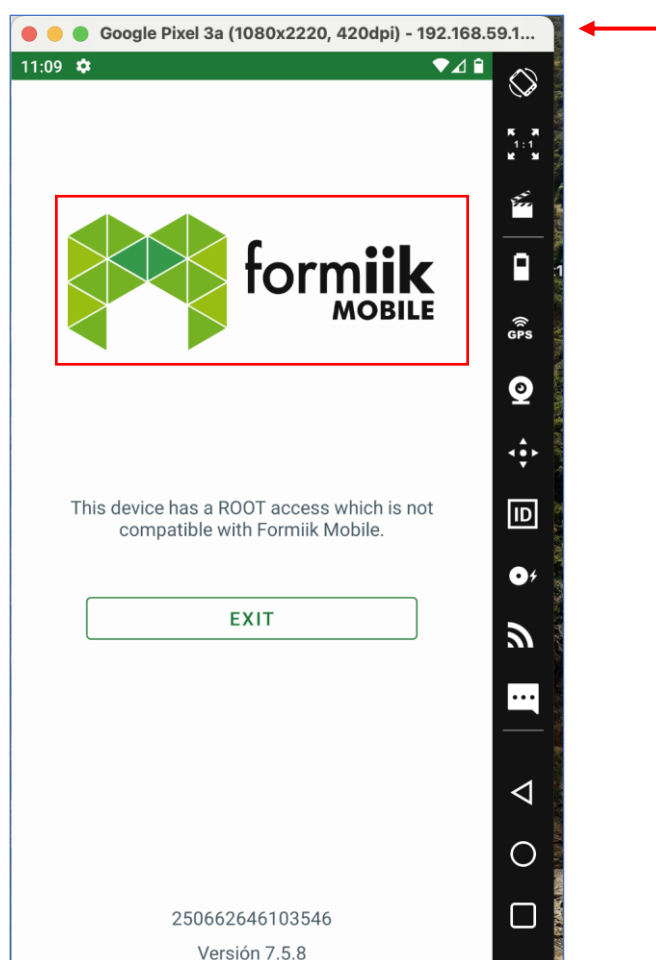




Imagen 01.- Ejecución del App Formiik dentro de un emulador.

Recomendación

- Evitar la ejecución del APP dentro de emuladores en base a la arquitectura de despliegue.

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 21 de 32	

Vulnerabilidad	Brute Force		
Código ID	Vuln 09	Riesgo	Medio
Target	https://app.formiik.com		

Resultados de Evaluación

Se valida que el aplicativo permite realizar múltiples ataques de fuerza bruta dentro del parámetro **userName** sin ningún tipo de bloqueo.

Aplicación Formiik

- a) Se procede a seleccionar el parámetro para realizar el fuzzer.

```

1 POST /Login/bf HTTP/2
2 Host: app.formiik.com
3 Cookie: ai_user=K+VNw+1JgKZPdSBioFt50I|2021-11-05T02:44:28.568Z; ai_session=01UR7ucQvjsbCrI
4 Content-Length: 59
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "macOS"
9 Upgrade-Insecure-Requests: 1
10 Origin: null
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Accept-Encoding: gzip, deflate
19 Accept-Language: es-419,es;q=0.9
20
21 client=bc&differenceTimespan=-5&userName=trc_$juan.santos$&password=$Mibanco2021*
```

Imagen 01.- Parámetro userName.

- b) Se establece una base de posibles usuarios válidos.

