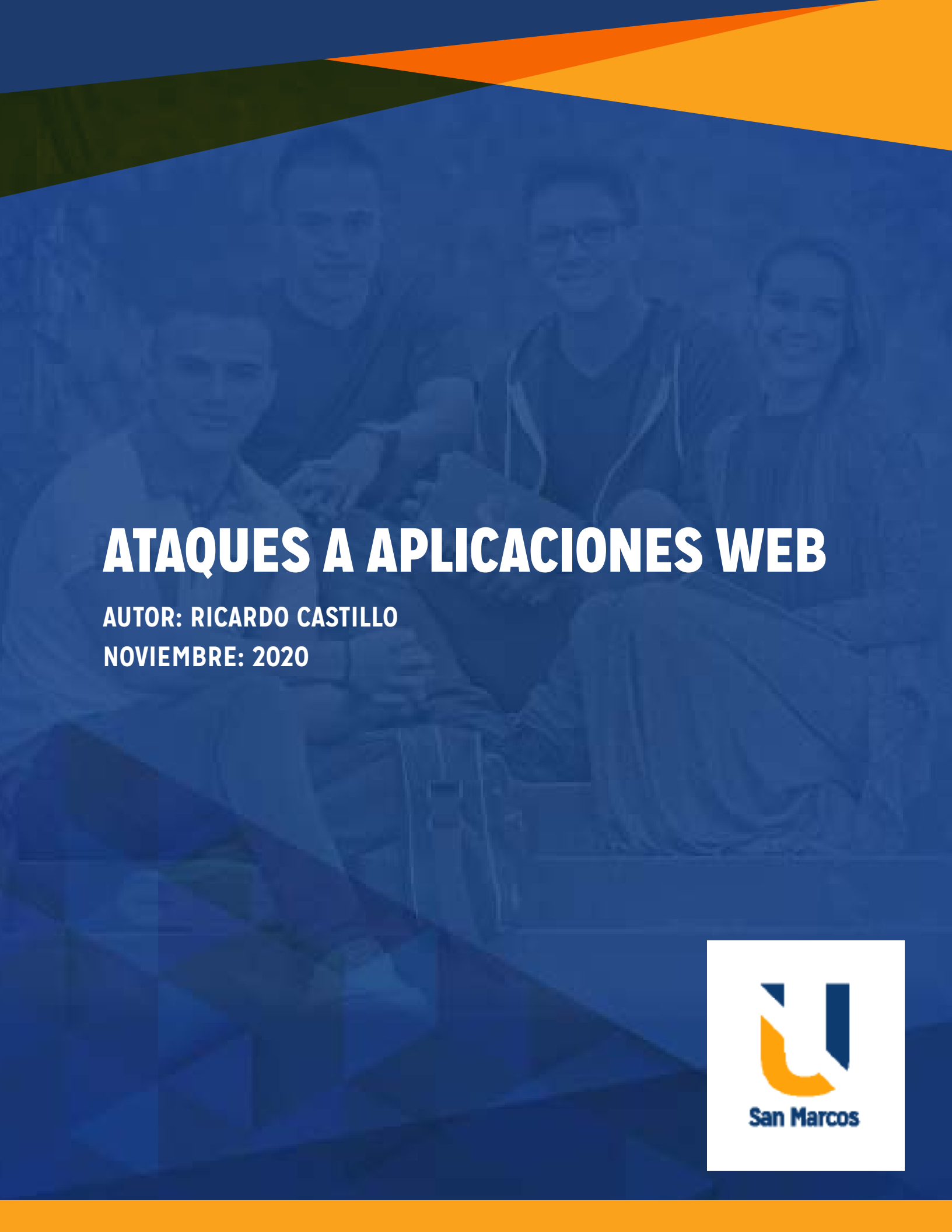

# ATAQUES A APLICACIONES WEB

AUTOR: RICARDO CASTILLO

NOVIEMBRE: 2020

San Marcos

# Introducción

Los softwares maliciosos son aquellos que está diseñados para operar de una manera inconsistente con las intenciones del usuario y que típicamente resulta en molestia o daño a los sistemas de información del usuario.
El aumento de la captura de información personal ocasiona el aumento de los programas de scareware. Este tipo de estafas comienzan con un mensaje emergente en un sitio web, que dice que el equipo está infectado y que se debe descargar un programa gratuito (como un antivirus) para eliminar el malware que supuestamente se ha encontrado. Pero cuando se descarga y ejecuta el programa, se le dice que necesita la versión 'completa' con el fin de desinfectar su ordenador y usted tiene que pagar por esto.
A coontinuación se detalla aspectos generales sobre las herramientas tanto para analizar los códigos malisiosos como aquellas otras que se utilizan por los atacantes para el secuestro de información de los usuarios.

