telecom

BANCO DE LA NACION ARGENTINA

Pentest (Pruebas de Intrusión)

Informe Técnico

22/05/2025

Tabla de Contenidos

Objetivos 3
Alcance 3
Resumen 4
Hallazgos 5
Detalle de Hallazgos 6
#1 Key Management: Hardcoded Encryption Key 6
#2 Information disclosure 8
#3 Debug Enabled For App 9
#4 Frameable response (potential Clickjacking) 10
#5 LUCKY13 – TLS CBC Timing Side-Channel Attack 12
#6 Data Exposure After Authentication 13
Pruebas de Intrusión ..... **¡Error! Marcador no definido.**
Conclusiones 17
Recomendaciones Generales 18
Actividades Realizadas 19
Anexo 1: Metodología 20
Anexo 2: Herramientas 21
Anexo 3: Clasificación del Riesgo 22

Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Pentest (Pruebas de Intrusión)** sobre la infraestructura de **BANCO DE LA NACION ARGENTINA** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **21/04/2025** y el **05/05/2025**.

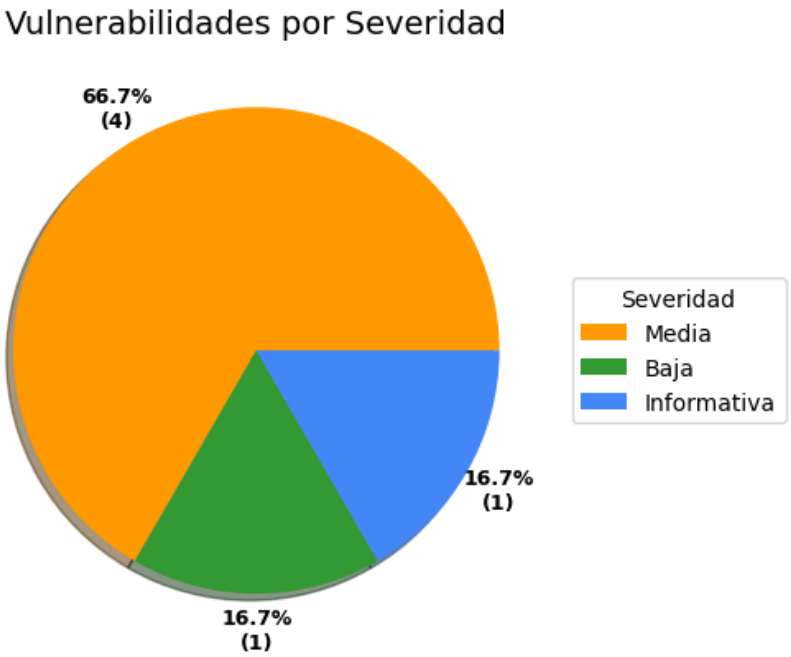
Alcance

Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Pentest (Pruebas de Intrusión).

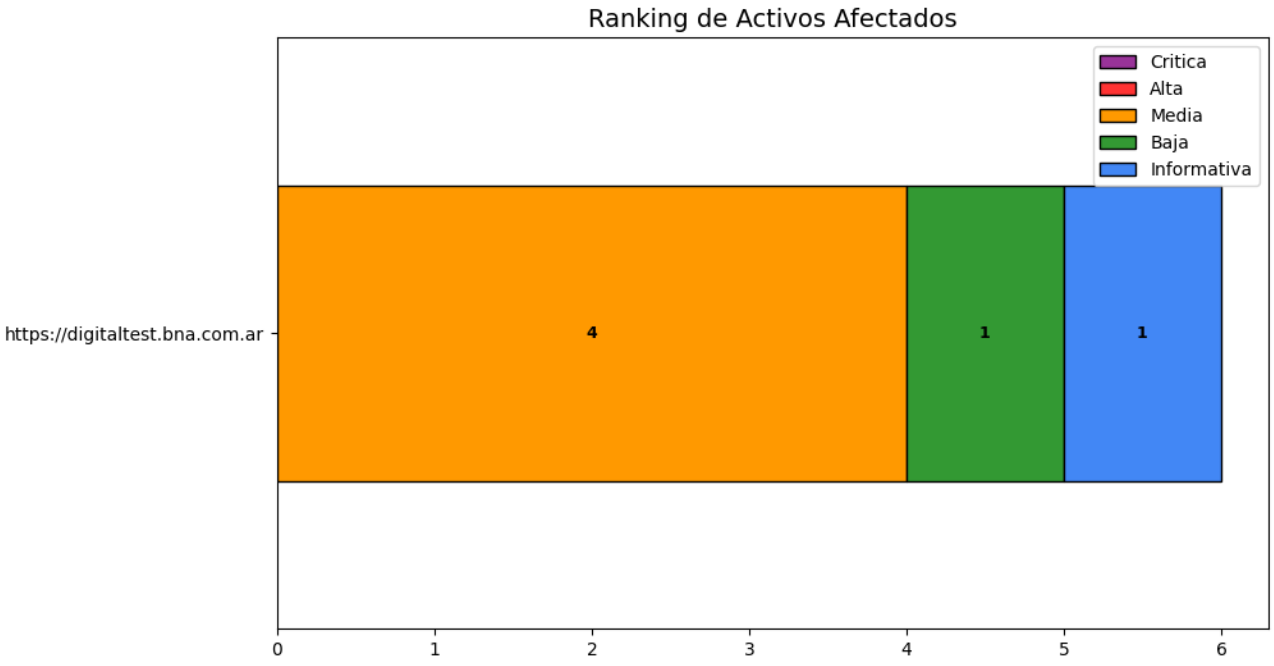
https://digitaltest.bna.com.ar

Resumen

Como resultado del análisis se han identificado **6** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **4** de severidad media, **1** de severidad baja y **1** de carácter informativo. Cada vulnerabilidad identificada en el presente informe incluye una breve descripción, los recursos afectados por la misma junto a las evidencias pertinentes, y recomendaciones de solución y/o mitigación.



En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades detectadas.



Hallazgos

En el siguiente listado se pueden visualizar las vulnerabilidades detectadas en el presente análisis clasificadas por Severidad.

#ID	Nombre	Severidad	Hosts Afectados
#1	Key Management: Hardcoded Encryption Key	**Media**	1
#2	Information disclosure	**Media**	1
#3	Debug Enabled For App	**Media**	1
#4	Frameable response (potential Clickjacking)	**Media**	1
#5	LUCKY13 – TLS CBC Timing Side-Channel Attack	**Baja**	1
#6	Data Exposure After Authentication	**Informativa**	1

Detalle de Hallazgos

#1 Key Management: Hardcoded Encryption Key				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 4.3	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	None
	User Interaction	Required	**Availability Impact**	None