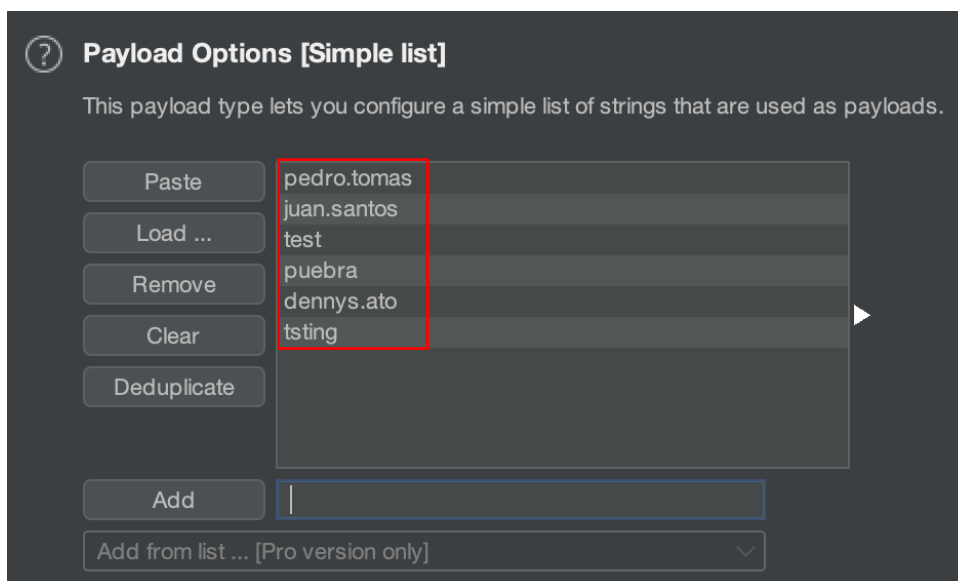




Imagen 02.- Creación de base.

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 22 de 32	

- c) Luego de ingresar los posibles usuarios, se ejecuta el fuzzer y se detecta un cambio en la longitud de respuesta del servidor, con lo cual un atacante podría interpretar esta respuesta como un usuario valido.

Request ^	Payload	Status	Error	Timeout	Length
0		200	<input type="checkbox"/>	<input type="checkbox"/>	10997
1	pedro.tomas	200	<input type="checkbox"/>	<input type="checkbox"/>	10998
2	juan.santos	302	<input type="checkbox"/>	<input type="checkbox"/>	3715
3	test	200	<input type="checkbox"/>	<input type="checkbox"/>	10991
4	puebra	200	<input type="checkbox"/>	<input type="checkbox"/>	10993
5	dennys.ato	302	<input type="checkbox"/>	<input type="checkbox"/>	3735
6	tsting	200	<input type="checkbox"/>	<input type="checkbox"/>	10993

Request

Response

Pretty

Raw

Hex

Render

\n

≡

```

1 HTTP/2 302 Found
2 Cache-Control: private,no-cache; no-store; max-age=0
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: 0
6 Location: /Operation
7 Set-Cookie: frmk=6174CEAFCFB334E16E2CCC67CD6C1DC03A60BD2CA2F996410A7
8 C2E049434D282ADDD8F0BB25881954B9C52C9A471DA9867772F74082BDBFA8DD550F
9 AFC8A1E00A6E90E0AA5A2195B8E98F32F2CDCC3161B8B1689A6449770FFDE416AB9A
10 CC8CDD76A7EE44F4672191EF52DC5C137ACB5B4C05774C3F97CE97B6CDD293E162C8
11 215EDD1D49616ECB3B00824CE45F369DA71DF49BFE503E02160FECF3B11C7EA4FBA6A
12 B8A5B80BC43566142821217A3A0FEC9BDCCFA9DB3B9FB8269BDD3858918667A229740
13
14 Set-Cookie: fcname=bc; path=/; secure; HttpOnly
15 Request-Context: appId=cid-v1:f6e058f7-2ea4-4760-9183-9df1234df52f
16

```

Imagen 03.- Usuario detectado.

- a) Ingreso exitoso con el usuario identificado.

