Tigo-Une

Prueba de Seguridad de Aplicación

Formulario ROI Sarlaft

http://sarlaft.une.com.co

Propuesta de servicios profesionales

28 de abril de 2015

Identidad

FLUID está dirigido a empresas que requieren servicios especializados de seguridad de la información, que buscan un aliado que entienda las necesidades particulares de su negocio.

FLUID es la mejor opción por su experiencia y conocimiento de los líderes de cada sector. Ofrece soluciones únicas, integrales y a la medida apoyadas en modelos de atención, metodologías especializadas y estructuradas por tipo de industria brindando herramientas para que la información de sus clientes esté más segura.

Somos un marca responsable y apasionada, comprometida con lo que hace, cercana a sus clientes y siempre dispuesta a ayudar.

Nuestros clientes

Nuestras capacidades

Colombia Clasificación - Página 1

Los mejores hackers y resuelve retos de Colombia.

Clasificación Global | Clasificación del Sitio | Clasificación por Idioma | Cla

1 2 3

#	Nombre de usuario	Puntuación	
1	hds	208039	Fluid
2	skloj	110715	exFluid
3	Santiagom	75364	Fluid
4	germanlm93	73161	Fluid
5	juanescobar	59525	Fluid
6	redexel	57120	Fluid
7	perskee	51121	Fluid
8	draiven	44100	
9	Phicar	42926	
10	bef0rd	39754	Fluid

Ranking a Febrero 2015

Necesidad

Identificar y valorar, las debilidades de seguridad que pueden afectar al **Formulario ROI Sarlaft** de la compañía, permitiendo integrar dichas debilidades con los activos de información afectados y amenazas probables para determinar los riesgos latentes y así lograr generar planes de acción que lleven a minimizar las pérdidas.

Solución - PSA

Pruebas de seguridad de aplicación

Comprende el intento de explotación de las vulnerabilidades más típicas en aplicaciones en la actualidad con el propósito de realizar operaciones no autorizadas sobre ellas, violando la privacidad de la organización y comprometiendo información sensible. Asimismo, se analizan los posibles riesgos derivados sobre la organización, junto con las opciones para mitigarlos.

Objetivos

- Realizar el diagnóstico técnico de las vulnerabilidades y proponer soluciones para prevenir la inclusión de nuevas vulnerabilidades.
- Articular la priorización de la solución de vulnerabilidades encontradas mediante su clasificación por criticidad.
- Contextualizar las vulnerabilidades encontradas en el marco del negocio de la organización.

Beneficios

- Detección de fallas que crean riesgos de seguridad.
- Entendimiento de los requisitos propios de cada solución.
- Disminución de incidentes de seguridad.
- Mejora en la calidad y reducción del tiempo de despliegue de tecnología.
- Perfil de requisitos de seguridad en constante actualización.
- Personal certificado en seguridad ofensiva práctica (OSCP y CEH).
- Personal clasificado en el top 10 de hackers en Colombia.
- Uso de polígrafo al final del proyecto sobre destrucción de la información generada (opcional).
- Entrega de soluciones de cómo corregir cada hallazgo.
- Informes de avance durante la ejecución del proyecto.

Metodología

Identificar ToE

- Identificar activos críticos de información definiendo el objetivo de evaluación

Perfil y vectores de ataque

- Análisis del diseño de seguridad.
- Contexto de negocio
- Identificar requisitos de seguridad y casos de abuso

Testing de seguridad

- Reconocimiento activo y pasivo del ToE
- Ejecución de casos de abuso
- Reportes de avance

Documentación

- Redacción de informes, generación de soluciones.

Presentación de hallazgos

- Validación de entregables con el cliente.
- Presentación de entregables a todos los interesados

Cierre de hallazgos

- Validación del cierre de los hallazgos de seguridad.