# Contenido

El secuestro de formularios con servidores web infectados que se llevan la información de pago de los consumidores fue la principal amenaza de 2018. Así lo revela el último informe sobre ciberataques de internet de la firma Symantec.

El informe detalla que al menos 4.800 URL fueron infectadas con Form Jacking, al mes en el 2018, lo que representa que uno de cada 10 sitios web en el mundo resultaron infectados con códigos maliciosos.

Symantec, referente sobre ciberseguridad, realizó un análisis profundo mediante la red de inteligencia civil más grande del mundo, que advierte que los ataques de Form jacking, para captar información de tarjetas de crédito de clientes de compras en línea, se dispararán para este 2019.

"El análisis muestra que el ransomware, ha modificado sus objetivos pasando de los consumidores a las empresas, con un aumento de un 12 por ciento de dichas infecciones. El ransomware es un software malicioso que usan los ciberdelincuentes para bloquear los dispositivos de una compañía, que pone en riesgo todos los datos y le quita a las organizaciones el control de la información almacenada. Este virus puede provocar una pérdida masiva de datos.

A lo que se suma que los piratas informáticos se robaron más de 70 millones de registros de buckets S3 con malas configuraciones como resultado de una adopción de la nube demasiado acelerada. Estos delincuentes cada vez optan más por atacar a empresas y usuarios con perfiles alto para extorsionarlos con ‘secuestro’ de información

De acuerdo con lo anterior es que las empresas desarrolladoras de software intentan crear herramientas utiles que permitan detectar y analisar los códigos malignos, mismas que se detallan a continuación.

## Ingeniería inversa de Adobe Flash

SWFRETools son una colección de herramientas para el análisis de vulnerabilidades del reproductor Adobe Flash y para el análisis de malware de archivos SWF maliciosos. Las herramientas están parcialmente escritas en Java y en parte en Python y están bajo la licencia GPL 2.0.

### Las siguientes herramientas forman parte de SWFRETools:

- Flash Dissector: es una herramienta que permite inspeccionar archivos SWF en un nivel binario. Cuando se abre un archivo SWF en Flash Dissector, ofrece la posibilidad de examinar las estructuras definidas en el archivo SWF en un editor hexadecimal y en un visor de estructura. Esto hace que sea fácil de entender qué bytes de un archivo SWF sostiene qué funcionalidad.
- SWF Parser: es un analizador de archivos SWF de código abierto implementado en Java que permite crear herramientas personalizadas de ingeniería inversa de Flash.
- Minimizer: es una entrada SWF que hace que Flash Player se bloquee y elimine automáticamente las partes del archivo SWF que no están relacionadas con el bloqueo. Esto hace más fácil determinar cuál es la causa raíz de un accidente.
- FP Debugger: engancha la secuencia de comandos que tiene una funcionalidad importante en Flash Player en tiempo de ejecución y descarga la información acerca de lo que Flash Player está analizando y ejecutando. Esto es muy útil en situaciones en las que Flash Player se dispara y el análisis estático no está sincronizado con lo que está haciendo Flash Player.
- StatsGenerator: puede crear estadísticas a partir de un conjunto de archivos SWF de entrada.

Por otro lado, se encuentran otras herramientas que son utilizadas por los delincuentes para inyectar código maligno, como los que se muestran a continuación.

## XSS o cross site scripting

Cross-site scripting (XSS) es una vulnerabilidad de seguridad que permite a un atacante inyectar en un sitio web código malicioso del lado del cliente. Este código es ejecutado por las víctimas y permite a los atacanteS eludir los controles de acceso y hacerse pasar por usuarios. Según el Open Web Application Security Project, XSS fue la séptima vulnerabilidad más común de las aplicaciones web en 2017.

Estos ataques tienen éxito si la aplicación web no emplea suficiente validación o codificación. El navegador del usuario no puede detectar que el script malicioso no es confiable, por lo que da acceso a cookies, tokens de sesión u otra información sensible específica del sitio, o permite que el script reescriba contenido HTML.

### Los ataques XSS suelen producirse cuando

1) Los datos entran en una aplicación web a través de una fuente no confiable (en la mayoría de los casos, una solicitud web).
2) El contenido dinámico se envía a un usuario web sin ser validado como contenido malicioso.

El contenido malicioso a menudo incluye JavaScript, pero a veces HTML, Flash o cualquier otro código que el navegador pueda ejecutar. La variedad de ataques basados en XSS es casi ilimitado. pero comúnmente incluyen la transmisión de datos privados como cookies u otra información de sesión al atacante, la redirección de la víctima a una página web controlada por el atacante o la realización de otras operaciones maliciosas en el equipo del usuario bajo la apariencia de un sitio vulnerable.