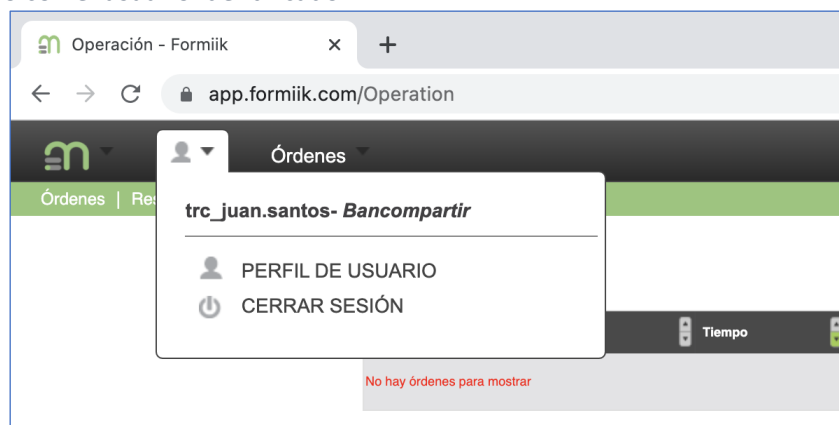




Imagen 04.- Evidencia de acceso.

Recomendación

- Implementar un reCaptcha para evitar múltiples intentos de validación de dominios.

Referencia

- <https://developer.android.com/training/safetynet/recaptcha?hl=es-419>

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 23 de 32	

Vulnerabilidad	Cifrados inseguros implementados		
Código ID	Vuln 10	Riesgo	-
Target	APP JARVIS		

Resultados de Evaluación

Se valida la correcta solución de la vulnerabilidad detectada en un primer informe de Ethical Hacking.

Aplicación Formiik Mobile

```
(kali㉿kali)-[~/Desktop/Tones/testssl.sh]
$ sslscan https://app.formiik.com/
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to 40.113.232.207
Testing SSL server app.formiik.com on port 443 using SNI name app.formiik.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2    enabled
TLSv1.3    disabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported
```



Imagen 01.- Evidencia.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 24 de 32	

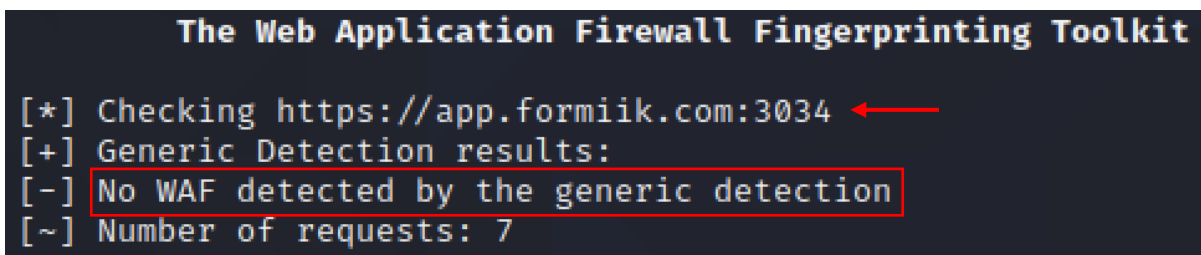
Vulnerabilidad	Ausencia de WAF		
Código ID	Vuln 11	Riesgo	Menor
Target	APP JARVIS		

Resultados de Evaluación

Se detecta que el aplicativo no cuenta con un sistema de seguridad WAF (Web application firewall) que permite detectar posibles manuales como automatizados bloqueando temporalmente el acceso y con ello impidiendo el hackeo exitoso.

Aplicación Formiik Mobile

- a) Validación de WAF.



```

The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://app.formiik.com:3034
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
  
```



Imagen 01.- Evidencia.

Recomendación

- Se debe implementar sistemas de seguridad para identificar y bloquear ataques.

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 25 de 32	

Vulnerabilidad	Detección de IP		
Código ID	Vuln 12	Riesgo	Menor
Target	APP JARVIS		

Resultados de Evaluación

Se detecta que dentro del aplicativo APP no cuenta con un sistema que enmascare la IP desde donde se realizan los request. Este tipo de escenario permite a un atacante realizar distintos tipos de ataque como DDos.

Aplicación Formiik Mobile

a) Validación de direcciones IP.