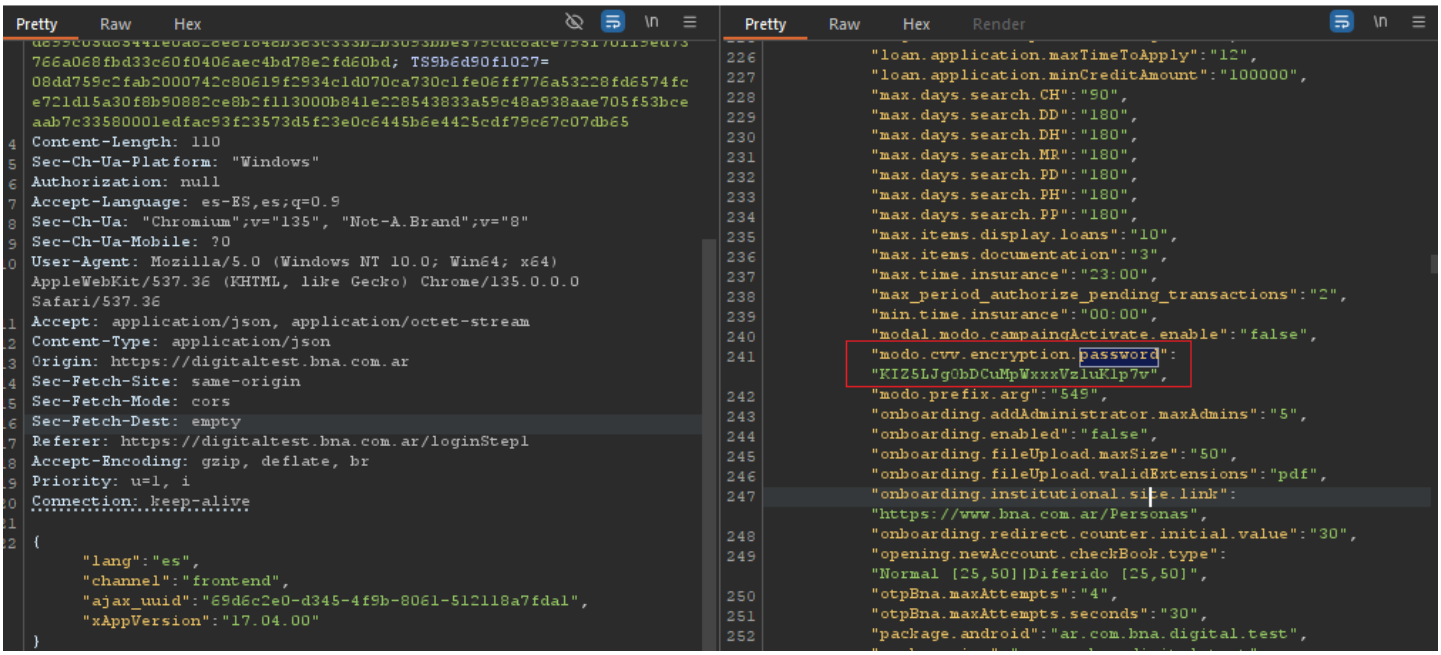
Recursos Afectados
https://digitaltest.bna.com.ar

Descripción
Nunca codifique una clave de cifrado porque hace que la clave de cifrado sea visible para todos los desarrolladores del proyecto y que solucionar el problema sea extremadamente difícil. Para cambiar la clave de cifrado después de que el código esté en producción se necesita una revisión de software. Si la cuenta que protege la clave de cifrado se ve comprometida, el propietario del sistema debe elegir entre seguridad y disponibilidad. Ejemplo 1: El siguiente ejemplo muestra una clave de cifrado dentro de un archivo .pem: ... \-----BEGIN RSA PRIVATE KEY----- MIICXwIBAAKBgQCtVacMo+w+TFOm0p8MlBWvwXtVRpF28V+o0RNPx5x/1TJTlKEl ... DiJPJY2LNBQ7jS685mb6650JdvH8uQl6oeJ/aUmq63o2zOw= \-----END RSA PRIVATE KEY----- ... Cualquiera que tenga acceso al código puede ver la clave de cifrado. Una vez distribuida la aplicación, no hay forma de cambiar la clave de cifrado a menos que se aplique una revisión al programa. Un empleado con acceso a esta información podría utilizarla para irrumpir en el sistema. Cualquier atacante con acceso al ejecutable de la aplicación puede extraer el valor de la clave de cifrado.

Solución
Nunca proteja las claves de cifrado en su sistema de control del código fuente y nunca las codifique de forma rígida. Siempre oculte y administre las claves de cifrado en un origen externo. Almacenar claves de cifrado en texto sin formato en alguna parte del sistema permite que cualquier persona con permisos suficientes lea y pueda usar de forma indebida la clave de cifrado.

Evidencias
Recurso: https://digitaltest.bna.com.ar

Se detectó que la aplicación expone una clave de cifrado (modo.cvv.encryption.password) en una respuesta accesible desde el cliente /api/v1/execute/configuration.listConfiguration. Esta clave se utiliza para cifrar el CVV de tarjetas de crédito, un dato extremadamente sensible.


Pretty
Raw
Hex
Content-Length: 110
Sec-Ch-Ua-Platform: "Windows"
Authorization: null
Accept-Language: es-ES,es;q=0.9
Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0
Safari/537.36
Accept: application/json, application/octet-stream
Content-Type: application/json
Origin: https://digitaltest.bna.com.ar
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://digitaltest.bna.com.ar/loginStep1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{
"lang":"es",
"channel":"frontend",
"ajax_uuid":"69d6c2e0-d345-4f9b-8061-512118a7fda1",
"xAppVersion":"17.04.00"
}
Pretty
Raw
Hex
Render
"loan.application.maxTimeToApply":"12",
"loan.application.minCreditAmount":"100000",
"max.days.search.CH":"90",
"max.days.search.DD":"180",
"max.days.search.DH":"180",
"max.days.search.MR":"180",
"max.days.search.PD":"180",
"max.days.search.PH":"180",
"max.days.search.PP":"180",
"max.items.display.loans":"10",
"max.items.documentation":"3",
"max.time.insurance":"23:00",
"min.time.insurance":"00:00",
"modal.modo.campaingActivate.enable":"false",
"modo.cvv.encryption.password":
"KIZ5LJg0bDCuMpWxxxVzluKlp7v",
"modo.prefix.arg":"549",
"onboarding.addAdministrator.maxAdmins":"5",
"onboarding.enabled":"false",
"onboarding.fileUpload.maxSize":"50",
"onboarding.fileUpload.validExtensions":"pdf",
"onboarding.institutional.site.link":
"https://www.bna.com.ar/Personas",
"onboarding.redirect.counter.initial.value":"30",
"opening.newAccount.checkBook.type":
"Normal [25,50]|Diferido [25,50]",
"otpBna.maxAttempts":"4",
"otpBna.maxAttempts.seconds":"30",
"package.android":"ar.com.bna.digital.test",

#2 Information disclosure				
Severidad: Media	**Attack Vector**	Network	**Scope**	Changed
CVSS: 5.8	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	None
	User Interaction	None	**Availability Impact**	None

