
CONSULTING

UBIQUO

INFORME EJECUTIVO DE ANÁLISIS DE PRUEBAS DE SEGURIDAD INFORMÁTICA

Índice

ES CONSULTING

ES Consulting cuenta con más de 16 años de experiencia en servicios de consultoría relacionados con Estrategia Empresarial, Calidad, Seguridad de la Información, Seguridad Informática, Continuidad de Negocios, Servicios de TI, entre otros.

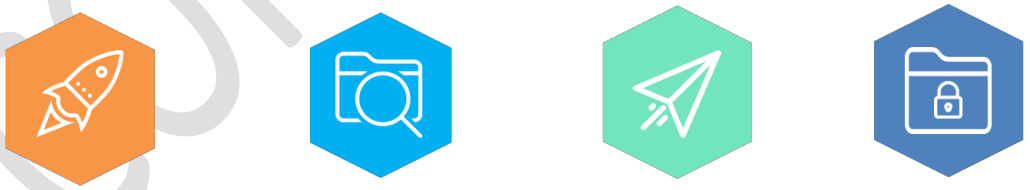
En estos años hemos formado un grupo de profesionales expertos en nuestras diferentes líneas de servicios, con el fin de responder a la necesidad de soluciones tecnológicas, de protección de la información e infraestructura tecnológica de las organizaciones. Ofreciendo una protección integral a las organizaciones y siempre a la vanguardia de la tecnología, integrando productos y servicios que permite a nuestros clientes tener un ritmo de innovación acelerado sin descuidar la seguridad de su información e infraestructura tecnológica.

Hemos apoyado a diferentes entidades financieras, sector de gobierno e industrias manufactureras, inmobiliarias, hoteleras, energéticas tanto a nivel nacional como internacional, a quienes proveemos de soluciones y servicios tecnológicos y de seguridad de la información.

SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA

Contamos con un equipo de consultores profesionales altamente calificados y capacitados, certificados bajo normas internacionales, que son aceptadas como los marcos de referencia ISO, y los de industria, como CISSP del (ISC)2, CISA, COBIT, entre otras.

Contamos con alianzas estratégicas con firmas internacionales en el ámbito de la Seguridad y capacidad instalada de profesionales en todas las regiones que garantizan nuestra capacidad de brindar a nuestros clientes asesoría y consultoría profesional de seguridad informática y de la Información; desde un enfoque sistémico y procesal; es decir, que involucra ya no únicamente infraestructura y soluciones de productos de Tecnología de la Información, sino también Procesos y Personas



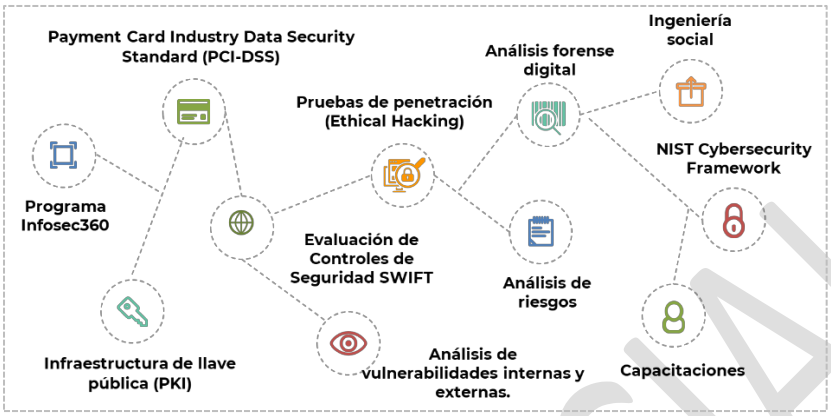
Business Excellence
Estrategia Corporativa

Seguridad de la Información
Sistemas de Gestión como ISO y estándares.

Efectividad Operacional
Gestion de Productividad .

Seguridad Informática
Cybersecurity

Algunos de nuestros servicios:



Todos los servicios son basados en metodologías internacionales y reconocidas como Códigos de Mejores Prácticas. Contamos con talento certificado como CISSP del (ISC)[2]; CISA de ISAC; Auditores Líder de ISO27001; OPST de OSSTMM; Microsoft; CISCO CCNA y CCNP; Checkpoint CCSA y CCSE; PCI-DSS; entre otras.

PROPÓSITO

El objetivo principal del análisis de vulnerabilidades es detectar las posibles brechas de seguridad que existen en los sistemas de información. Las vulnerabilidades detectadas son riesgos que deben ser mitigados.