Referencias

NIST
National Institute of Standards and Technology

OSSTMM
Open Source Security Testing Methodology Manual
www.osstmm.org

CVE
cve.mitre.org

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

ISO-27002

OWASP
The Open Web Application Security Project

CVSS

CMMI SM

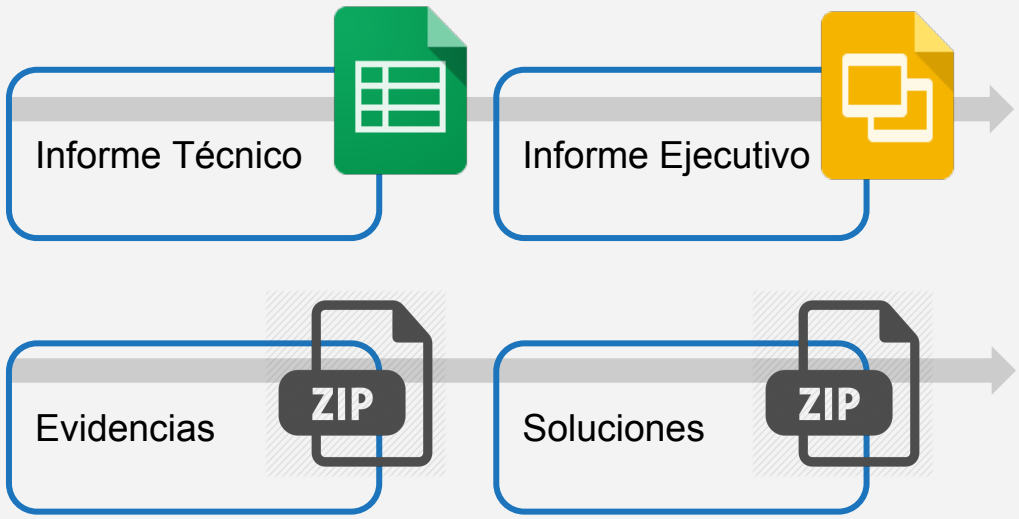
Common Criteria

PCI DSS COMPLIANT

APEC

Criterio de seguridad FLUID

Entregables



Por cada hallazgo de seguridad:

- ➔ Vulnerabilidad.
- ➔ Vector de ataque.
- ➔ Activos afectados.
- ➔ Valoración CVSSv2.
- ➔ Valoración de negocio.
- ➔ Requisitos incumplidos.
- ➔ Evidencia.
- ➔ Solución detallada.

Equipo de trabajo

Project Manager

Dirige y gestiona el proyecto en sus diferentes etapas.

Encargado de canalizar la comunicación con el cliente.

Security Architect

Diseña y entrega el servicio.

Es el líder técnico del proyecto

Security Tester

Ejecuta las pruebas de seguridad en el proyecto.

Diferenciadores

¿Por qué FLUID es mejor para usted?

Aspecto	FLUID	Otros
Método de revisión	Híbrido (Herramientas + revisión manual experta)	Estático (Solo herramientas)
Tipo de hallazgos	• De impacto específicos del negocio • Prácticas inseguras de programación • Alineación a estándares y regulaciones de seguridad	• Sintácticos
Posibilidad de falsos positivos	No	Sí
Estimación	Por campos de entrada de formularios, visibles, invisibles y cabeceras (mayor cobertura y rigurosidad)	Por pantallas o aplicación (menor cobertura y rigurosidad)
Capacidad de explotación	Sí (Si se tiene acceso a la aplicación desplegada)	No
Entregables	• Evidencias de explotación • Soluciones para los hallazgos	• Informe resumen

Alcance

Objetivos	Alcance	Escenario	Cobertura
Formulario ROI Sarlaft	41 campos	Internet	100%

- Los campos fueron estimados basados en pantallazos dado que no se tenía acceso al sitio

Insumos

- Diseño de seguridad (deseable)
  - Permite perfilar mejor el servicio.
- Perfilamiento.
- URL de aplicación.
- Usuarios de la aplicación según escenario.

Inversión

Servicio	Duración	Valor
Prueba de seguridad de aplicación	7 días hábiles	$4.872.000
Pruebas de cierre (Si se requieren)	2 días hábiles	$1.344.000

- Estos valores corresponden a la ejecución de una sola prueba programada de forma consecutiva, sin interrupciones y sobre el mismo sistema coherente. La duración total se determinará según los ingenieros disponibles en el momento para el que el cliente confirme la disponibilidad de todas las dependencias.
- Para alcances más grandes se tendrá un valor adicional en duración e inversión a prorrata del alcance y valor acordado.
- Duración en días hábiles.