Recursos Afectados
https://digitaltest.bna.com.ar

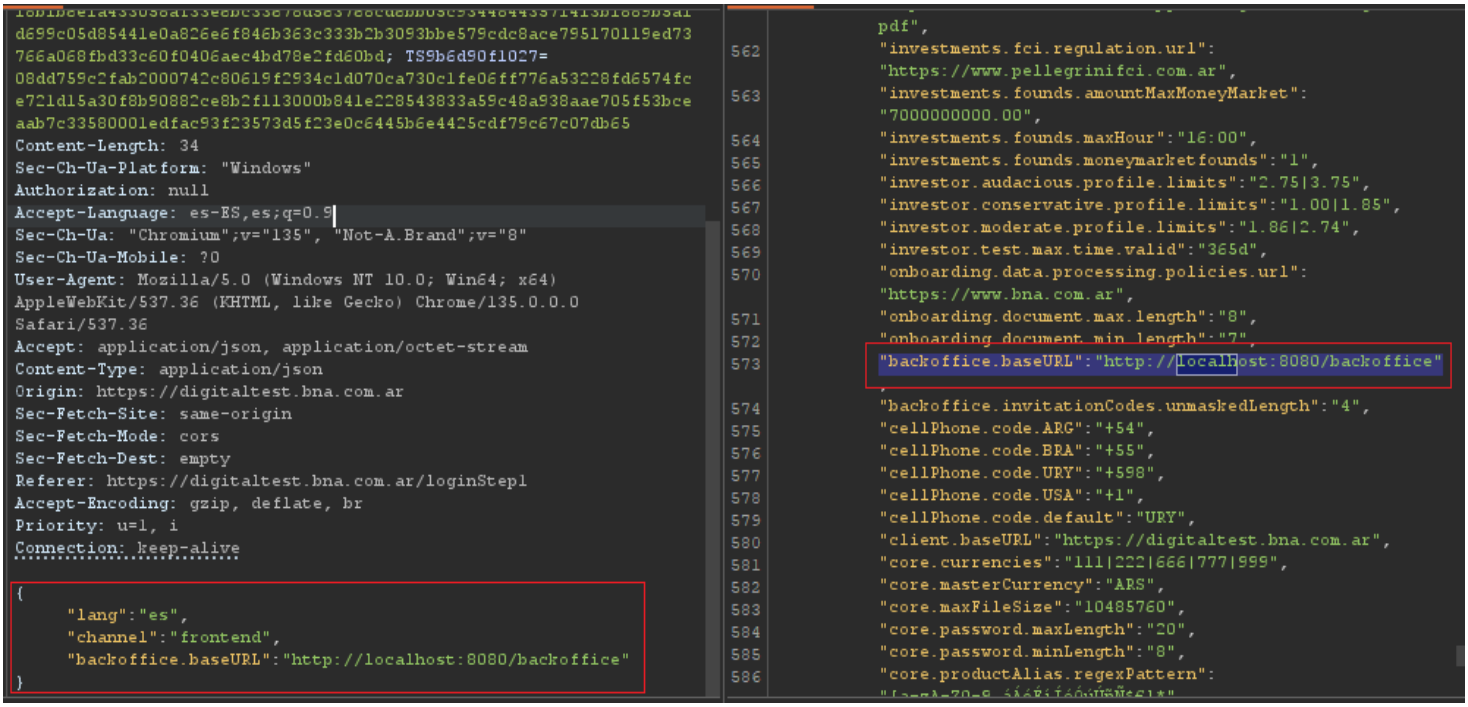
Descripción
Una exposición de información es la divulgación intencionada o no intencionada de información a un actor que no está explícitamente autorizado a tener acceso a este tipo de datos.

Impacto
Esta vulnerabilidad afecta la confidencialidad de la información.

Referencias
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/README
https://cwe.mitre.org/data/definitions/200.html

Solución
Validar la necesidad de contar con dicho activo expuesto a Internet sin autenticación previa, y limitar el acceso en caso de corresponder.

Evidencias
Recurso: https://digitaltest.bna.com.ar



#3 Debug Enabled For App

Severidad: Media
CVSS: 5.5
Ocurrencias: 1

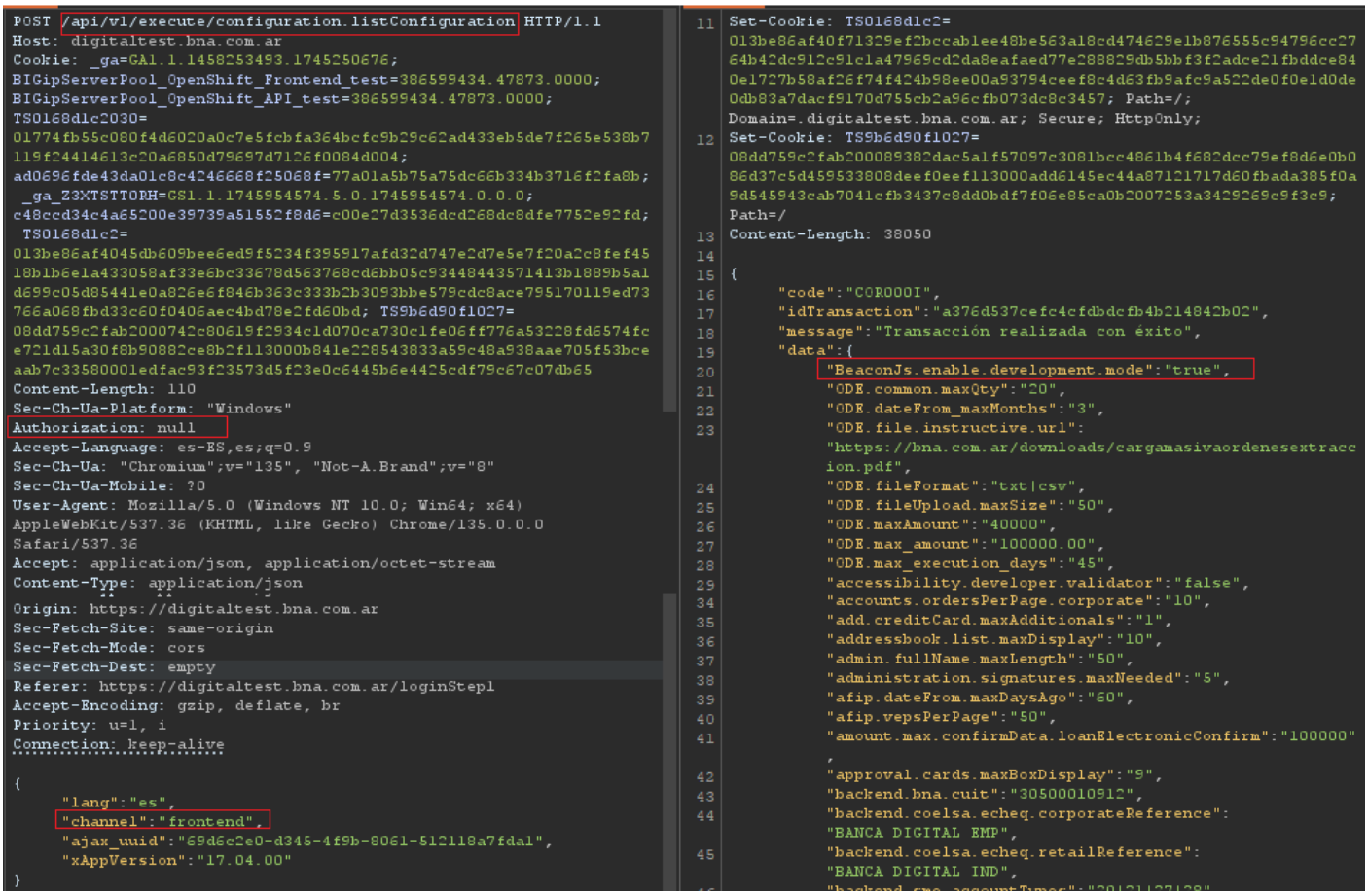
Recursos Afectados
https://digitaltest.bna.com.ar

Descripción
El modo debug se habilitó en la aplicación, esto puede facilitar el procedimiento de ingeniería inversa.

Impacto
Esto puede permitir realizar un seguimiento y acceder a las clases auxiliares de depuración.

Solución
Analizar si es necesario establecer esta opción en true. La recomendación general es establecer la opción de debug a falso ya que por defecto una aplicación no debería estar en modo de depuración.