BENEFICIOS

Nuestra organización se distingue por realizar las Pruebas de Seguridad evaluando la gente, procesos, tecnología, controles técnicos y administrativos. Nuestro método es exhaustivo y por lo tanto más certero.

- Se determina la factibilidad real de un ataque y su impacto en el negocio.
- Provee la información necesaria para enfocar la implementación de controles de seguridad y mitigar los riesgos descubiertos.
- Eleva la conciencia de la alta gerencia acerca de la seguridad de la información.

ALCANCE DE LAS PRUEBAS

OBJETIVOS WEB

URL
https://notificame.claro.com.gt/

FASES DEL ANÁLISIS DE VULNERABILIDADES

FASE 1: RECONOCIMIENTO

Esta fase consta de Identificar y obtener información acerca de los posibles riesgos dentro del alcance, recopilación y descubrimiento de información (topología de red, direcciones IP, correos electrónicos, etc.), además de identificar y obtener información sobre los posibles riesgos, en este caso se realizó un documento de Excel en cual se detalla los puertos abiertos y los servicios activos por host.

FASE 2: ANÁLISIS DE VULNERABILIDADES

Por medio de herramientas especializadas en análisis de vulnerabilidades, se realizó un análisis de cada una de las redes dentro del alcance con el fin de identificar los riesgos sobre las aplicaciones y servicios que soportan estas.

Dominios de análisis:

- Seguridad de Aplicaciones
- Control de Acceso
- Seguridad de Red
- Seguridad de Sistemas Operativos
- Manejo de Usuarios

METODOLOGÍA

La metodología CVSS considera tres áreas de evaluación:

- Métricas Base
- Métricas Temporales
- Métricas Ambientales

La métrica base representa las características intrínsecas de la vulnerabilidad evaluada y se conforma de la explotabilidad y el impacto de esa vulnerabilidad. La métrica temporal representa las características de una vulnerabilidad que pueden cambiar con el tiempo; éstas incluyen la madurez del código explotable, las remediaciones disponibles y la seguridad de la existencia de la vulnerabilidad. Finalmente, la métrica ambiental representa las características de la vulnerabilidad que son particulares al ambiente del usuario, ésta métrica consiste en ajustar la métrica base según necesidad particular de la organización. Ver el siguiente cuadro para descripción de los criterios:

		Descripción	
Criterio	**Valoración**	**Métrica Base**	**Métrica Temporal**
Bajo	0.1 – 3.9	El atacante puede explotar la vulnerabilidad únicamente con acceso local y no por medios remotos o adyacentes, la vulnerabilidad es muy compleja y el atacante necesita un gran nivel de conocimiento para explotarla, el atacante necesita un perfil con permisos privilegiados para poder explotar la vulnerabilidad, el atacante necesita una interacción con el usuario significativa para poder explotar la vulnerabilidad. La vulnerabilidad, en caso sea explotada, no afecta otros recursos negativamente.	La Vulnerabilidad no es madura y muy pocas personas la conocen por lo que se reduce el número de atacantes potenciales, la vulnerabilidad cuenta con remediaciones oficiales y fáciles de aplicar, la vulnerabilidad no ha sido validad por fuentes confiables
Medio	4.0 – 6.9	El atacante puede explotar la vulnerabilidad por redes adyacentes lo cual incrementa la cantidad de potenciales atacantes, la vulnerabilidad tiene un nivel de complejidad medio y el atacante necesita más conocimiento de lo normal para poder explotarla, el atacante requiere un nivel medio de permisos para explotar la vulnerabilidad, el atacante necesita una interacción con el usuario mínima para poder explotar la vulnerabilidad. La vulnerabilidad, en caso sea explotada, podría afectar a otros recursos negativamente. La vulnerabilidad si es explotada tiene algún impacto negativo en la	Si existe conocimiento sobre la vulnerabilidad y hay una mayor posibilidad de atacantes, hay algunas remediaciones disponibles para las vulnerabilidades la vulnerabilidad y sus consecuencias se puede validar con cierto grado de certeza.