#	Host ^	Method	URL	Params	Edited	Status	Length	IP
25	https://app.formiik.com	GET	/Scripts/scriptsViews/login/jLoginUser.js			200	2476	40.113.232.207
29	https://app.formiik.com	POST	/Login/bf	✓		200	11013	40.113.232.207
32	https://app.formiik.com	GET	/Content/bootsrapmd/js/mdb.min.js?v...	✓		200	237576	40.113.232.207
33	https://app.formiik.com	GET	/Scripts/scriptsViews/app/jAppCore.js...	✓		200	1056	40.113.232.207
34	https://app.formiik.com	GET	/Content/bootsrapmd/js/vue.min.js?v=...	✓		200	94963	40.113.232.207
35	https://app.formiik.com	GET	/Content/bootsrapmd/js/axios.min.js?v...	✓		200	15164	40.113.232.207
36	https://app.formiik.com	GET	/Scripts/plugins/Utilities/ganalytics.js			200	1877	40.113.232.207
37	https://app.formiik.com	GET	/Scripts/scriptsViews/login/jLoginUser.js			200	2476	40.113.232.207
15	https://dc.services.visualstudio....	OPTIONS	/v2/track			200	309	40.71.12.235
16	https://dc.services.visualstudio....	POST	/v2/track	✓		200	517	40.71.12.235
28	https://dc.services.visualstudio....	POST	/v2/track	✓		200	517	40.71.12.235
41	https://dc.services.visualstudio....	POST	/v2/track	✓		200	517	40.71.12.235



Imagen 01.- Evidencia.

Recomendación

- Emplear un Cloudflare como restricción de consultas directas a las rutas del APP.

Referencia

- <https://www.cloudflare.com/>

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 26 de 32	

Vulnerabilidad	Enumeración de usuarios		
Código ID	Vuln 13	Riesgo	Bajo
Target	APP JARVIS		

Resultados de Evaluación

Se detecta que dentro del aplicativo se logra identificar múltiples usuarios.

Aplicación Formiik Mobile

a) Usuarios dentro del aplicativo.

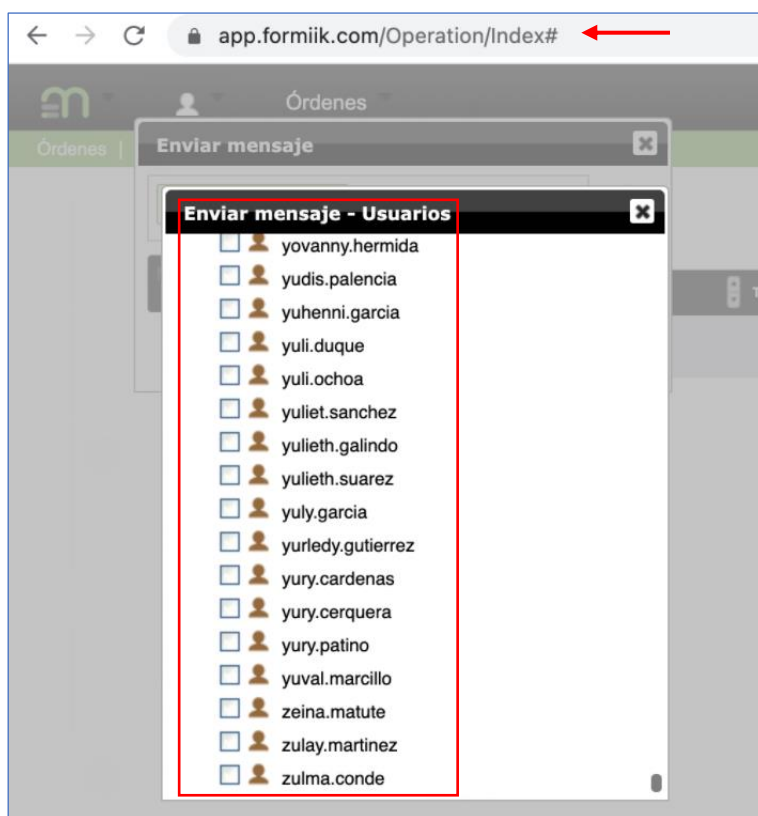




Imagen 01.- Acceso no permitido.

Recomendación

- Validar el acceso a dicha información.