Evidencias
Recurso: https://digitaltest.bna.com.ar



#4 Frameable response (potential Clickjacking)				
Severidad: Media	**Attack Vector**	Network	**Scope**	Unchanged
CVSS: 5.0	**Attack Complexity**	Low	**Confidentiality Impact**	Low
Ocurrencias: 1	**Privileges Required**	None	**Integrity Impact**	Low
	User Interaction	None	**Availability Impact**	None

Recursos Afectados
https://digitaltest.bna.com.ar/

Descripción
Si una página no establece un encabezado HTTP adecuado X-Frame-Options o Content-Security-Policy, puede ser posible que una página controlada por un atacante la cargue dentro de un iframe. Esto puede permitir un ataque de secuestro de clicks, en el que la página del atacante superpone la interfaz de la aplicación de destino con una interfaz diferente proporcionada por el atacante. Al inducir a los usuarios a realizar acciones tales como clicks de ratón y pulsaciones de teclas, el atacante puede hacer que realicen involuntariamente acciones dentro de la aplicación que está siendo apuntada. Esta técnica permite al atacante eludir las defensas contra la falsificación de solicitud inter-sitio, y puede resultar en acciones no autorizadas.
Tenga en cuenta que algunas aplicaciones intentan evitar estos ataques dentro de la propia página HTML, utilizando el código "framebusting". Sin embargo, este tipo de defensa es normalmente ineficaz y generalmente puede ser eludido por un atacante.
Usted debe determinar si cualquier función accesible dentro de páginas enmarcables puede ser utilizado por los usuarios de aplicaciones para realizar cualquier acción sensible dentro de la aplicación.
Referencias:
  * [X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options)

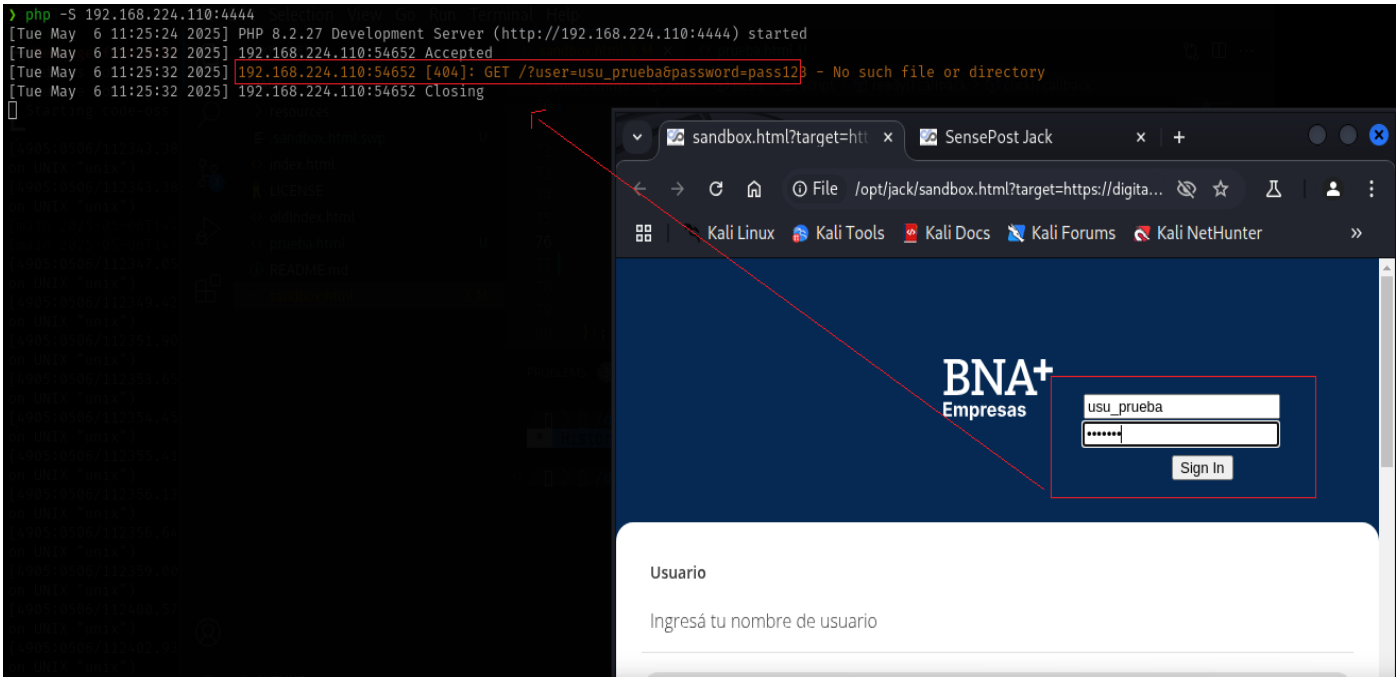
Impacto
* [CWE-693: Mecanismo de protección](https://cwe.mitre.org/data/definitions/693.html)

Referencias
* [Web Security Academy: Clickjacking](https://portswigger.net/web-security/clickjacking)
  * [X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options)

Solución
Para prevenir eficazmente los ataques de framing, la aplicación debe devolver un encabezado de respuesta con el nombre **X-Frame-Options** y el valor **DENY** para evitar el encuadre total, o el valor **SAMEORIGIN** permitir el encuadre sólo por páginas en el mismo origen que la respuesta misma. Tenga en cuenta que el encabezado SAMEORIGIN puede ser eliminado parcialmente si la aplicación en sí puede ser hecha para enmarcar sitios web no confiables.

Evidencias
Recurso: https://digitaltest.bna.com.ar/

```
This issue was found in multiple locations under the reported path.
```


❯ php -S 192.168.224.110:4444
[Tue May 6 11:25:24 2025] PHP 8.2.27 Development Server (http://192.168.224.110:4444) started
[Tue May 6 11:25:32 2025] 192.168.224.110:54652 Accepted
[Tue May 6 11:25:32 2025] 192.168.224.110:54652 [404]: GET /?user=usu_prueba&password=pass123 - No such file or directory
[Tue May 6 11:25:32 2025] 192.168.224.110:54652 Closing
sandbox.html?target=htt
SensePost Jack
File /opt/jack/sandbox.html?target=https://digita...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
BNA+
Empresas
usu_prueba
Sign In
Usuario
Ingresá tu nombre de usuario

#5 LUCKY13 – TLS CBC Timing Side-Channel Attack				
Severidad: Baja	**Access Vector**	Network	**Confidentiality Impact**	Partial
CVSS: 2.6	**Access Complexity**	High	**Integrity Impact**	None
Ocurrencias: 1	**Authentication**	None	**Availability Impact**	None

Recursos Afectados
https://digitaltest.bna.com.ar

Descripción
Los protocolos TLS 1.1 y 1.2 y DTLS 1.0 y 1.2, tal como se usan en OpenSSL, OpenJDK, PolarSSL y otros productos, no consideran adecuadamente los ataques de canal lateral de tiempo en un requisito de verificación MAC durante el procesamiento de relleno CBC malformado, lo que permite a los atacantes remotos realizar ataques de distinción y ataques de recuperación de texto simple a través del análisis estadístico de datos de tiempo para paquetes creados, también conocido como el problema "Lucky Thirteen".

Utiliza cifrados de encadenamiento de bloques (CBC) con TLS.

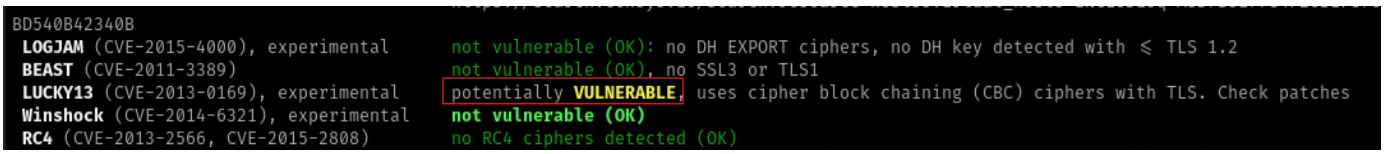
Impacto
Una falla en el manejo de la verificación de respuesta OCSP por parte de OpenSSL puede explotarse en un ataque de denegación de servicio. Todas las versiones de OpenSSL se ven afectadas, incluidas 1.0.1c, 1.0.0j y 0.9.8x

CVEs
https://nvd.nist.gov/vuln/detail/CVE-2013-0169

Referencias
https://openssl-library.org/news/secadv/20130205.txt

Solución
Actualizar la biblioteca OpenSSL del servidor a una versión estable y soportada, posterior a la corrección de LUCKY13

Evidencias
Recurso: https://digitaltest.bna.com.ar



#6 Data Exposure After Authentication
Severidad: Informativa
CVSS: 0.0
Ocurrencias: 1

Recursos Afectados

https://digitaltest.bna.com.ar/loginStep1

Descripción

Durante el análisis se observó que, tras el proceso de autenticación exitoso, ciertas respuestas del servidor contienen información en formato JSON que incluye datos internos de la aplicación o del usuario autenticado (por ejemplo, nombre, ID, token, o similares).
Este comportamiento es esperable en aplicaciones web modernas, donde el cliente (navegador) obtiene los datos tras la autenticación para renderizarlos dinámicamente (por ejemplo, usando JavaScript/AJAX). Sin embargo, se deja constancia informativa para destacar la importancia de:
Minimizar el contenido sensible entregado innecesariamente.
Evitar exponer información innecesaria, incluso autenticado, si no es estrictamente requerida.