Criterio	Valoración	Descripción	
		Métrica Base	Métrica Temporal
		confidencialidad, integridad y disponibilidad de la información.	
Alto/Crítico	7.0 – 10.0	El atacante puede explotar la vulnerabilidad de manera remota y no necesita acceso local, la vulnerabilidad no es compleja y el atacante no necesita mayor nivel de conocimiento para explotarla, el atacante no requiere privilegios de usuario para poder explotar la vulnerabilidad, el atacante puede explotar la vulnerabilidad sin ninguna interacción por el usuario. La vulnerabilidad, en caso sea explotada si afecta otros recursos negativamente. La vulnerabilidad si es explotada tiene un alto impacto negativo en la confidencialidad, integridad y disponibilidad de la información.	La vulnerabilidad está disponible fácilmente en línea y hay un numero grande de potenciales atacantes, no hay remediaciones disponibles y oficiales para la vulnerabilidad, la existencia y consecuencia de la vulnerabilidad ha sido validada y/o comunicada por fuentes confiables y/o por el proveedor.

OWASP TOP 10

El proyecto de seguridad de aplicaciones web abiertas (OWASP) es una comunidad abierta dedicada a permitiendo a las organizaciones desarrollar, comprar y mantener aplicaciones y API en las que se pueda confiar. El OWASP Top 10 se enfoca en identificar los riesgos más críticos para un amplio tipo de organizaciones. Para cada uno de estos riesgos, se proporciona información genérica sobre la probabilidad y el impacto técnico, utilizando el siguiente esquema de evaluación, basado en la metodología de evaluación de riesgos de OWASP.

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

ID	FALLO	DESCRIPCION
A1	Pérdida de Control de Acceso	El control de acceso implementa el cumplimiento de política de modo que los usuarios no pueden actuar fuera de los permisos que le fueron asignados. Las fallas generalmente conducen a la divulgación de información no autorizada, la modificación o la destrucción de todos los datos o la ejecución de una función de negocio fuera de los límites del usuario.

ID	FALLO	DESCRIPCION
A2	Fallas Criptográficas	Lo primero es determinar las necesidades de protección de los datos en tránsito y en reposo. Por ejemplo, contraseñas, números de tarjetas de crédito, registros médicos, información personal y secretos comerciales requieren protección adicional, principalmente si están sujetos a leyes de privacidad (por ejemplo, el Reglamento General de Protección de Datos -GDPR- de la UE), o regulaciones, (por ejemplo, protección de datos financieros como el Estándar de Seguridad de Datos de PCI -PCI DSS-).
A3	Inyección	Algunas de las inyecciones más comunes son SQL, NoSQL, comandos de sistema operativo, Object-Relational Mapping (ORM), LDAP, expresiones de lenguaje u Object Graph Navigation Library (OGNL). El concepto es idéntico para todos los intérpretes. La revisión del código fuente es el mejor método para detectar si las aplicaciones son vulnerables a inyecciones. Las pruebas automatizadas en todos los parámetros, encabezados, URL, cookies, JSON, SOAP y XML son fuertemente recomendados. Las organizaciones pueden incluir herramientas de análisis estático (SAST), dinámico (DAST) o interactivo (IAST) en sus pipelines de CI/CD con el fin de identificar fallas recientemente introducidas, antes de ser desplegadas en producción.
A4	Diseño Inseguro	El diseño inseguro es una categoría amplia que representa diferentes debilidades, expresadas como "diseño de control faltante o ineficaz". El diseño inseguro no es la fuente de las otras 10 categorías. Existe una diferencia entre un diseño y una implementación inseguros. Distinguimos entre fallas de diseño y defectos de implementación por un motivo, difieren en la causa raíz y remediaciones. Incluso un diseño seguro puede tener defectos de implementación que conduzcan a vulnerabilidades que pueden explotarse. Un diseño inseguro no se puede arreglar con una implementación perfecta, ya que, por definición, los controles de seguridad necesarios nunca se crearon para defenderse de ataques específicos.
A5	Configuración de Seguridad Incorrecta	La aplicación puede ser vulnerable si falta el hardening de seguridad adecuado en cualquier parte del stack tecnológico o permisos configurados. Tiene funciones innnecesarias habilitadas o instaladas. Las cuentas predeterminadas y contraseñas aún están habilitadas y sin cambios. El manejo de errores revela a los usuarios rastros de pila u otros mensajes de error. El servidor no envia encabezados o directivas de seguridad.
A6	Componentes Vulnerables y Desactualizados	Una aplicación puede ser vulnerable si no conoce las versiones de todos los componentes que utiliza (tanto en el cliente como en el servidor). Esto incluye los componentes que usa directamente, así