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 28 de 32	

Vulnerabilidad	Errores genéricos		
Código ID	Vuln 15	Riesgo	Bajo
Target	https://app.formiik.com:3034/%7C~.aspx		

Resultados de Evaluación

La ausencia de errores genéricos en una plataforma permite a un atacante validar versiones o respuestas del servidor como punto de partida para futuros ataques.

Aplicación Formiik

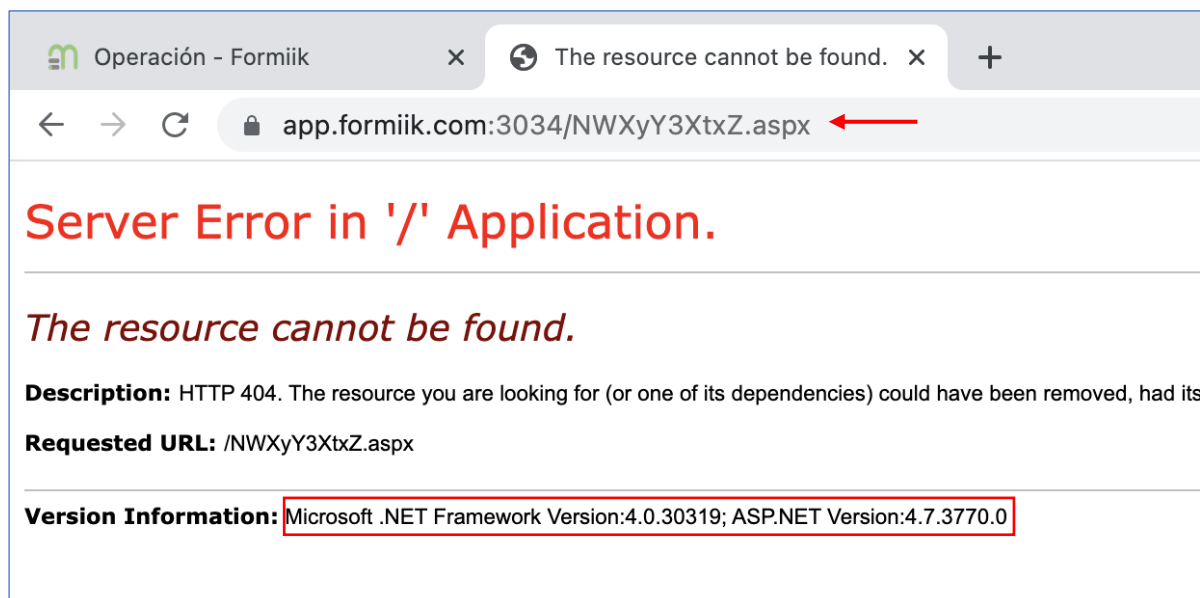




Imagen 01.- Evidencia.


 Operación - Formiik

x
  Illegal characters in path.
 x
 +

←

→

↻

 app.formiik.com:3034/%7C~.aspx

Server Error in '/' Application.

Illegal characters in path.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information.

Exception Details: System.ArgumentException: Illegal characters in path.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception may be available in the stack trace.