Impacto

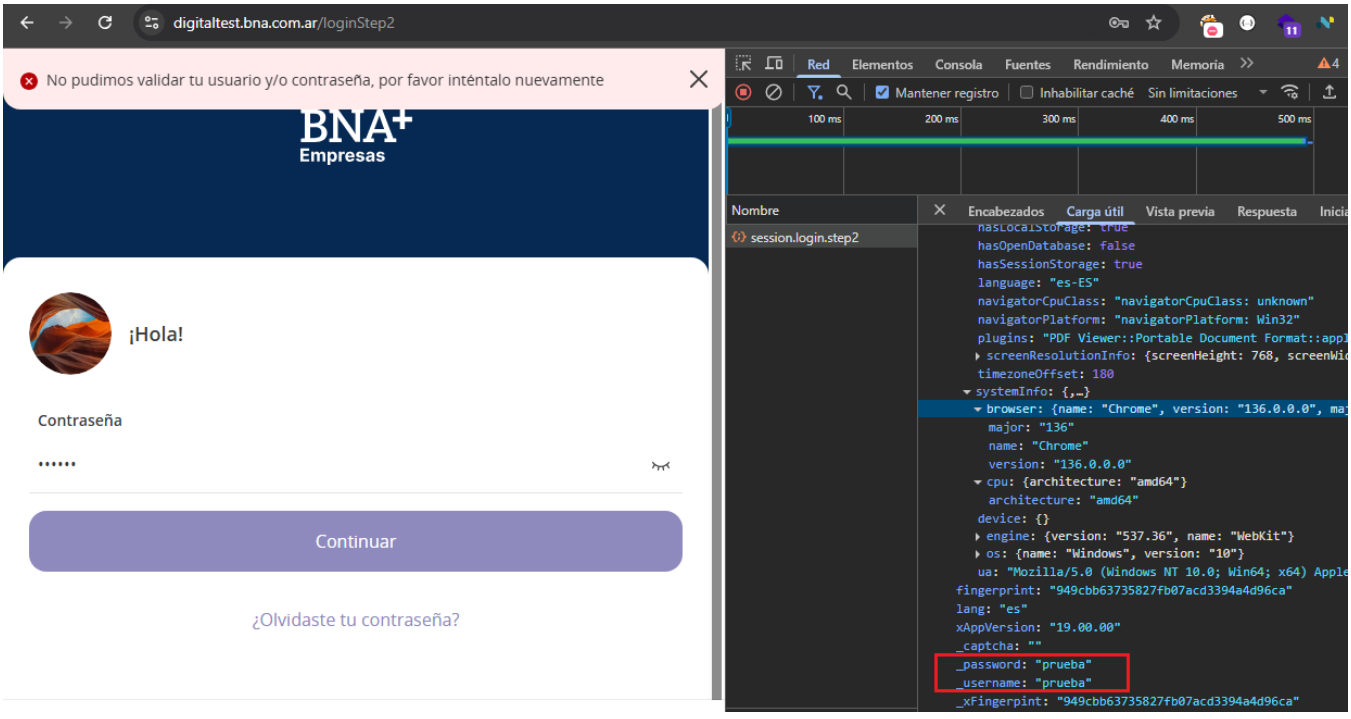
No se detectó acceso a esta información sin autenticación. La entrega de datos ocurre sólo tras el login y dentro de una sesión HTTPS válida, por lo tanto no representa una vulnerabilidad de seguridad activa, pero se documenta como buena práctica de revisión y control de exposición de datos

Solución

Evaluar si los datos devueltos al frontend post-login son estrictamente necesarios.
Aplicar técnicas de minimización u ofuscación si los datos no necesitan mostrarse al usuario.
Evitar exponer objetos completos con estructura interna de la lógica del backend si no es requerido.
Como buena práctica, seguir el principio de “mínima exposición necesaria”.

Evidencias

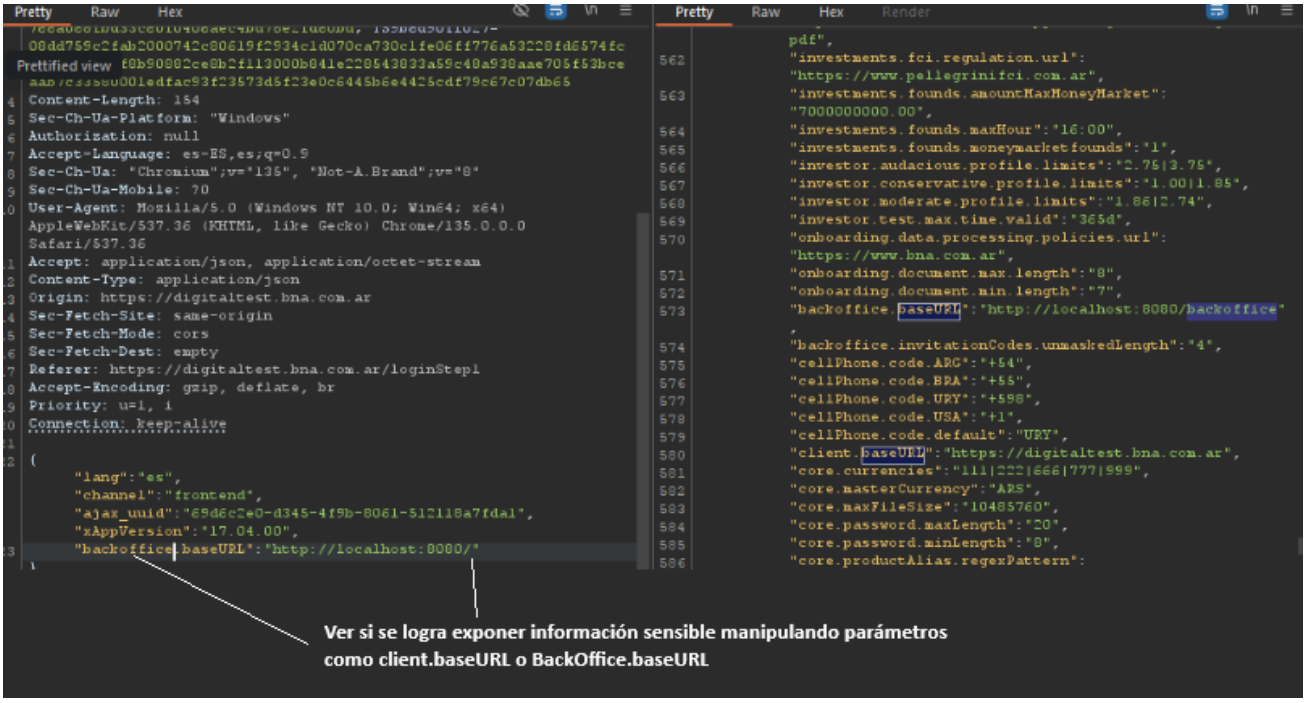
Recurso: https://digitaltest.bna.com.ar/loginStep1