ID	FALLO	DESCRIPCION
		como las dependencias anidadas. Si no repara o actualiza la plataforma subyacente, frameworks y dependencias de manera oportuna y basada en el riesgo. Esto suele ocurrir en entornos en los que la aplicación de parches de seguridad es una tarea mensual o trimestral bajo control de cambios, lo que deja a las organizaciones abiertas a días o meses de exposición innecesaria a vulnerabilidades con soluciones disponibles.
A7	Fallas de Identificación y Autenticación	La confirmación de la identidad, la autenticación y la gestión de sesiones del usuario son fundamentales para protegerse contra ataques relacionados con la autenticación.
A8	Fallas en el Software y en la Integridad de los Datos	Los fallos de integridad del software y de los datos están relacionados con código e infraestructura no protegidos contra alteraciones (integridad). Ejemplos de esto son cuando una aplicación depende de plugins, bibliotecas o módulos de fuentes, repositorios o redes de entrega de contenidos (CDN) no confiables. Un pipeline CI/CD inseguro puede conducir a accesos no autorizados, la inclusión de código malicioso o el compromiso del sistema en general.
A9	Fallas en el Registro y Monitoreo	Volviendo al OWASP Top 10 2021, la intención es apoyar la detección, escalamiento y respuesta ante brechas activas. Sin registros y monitoreo, las brechas no pueden ser detectadas.
A10	Fallas de Solicitudes del Lado del Servidor	Las fallas de SSRF ocurren cuando una aplicación web está obteniendo un recurso remoto sin validar la URL proporcionada por el usuario. Permite que un atacante coaccione a la aplicación para que envíe una solicitud falsificada a un destino inesperado, incluso cuando está protegido por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL).

HERRAMIENTAS UTILIZADAS

Nombre de la herramienta	Escenario	Descripción
Acunetix	Aplicaciones web	Es un escáner de vulnerabilidades de aplicaciones web. Está diseñado para encontrar agujeros de seguridad en las aplicaciones web que un atacante podría aprovechar para obtener acceso a los sistemas y datos.
BurpSuite	Aplicaciones web	Burp Suite es una plataforma integrada para la realización de las pruebas de seguridad de aplicaciones, funcionando como proxy entre nuestro dispositivo e Internet.
SSLScan	Infraestructura y aplicaciones web	Esta es una herramienta para validar los certificados TLS de aplicaciones web y direcciones IP.
GoBuster	Aplicaciones web	Es una herramienta diseñada para obtener por fuerza bruta los nombres de directorios y archivos en servidores Web/de aplicación.
SQLMap	Aplicaciones web	SQLMap es una herramienta de pentesting utilizada para encontrar y explotar vulnerabilidades del tipo SQL Injection.
Kali Linux	Aplicaciones web, infraestructura externa e interna	Kali Linux es una distribución de Linux especialmente diseñada para penetration testing y análisis forense. Contiene más de 300 herramientas y programas pre instalados de análisis de vulnerabilidades y penetración.
Nuclei	Aplicaciones web	Nuclei se utiliza para enviar solicitudes a través de objetivos en función de una plantilla, lo que genera cero falsos positivos y proporciona un escaneo

		rápido en una gran cantidad de hosts. Nuclei ofrece escaneo para una variedad de protocolos, incluidos TCP, DNS, HTTP, SSL, File, Whois, Websocket, Headless, etc. Con plantillas poderosas y flexibles, Nuclei se puede usar para modelar todo tipo de controles de seguridad.

PRUEBAS REALIZADAS

La siguiente tabla muestra las pruebas realizadas, es estado PASS corresponde a que la prueba no fue exitosa en explotar la vulnerabilidad si existe. El estado FAILED corresponde a que la vulnerabilidad fue explotada o que existe la vulnerabilidad.