Stack Trace:

```
[ArgumentException: Illegal characters in path.]
   System.IO.Path.CheckInvalidPathChars(String path, Boolean checkAdditional)
   System.IO.Path.Combine(String path1, String path2) +50
   System.Web.Compilation.DiskBuildResultCache.GetPreservedDataFileName(String cacheKey)
   System.Web.Compilation.DiskBuildResultCache.GetBuildResult(String cacheKey)
   System.Web.Compilation.BuildManager.GetBuildResultFromCacheInternal(String cacheKey)
   System.Web.Compilation.BuildManager.GetVPathBuildResultFromCacheInternal(VirtualPathRequest request)
   System.Web.Compilation.BuildManager.GetVPathBuildResultInternal(VirtualPathRequest request)
   System.Web.Compilation.BuildManager.GetVPathBuildResultWithNoAssert(HttpContext context, VirtualPathRequest request)
   System.Web.Compilation.BuildManager.GetVirtualPathObjectFactory(VirtualPathRequest request)
   System.Web.Compilation.BuildManager.CreateInstanceFromVirtualPath(VirtualPathRequest request, Type type, String path)
   System.Web.UI.PageHandlerFactory.GetHandlerHelper(HttpContext context, String requestType, String virtualPath)
   System.Web.MaterializeHandlerExecutionStep.System.Web.HttpApplication.IExecuteStep.ExecuteStepImpl() +35
   System.Web.HttpApplication.ExecuteStepImpl(IExecuteStep step) +143
   System.Web.HttpApplication.ExecuteStep(IExecuteStep step, Boolean& completed) +11
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3770.0



Imagen 02.- Evidencia.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 30 de 32	

Vulnerabilidad	Mensajes genéricos		
Código ID	Vuln 16	Riesgo	-
Target	APP JARVIS		

Resultados de Evaluación

Se valida la correcta solución de la vulnerabilidad detectada en un primer informe de Ethical Hacking.

Aplicación Formiik Mobile

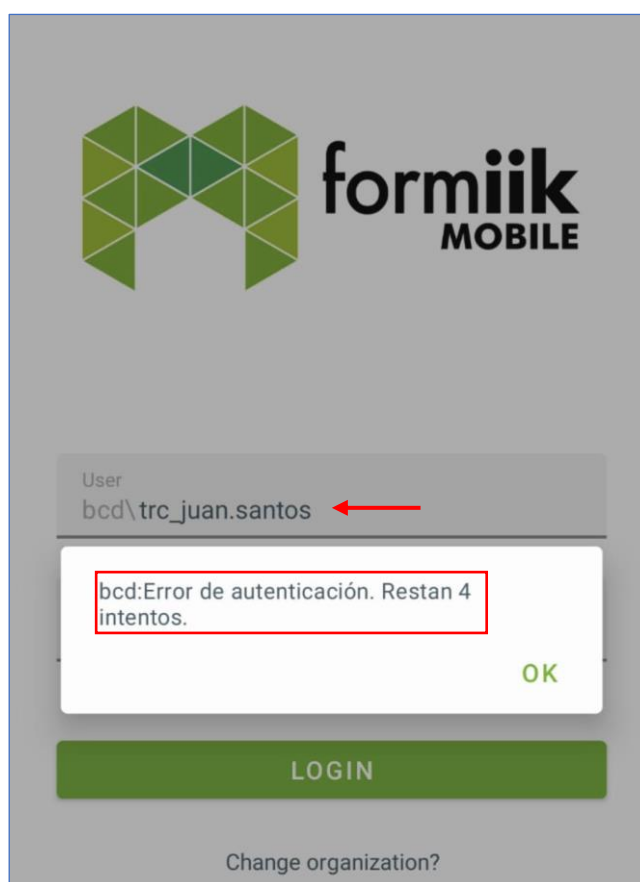




Imagen 01.- Error genérico implementado.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 31 de 32	

Vulnerabilidad	Use of a Broken or Risky Cryptographic Algorithm		
Código ID	Vuln 17	Riesgo	-
Target	APP JARVIS		