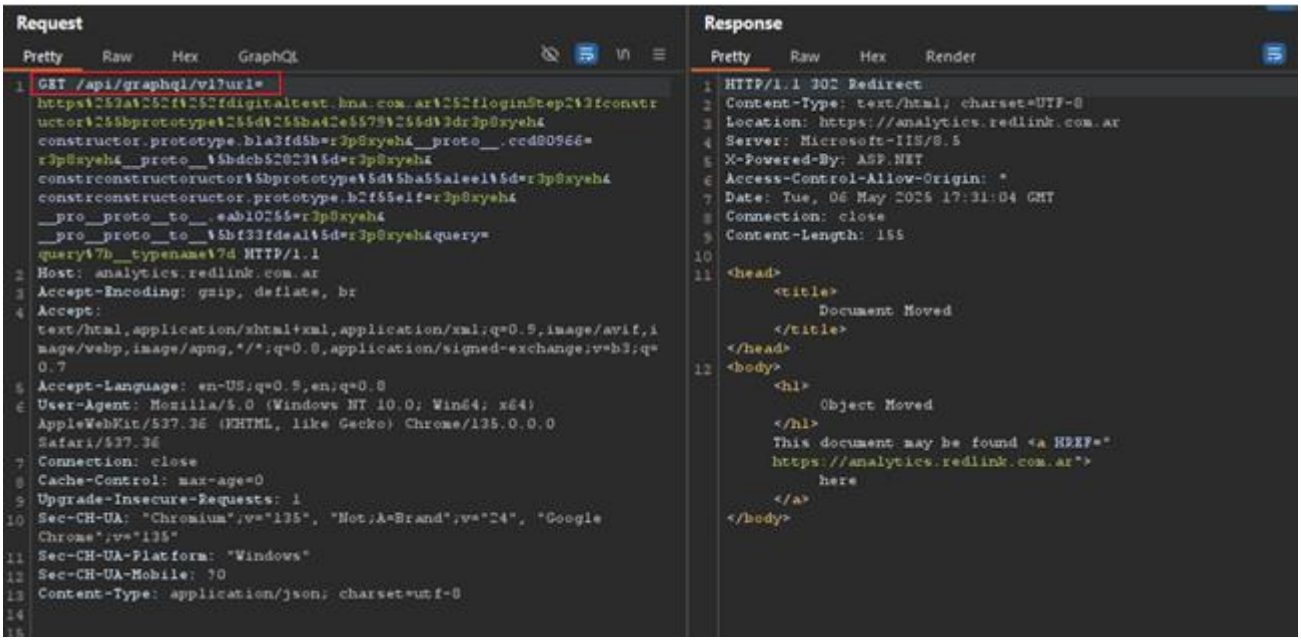
Pruebas de Intrusión

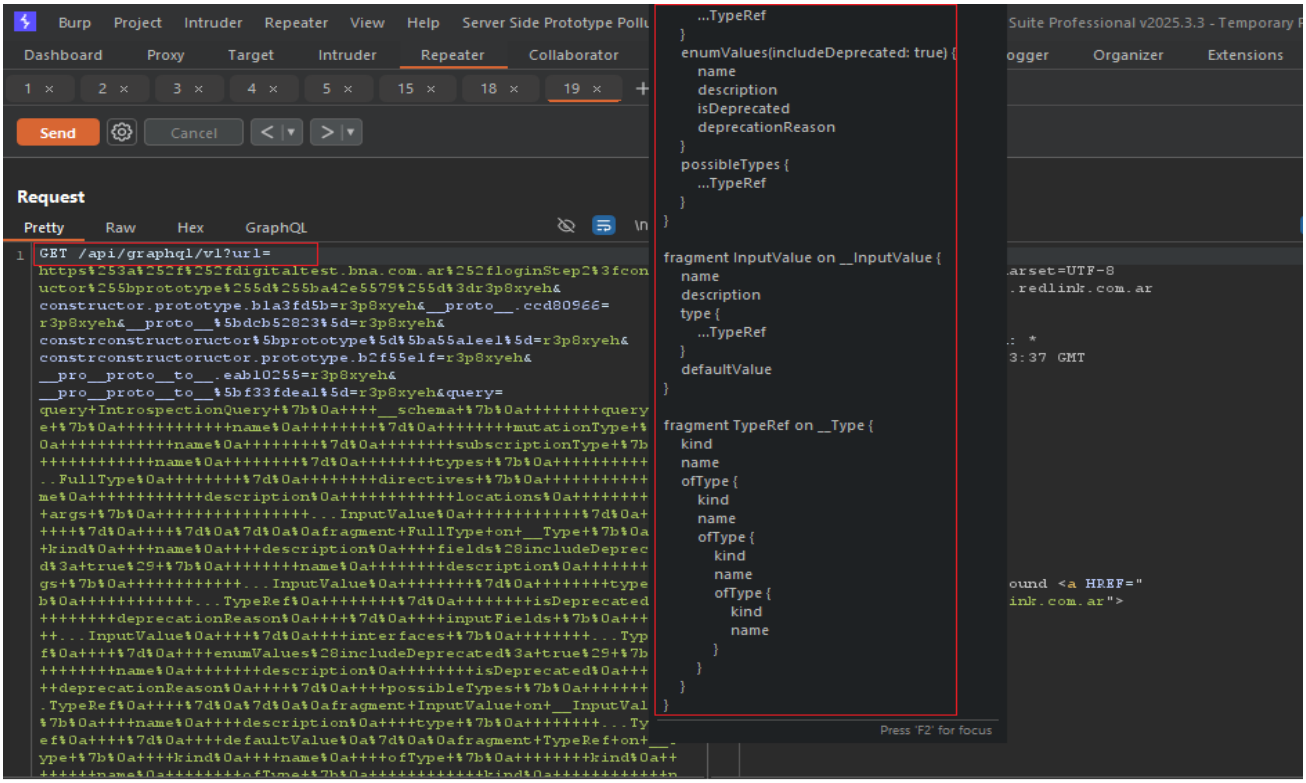
Durante las pruebas de intrusión si bien se llevaron a cabo técnicas manuales de reconocimiento, enumeración y prueba de vectores de ataque en los endpoints identificados.
No fue posible explotarlos o provocar un comportamiento anómalo verificable durante el tiempo disponible para el análisis. Si embargo se detallan algunas pruebas que se realizaron:

1_Manipulación sobre parámetros del cuerpo de la solicitud tomando como base la ruta interna del sistema como client.baseURL, backoffice.baseURL:



2_ Se realiza una consulta especial sobre el endpoint GraphQL para obtener información del esquema completo del backend:






Request
Pretty
Raw
Hex
GET / HTTP/1.1
Host: analytics.redlink.com.ar
Accept-Encoding: gzip, deflate, br
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: "Chromium";v="135", "Not;A=Brand";v="24", "Google Chrome";v="135"
Sec-CH-UA-Platform: "Windows"
Sec-CH-UA-Mobile: ?0
Referer:
https://analytics.redlink.com.ar/api/graphql/v1?url=https%253a%252f%252fdigitaltest.bna.com.ar%252floginStep2%3fconstructor%255bprototype%255d%255ba42e5579%255d%3dr3p8xyeh&constructor.prototype.bla3fd5b=r3p8xyeh&__proto__.ccd80966=r3p8xyeh&__proto__%5bdcb52823%5d=r3p8xyeh&constrconstructoructor%5bprototype%5d%5ba55aleel%5d=r3p8xyeh&constrconstructoructor.prototype.b2f55elf=r3p8xyeh&__pro__proto__to__.eab10255=r3p8xyeh&__pro__proto__to__%5bf33fdeal%5d=r3p8xyeh&query=query%7b__typename%7d
Search
0 highlights
Response
Pretty
Raw
Hex
Render
Sitio en Construcción.