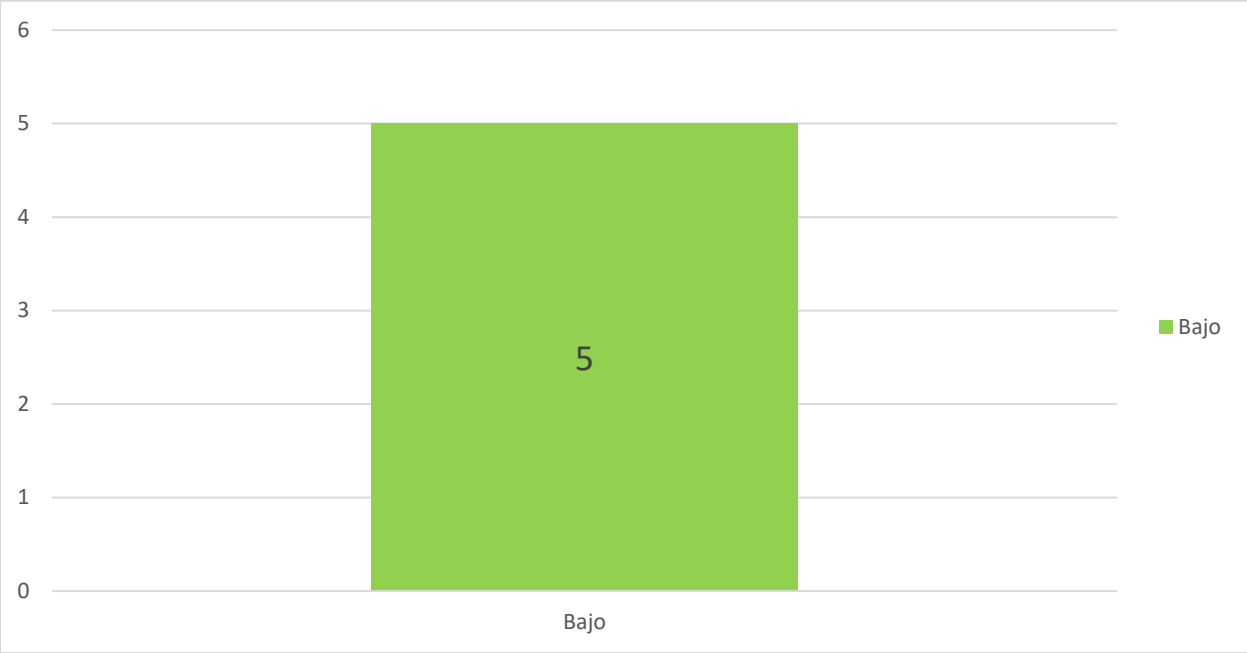
No.	Prueba	Descripción	Estado
1	Inyecciones SQL	Pruebas para listar bases de datos.	**PASS**
2	Inyecciones XSS	Pruebas para inyectar comandos y que refleje alertas o robo de sesiones o cookies	**PASS**
3	Inyecciones HTML	Pruebas sobre el código HTML de la aplicación.	**PASS**
4	Idors	Prueba para el listado de archivos o usuarios.	**PASS**
5	Escalamiento de privilegios	Prueba para tener acceso desde un perfil bajo,	**PASS**
6	Decodeo de parámetros	Decodificación de parámetros mediante la comunicación cliente-servidor	**PASS**
7	Búsqueda de plugins desactualizados	Búsqueda de versiones deprecadas.	**FAILED**
8	Configuraciones de seguridad incorrecta	Pruebas para validar la configuración general de la aplicación.	**PASS**
9	Directorio transversal	Pruebas para listar otros directorios visibles en la aplicación,	**PASS**
10	Revisión de software desactualizado	Validación del software utilizado en la aplicación,	**PASS**

11	Mala configuración de validaciones	Pruebas para validar errores en la aplicación,	**PASS**
12	Mala configuración de permisos	Pruebas sobre los usuarios de bajo perfil.	**PASS**
13	Listado de directorios	Pruebas para listar archivos de la aplicación.	**PASS**
14	Configuraciones por defecto	Pruebas sobre configuraciones por defecto como contraseñas.	**PASS**
15	Revisión de componentes vulnerables y desactualizados	Revisión de librerías en la aplicación web.	**FAILED**
16	Desencriptación de información	Validación de la información enviada.	**PASS**
17	Inyección de comandos	Prueba para validar comandos sobre el servidor.	**PASS**
18	Librerías desactualizadas	Validación de librerías sobre la aplicación web.	**FAILED**
19	Revisión de botones ocultos	Habilitación y deshabilitación de botones en la aplicación.	**PASS**

RESULTADOS
OBJETIVOS WEB

Dentro de las pruebas hacia los objetivos web que se brindaron se descubrieron vulnerabilidades de nivel Bajo distribuidas de la siguiente manera:

- Vulnerabilidades de nivel Bajo: 5



El siguiente cuadro representa los controles OWASP TOP 10 v2021, las casillas en rojo es señal de fallo y las casillas en verde es señal de no alertas generadas. La mayoría de vulnerabilidades es de nivel bajo, pero estas pueden entrar en distintas categorías del OWASP TOP 10 v2021.

URL	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
https://notificame.claro.com.gt/										

--- REPORTE TRUNCADO POR CONFIDENCIALIDAD ---