Términos

Aplicables al cliente:

- Esta propuesta tiene una vigencia de **30 días** calendario después de su envío,
- Esta propuesta se vuelve obsoleta si FLUID envía otra versión antes de un pedido formal,
- Todos los valores mencionados son **antes de impuestos,**
- El proyecto se realizará en la ciudad de **Medellín, Colombia.**
- El horario es días laborables de **Lunes a Viernes de 7AM-12M, 1PM-6PM**.
- La aceptación escrita de este documento por parte de cualquier funcionario del CLIENTE será entendida como un compromiso de compra.
- Si sobre un proyecto con fechas acordadas entre las partes, éstas deben cambiar por razones ajenas a FLUID, aplicarán los siguientes escenarios:
    - Si el proyecto es cancelado definitivamente, se factura el avance real más un adicional del 25% del avance no ejecutado.
    - Si el proyecto se ejecuta sin detenerse, pero se extiende en duración o en recursos para cumplir con el alcance acordado, se facturará el total más un adicional al porcentaje de avance a excluir de no haberse extendido.
    - Si el proyecto debe ser reprogramado, se facturará un adicional del 10% del avance no ejecutado o $500 USD antes de impuestos si fuere inferior.

Glosario

- **ToE:** sigla de *Target of Evaluation*. Objetivo de evaluación a ser probado.
- **Campo de entrada**: es el punto donde un usuario puede interactuar con una aplicación, ingresando información o eligiendo una opción. Ejemplo: campo de usuario, campo de contraseña, campo de búsqueda.
- **Puerto**: "es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir" [Tomado de Wikipedia]. Esta interfaz permite prestar servicios, como el acceso a sitios web, el acceso a FTP, conexiones a bases de datos, entre otros, a usuarios en una red.
- **Líneas de código**: se refiere a la codificación que realiza un desarrollador de software cuando construye una aplicación. En este caso, las líneas son efectivas (se excluyen líneas vacías o con sólo la apertura o el cierre mediante corchetes)
- **Dirección IP**: es una identificación en la capa de red del modelo OSI o en la capa de Internet del modelo TCP/IP. En este documento, usamos las direcciones IP para contabilizar objetivos de evaluación.
- **PSI**: sigla de Pruebas de Seguridad de Infraestructura.
- **PSA**: sigla de Pruebas de Seguridad de Aplicación.
- **ACF**: sigla de Análisis de Código Fuente.
- **AV**: sigla de Análisis de Vulnerabilidades.
- **Diseño de seguridad**: documento(s) que contienen las consideraciones de seguridad de algún artefacto tecnológico, sea una solución de infraestructura, una aplicación o alguna de sus partes.

Contáctenos

FLUID
SECURITY WITHOUT MYSTERY

Web: http://fluid.la/
Correo: relations@fluid.la
Teléfono: +57 (1) 4661673, +57 (4) 4442637
Ubicación: Bogotá, CL 66 No. 11 – 50, of. 502, Ed. Villorio
Medellín, CL 7 Sur 42 - 70, of. 315, Ed. Forum

Cláusula legal

Clasificación: Propietaria

Este documento contiene información de propiedad de Fluidsignal Group. El cliente puede usar dicha información sólo con el propósito de documentación sin poder divulgar su contenido a terceras partes ya que contiene ideas, conceptos, precios y/o estructuras de propiedad de Fluidsignal Group S.A. La clasificación "propietaria" significa que esta información es solo para uso de las personas a quienes está dirigida. En caso de requerirse copias totales o parciales se debe contar con la autorización expresa y escrita de Fluidsignal Group S.A. Las normas que fundamentan la clasificación de la información son los artículos 72 y siguientes de la decisión del acuerdo de Cartagena, 344 de 1.993, el artículo 238 del código penal y los artículos 16 y siguientes de la ley 256 de 1.996.