Conclusiones

En base a las vulnerabilidades detectadas y el análisis de las mismas, se puede determinar el siguiente nivel de severidad general, dada la existencia de **4** vulnerabilidades con dicha severidad.

Nivel de Severidad	Media

A continuación se ofrece un listado de acciones recomendadas para mejorar la postura de seguridad del sistema y reducir el riesgo de explotación:

Acciones Recomendadas
Priorizar la remediación según la clasificación de riesgo.
Desarrollar un plan de acción para implementar la recomendación o remediación.
Realizar un análisis de la causa raíz.
Realizar entrenamiento de concientización.
Realizar el manejo de excepciones y la aceptación de riesgos para las vulnerabilidades que no se pueden remediar.
Volver a realizar el análisis de vulnerabilidades para identificar si las soluciones aplicadas son eficaces para remediar las vulnerabilidades expuestas.
Tener en cuenta las soluciones y referencias recomendadas en cada vulnerabilidad expuesta en este informe.

En base a los resultados obtenidos durante el análisis, se ofrecen las siguientes sugerencias de remediación para abordar y mitigar las vulnerabilidades identificadas:

Sugerencia de Remediación	Vulnerabilidad Abordada
Dejar de publicar a Internet servicios que no se encuentren en uso o sean innecesarios.	**#2 Information disclosure**

Recomendaciones Generales

Más allá de los hallazgos obtenidos a través del análisis realizado, resulta crucial establecer un enfoque holístico y multicapa en ciberseguridad. Las recomendaciones que proponemos buscan reforzar su infraestructura de TI y promover una cultura de seguridad resiliente, alineada con las tendencias y prácticas avanzadas del sector, adaptándose así a las dinámicas de un panorama digital que no cesa de cambiar. Recomendamos:

- **Visibilidad, detección y respuesta :** La habilidad para detectar y responder con celeridad a los incidentes de seguridad es fundamental. Contar con un servicio de SOC asegura que esté siempre un paso adelante de los riesgos potenciales.
- **Fortalecimiento de la Infraestructura de Red :** Los puntos débiles identificados en su red pueden fortalecerse de manera significativa a través de Firewalls de última generación y soluciones de seguridad para endpoints. Estas tecnologías son cruciales para una defensa perimetral robusta y ofrecen una protección proactiva contra una variedad de amenazas.
- **Capacitación y Conciencia de Seguridad :** Fomentar la conciencia sobre seguridad entre el personal es esencial, ya que los usuarios informados son la primera línea de defensa. Los programas de formación pueden disminuir de manera significativa el riesgo de brechas de seguridad al educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
- **Análisis Continuo de Vulnerabilidades :** Es vital realizar análisis de vulnerabilidades y pruebas de penetración de forma regular para identificar y mitigar proactivamente las nuevas vulnerabilidades. Esta práctica garantiza la solidez y la adaptabilidad de su infraestructura frente a las amenazas emergentes.
- **Evaluaciones regulares :** Es vital realizar evaluaciones regulares, mantener la seguridad operativa de las plataformas y hardening de los firewalls para protección contra intrusiones. El cumplimiento de los estándares de seguridad es esencial, al igual que revisar los controles de seguridad IT y practicar una gobernanza y gestión de riesgos efectivas. Además, planes de crisis preparados son clave para una respuesta ágil y minimizar impactos en el negocio. Finalmente, tener planes de gestión de crisis bien desarrollados y probados asegura una respuesta rápida y eficaz ante incidentes imprevistos, mitigando los daños y preservando la continuidad del negocio.

Estas recomendaciones están pensadas para ser integradas dentro de un enfoque estratégico de seguridad, garantizando que no solo se atiendan los puntos débiles actuales, sino que también se establezca una base sólida para la seguridad futura. Nuestro equipo de expertos en ciberseguridad está listo para asesorar y apoyar la implementación de estas soluciones, asegurando que su empresa se mantenga a la vanguardia en protección y cumplimiento.
En Telecom, entendemos los desafíos intrincados de la ciberseguridad y estamos equipados para apoyar su empresa en cada paso del camino. Con nuestro portafolio integral y un equipo de profesionales experimentados, nos dedicamos a ayudarlo a alcanzar y mantener una postura de seguridad que no solo responda a las amenazas actuales, sino que también se anticipe y adapte a los riesgos del mañana.

Actividades Realizadas

Las actividades que se realizaron para el presente análisis se separaron en las etapas descriptas a continuación:

Etapa 1: Reconocimiento y Enumeración

En esta etapa se recopiló información sobre los activos informados en el alcance, incluyendo la identificación de rangos de IP, dominios, servidores, y cualquier información pública disponible. La enumeración implica descubrir y mapear activos, servicios y aplicaciones en la red para conformar la superficie de ataque. También se utilizó inteligencia de fuentes abiertas (OSINT) para complementar y ampliar la información obtenida.

Etapa 2: Análisis de Vulnerabilidades

Se utilizaron diferentes herramientas de análisis manual para identificar y evaluar los servicios brindados y el tráfico de red en el sistema objetivo. Este proceso puede incluir análisis de código, análisis de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.

A continuación se listan algunas de las debilidades buscadas, sin ser el presente un listado exhaustivo:

- Detección de vulnerabilidades conocidas asociadas a la versión de software de los servicios instalados.
- Verificación de vulnerabilidades conocidas sobre el sistema operativo de base instalado.
- Detección de falta de actualizaciones (parches).
- Detección de errores de configuración o configuraciones predeterminadas.
- Utilización de algoritmos de cifrado inseguros, o ausencia de cifrado.
- Exposición de información.
- Tratamiento incorrecto de entradas manipuladas por el usuario (XSS, Inyección de comandos o código, etc)
- Detección de falencias en el proceso de autenticación.
- Errores en manejo de sesiones de usuario.
- Posibilidad de generar ataques de fuerza bruta.
- Credenciales predeterminadas o conocidas.
- Control de acceso inadecuado o inexistente.

Etapa 3: Modelado de Amenazas

Se utilizaron todos los datos recopilados en las fases anteriores para determinar la posibilidad de explotación. Se determinó el riesgo de las vulnerabilidades descubiertas durante esta fase utilizando principalmente la National Vulnerability Database (NVD), creada y mantenida por el gobierno de EE.UU. que analiza las vulnerabilidades de software publicadas en la base de datos Common Vulnerabilities and Exposures (CVE). La NVD clasifica la gravedad de las vulnerabilidades utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS). Esta etapa se complementó con verificaciones manuales sobre estos equipos a fin de eliminar los “falsos positivos” y corroborar las detecciones.

Etapa 4: Explotación

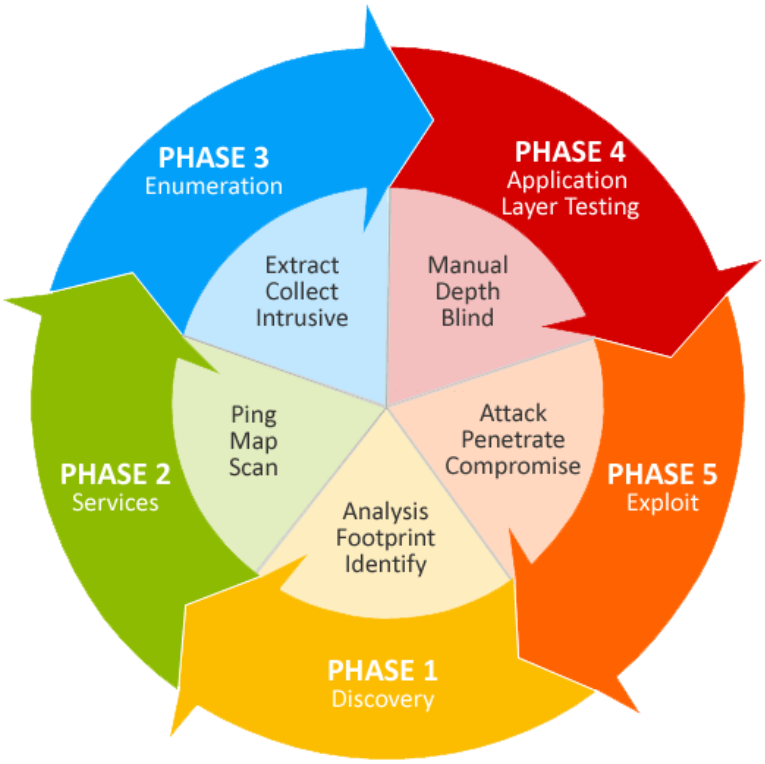
En esta etapa se intentaron explotar las vulnerabilidades identificadas para evaluar la resistencia del sistema a ataques reales. Se buscó determinar si las contramedidas de seguridad eran efectivas y si las vulnerabilidades podían ser explotadas con éxito para validar la profundidad y el alcance de las mismas.