Resultados de Evaluación

Se valida la correcta solución de la vulnerabilidad detectada en un primer informe de Ethical Hacking.

Aplicación Formiik Mobile

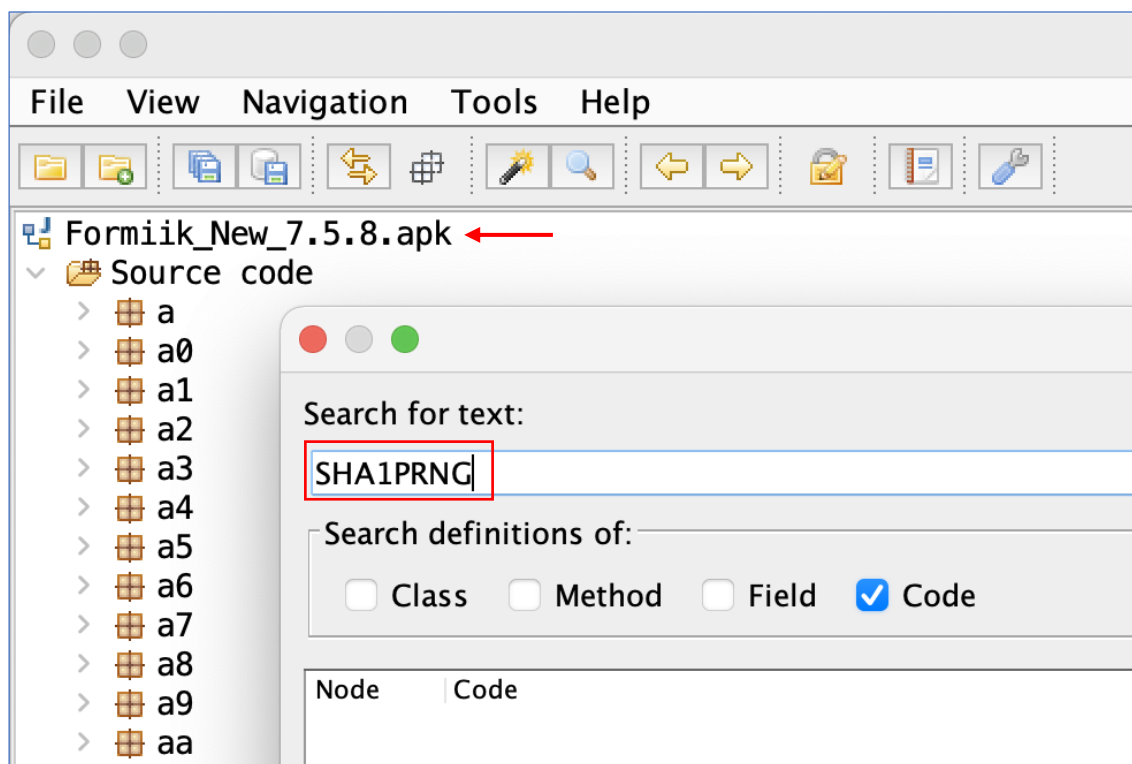




Imagen 01.- Evidencia.

Recomendación

- N/A

Referencia

- [N/A](#)

	Documento:	Informe de Ethical Hacking	Ticket	TISO-2867
	Tema de Análisis:	Análisis Aplicativo Jarvis	Versión	V.2.0
	Elaborado por:	TISO	Fecha	05/11/21
	 Reservada		Página 32 de 32	

7. CONCLUSIONES

- Se valida que el aplicativo aun es vulnerable a un bypass del Root que tiene un nivel de riesgo Crítico.
- Como resultado del retest se determina la solución de 07 vulnerabilidades y 10 persistencias.

8. RECOMENDACIONES

- Evaluar el correcto despliegue de la solución por el bypass del Root en el aplicativo Jarvis ya que si figura un sistema para evitar el ataque; sin embargo, aún persiste.

9. NOMENCLATURA

PoC (Proof Of Concept exploit)

Un ataque contra una computadora o red que se realiza solo para probar que se puede hacer. En general, no causa ningún daño, pero muestra cómo un pirata informático puede aprovechar una vulnerabilidad en el software o posiblemente en el hardware.

Vulnerabilidad

Un error, fallo, debilidad, o exposición de una aplicación, sistema, dispositivo o servicio que podría comprometer la confidencialidad, integridad o disponibilidad del sistema o de la información que trata.

Ocurrencia

Una ocurrencia es la instancia concreta de una vulnerabilidad que afecta a un activo de la organización, facilitando de este modo que no existan repeticiones y homogeneizando las definiciones independientemente del módulo que la detectó.

Activo

Recurso de valor empleado en una empresa u organización.

Amenaza

Se trata de circunstancias o eventos que tienen una probabilidad de ocasionar un daño a un recurso de información al explotar las vulnerabilidades que posea.

Riesgo

Se trata de la probabilidad de que una amenaza explote una vulnerabilidad y pueda ocasionar un daño potencial a los activos de la organización.