Etapa 5: Informes

Una vez finalizadas las etapas de análisis, se generó un informe ejecutivo con un resumen gerencial de los hallazgos y equipos detectados, junto a un informe técnico donde se describen las vulnerabilidades, detallando el nivel de riesgo asociado, el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información adicional que fuera considerada útil para su identificación y corrección.

Anexo 1: Metodología

El enfoque utilizado se basa en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), e incluye una combinación de pruebas automatizadas (cuando es posible) y de inspección manual (cuando sea necesario) de los servicios expuestos. El OSSTMM es un estándar ampliamente reconocido y utilizado en la industria de la seguridad informática. Fue desarrollado y publicado inicialmente por el ISECOM (Institute for Security and Open Methodologies) en el año 2001. Proporciona un marco completo y estructurado para llevar a cabo pruebas de penetración y evaluación de la seguridad en sistemas, redes y aplicaciones.



OSSTMM proporciona una serie de escenarios de prueba, técnicas y herramientas para realizar evaluaciones exhaustivas de seguridad. Está diseñado para ser utilizado por profesionales de la seguridad, equipos de pruebas de penetración y auditores de seguridad para identificar vulnerabilidades, evaluar la efectividad de las políticas de seguridad y proporcionar recomendaciones para fortalecer la infraestructura de una organización. Gracias a su enfoque cuantitativo y en detalle, el OSSTMM ha sido adoptado por muchas empresas y organizaciones como una metodología confiable para mejorar la seguridad informática y proteger los activos críticos.

Por requerimiento del cliente, las pruebas debieron ejecutarse de manera manual, lo que limitó el uso de herramientas automatizadas o escaneos extensivos. Asimismo, si bien inicialmente se proporcionaron credenciales para la evaluación bajo un enfoque Gray Box, dichas credenciales dejaron de funcionar durante el transcurso del proyecto. Debido a ello, se continuó la ejecución bajo una modalidad Black Box.

Anexo 2: Herramientas

Durante el presente análisis se utilizó un conjunto de herramientas manuales especializadas que nos permiten evaluar la seguridad de sistemas y redes. Se presenta un listado no exhaustivo de las mismas:

- Burp Suite: Suite de herramientas para pruebas de seguridad de aplicaciones web, incluyendo escaneo de vulnerabilidades y manipulación de solicitudes y respuestas.
- Nmap: Herramienta de escaneo de red utilizada para descubrir hosts y servicios, así como para evaluar la seguridad y configuración de los dispositivos conectados.
- Programas internos: Scripts desarrollados por el área de Ethical Hacking para efectuar el análisis de determinadas configuraciones y confirmar vulnerabilidades encontradas.

Anexo 3: Clasificación del Riesgo

La evaluación de cada vulnerabilidad se calcula a través del CVSS (Common Vulnerability Scoring System). CVSS es un sistema estandarizado y de código abierto utilizado para evaluar y clasificar la gravedad de las vulnerabilidades informáticas. Fue desarrollado para proporcionar una medida cuantitativa y objetiva de la severidad de una vulnerabilidad, ayudando a los equipos de seguridad a priorizar las acciones de mitigación, lo que permite una respuesta más efectiva y coordinada ante posibles amenazas.
El CVSS se compone de un conjunto de métricas que consideran diferentes aspectos de la vulnerabilidad:

AV: Attack Vector
Representa cómo un atacante podría explotar la vulnerabilidad

- AV:N (Network) : El ataque se realiza a través de la red (por ejemplo Internet).
- AV:A (Adjacent) : El ataque se realiza desde una red adyacente (por ejemplo, una red local).
- AV:L (Local) : El ataque se realiza de manera local en el sistema afectado.
- AV:P (Physical) : El atacante necesita acceso físico al sistema para explotar la vulnerabilidad.

AC: Attack Complexity
Describe la complejidad del ataque necesario para explotar la vulnerabilidad.

- AC:L (Low) : El ataque es sencillo y no requiere condiciones especiales.
- AC:H (High) : El ataque es complicado y puede requerir condiciones adicionales o conocimientos técnicos específicos.

PR: Privileges Required
Indica los privilegios previos necesarios para explotar la vulnerabilidad.

- PR:N (None) : No se requieren privilegios adicionales para explotar la vulnerabilidad.
- PR:L (Low) : Se requieren privilegios limitados (por ejemplo, acceso de usuario).
- PR:H (High) : Se requieren privilegios elevados (por ejemplo, acceso de administrador).

UI: User Interaction
Describe si la explotación de la vulnerabilidad requiere la interacción de un usuario del sistema afectado.

- UI:N (None) : No se requiere interacción de un usuario para explotar la vulnerabilidad
- UI:R (Required) : Se requiere la interacción activa de un usuario para que el ataque tenga éxito.

S: Scope
Indica el alcance de la vulnerabilidad.

- S:U (Unchanged) : La vulnerabilidad solo afecta a los recursos directamente afectados por la explotación.
- S:C (Changed) : La vulnerabilidad afecta a componentes adicionales o recursos controlados por el mismo autor del ataque.

C: Confidentiality Impact
Describe el impacto de la vulnerabilidad en la confidencialidad de los datos.

- C:N (None) : No hay impacto en la confidencialidad. La vulnerabilidad no afecta la confidencialidad de los datos.
- C:L (Low) : El impacto en la confidencialidad es bajo. La explotación de la vulnerabilidad podría resultar en la divulgación limitada de información sensible o datos confidenciales.
- C:H (High) : El impacto en la confidencialidad es alto. La explotación de la vulnerabilidad podría resultar en la divulgación significativa o completa de información sensible o datos confidenciales.

I: Integrity Impact
Indica el impacto de la vulnerabilidad en la integridad de los datos.

- I:N (None) : No hay impacto en la integridad. La vulnerabilidad no afecta la integridad de los datos.
- I:L (Low) : El impacto en la integridad es bajo. La explotación de la vulnerabilidad podría resultar en una alteración limitada o superficial de los datos o información del sistema.
- I:H (High) : El impacto en la integridad es alto. La explotación de la vulnerabilidad podría resultar en una alteración significativa o completa de los datos o información del sistema.

A: Availability Impact
Describe el impacto de la vulnerabilidad en la disponibilidad de los recursos.

- A:N (None) : No hay impacto en la disponibilidad. La vulnerabilidad no afecta la disponibilidad de los recursos o servicios.
- A:L (Low) : El impacto en la disponibilidad es bajo. La explotación de la vulnerabilidad podría resultar en una degradación temporal o parcial de los recursos o servicios.
- A:H (High) : El impacto en la disponibilidad es alto. La explotación de la vulnerabilidad podría resultar en una interrupción completa o prolongada de los recursos o servicios, afectando significativamente su disponibilidad.