### Los ataques XSS se pueden clasificar en tres categorías

**XSS Almacenados**: El script inyectado se almacena permanentemente en los servidores de destino. La víctima recupera entonces este script malicioso del servidor cuando el navegador envía una solicitud de datos.

**XSS Reflejados**: Cuando se engaña a un usuario para que haga clic en un enlace malicioso, envía un formulario especialmente diseñado o navegue a un sitio malicioso, el código inyectado viaja al sitio web vulnerable. El servidor web refleja el script inyectado en el navegador del usuario, por ejemplo, en un mensaje de error, un resultado de búsqueda o cualquier otra respuesta que incluya datos enviados al servidor como parte de la solicitud. El navegador ejecuta el código porque asume que la respuesta proviene de un servidor "de confianza" con el que el usuario ya ha interactuado.

**XSS basados en DOM**: El payload se ejecuta como resultado de la modificación del entorno DOM (en el navegador de la víctima) utlizado por el script original del lado del cliente. Es decir, la página en sí no cambia, pero el código del lado del cliente contenido en la página se ejecuta de forma inesperada debido a las modificaciones maliciosas del entorno DOM.

## Exploits

Un exploit es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.
Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la concesión privilegios de administrador al intruso o el lanzamiento de un ataque de denegación de servicio (DoS o DDoS).

## Tipos de exploit

Una vulnerabilidad remota se extiende a través de una red y explota las brechas de seguridad sin necesidad de ningún acceso previo al sistema que ataca.
Por el contrario, una vulnerabilidad local sí requiere que se haya accedido antes al sistema vulnerable, normalmente con la intención de aumentar los privilegios para la persona que, posteriormente, va a ejecutar el exploit.
También existen exploits específicos contra aplicaciones de cliente (aquellas que requieren contacto con un servidor) que normalmente se originan en la modificación de los servidores para que estos envíen entonces el exploit al equipo. Las vulnerabilidades contra las aplicaciones cliente también puede requerir cierta interacción con el usuario, por lo que en ocasiones se utilizan en combinación con métodos de ingeniería social para manipular a las víctimas.

## Zero day exploits

Las vulnerabilidades de Día Cero (también conocidas como 0-day exploits) son las brechas de seguridad en el software desconocidas hasta el momento del ataque. Desde ese punto hasta que la vulnerabilidad es suprimida se entra en el momento en el que los hackers pueden explotarla para lograr el máximo impacto en programas, datos, ordenadores adicionales o en toda una red.
Así, los exploits dirigidos contra ese tipo de vulnerabilidades se denominan zero-day exploits, o ataques zero-day. Cuanto más masivo sea el ataque y menos días hayan transcurrido desde ese Día Cero, mayor será la probabilidad de que no se haya desarrollado ninguna solución o mitigación y los daños pueden ser más extensos.
E incluso después de haber desarrollado la corrección, esos primeros días no todos los usuarios de software habrán podido aplicarla. El caso de WannaCry fue paradigmático en este sentido: el malware se aprovechaba de un exploit de Windows desarrollado por

la Agencia de Seguridad de Estados Unidos y revelado en las semanas previas por Wikileaks.
En los primeros días el problema fue corregido por Microsoft mediante una actualización, pero todos los equipos que no hubieran realizado la puesta al día los días posteriores seguían siendo vulnerables. La activación el lunes de estos equipos que no habían sido utilizados durante el fin de semana inició una segunda oleada de propagación.

## Amenaza occulta

Cuando se hace público un exploit los autores del software afectado toman medidas: la vulnerabilidad se arregla -a menudo a través de un parche- y el exploit se vuelve inutilizable. Por esa razón algunos black hat hackers, así como los hackers de agencias militares o servicios de inteligencia, no publican esas incursiones sino que las mantienen en privado para continuar explotándolas.
Muchos exploits están diseñados para proporcionar acceso a como administrador o superusuario de un sistema. Sin embargo, también es posible que los hackers utilicen varios exploits diferentes para este mismo fin: primero para obtener acceso de bajo nivel, luego para escalar privilegios repetidamente hasta llegar al nivel administrativo más alto (también menudo llamado root)

## Conclusiones y recomendaciones

Actualmente, hay una serie de recursos públicos que proporcionan consejos sobre la seguridad en Internet. Estos incluyen Get Safe Online, identitytheft.org.uk y el Banco en línea seguro. Además, los proveedores de seguridad suelen proporcionar una guía para la seguridad en línea para detener el crimen cibernético. Todos ellos proporcionan una buena orientación sobre cómo reducir al mínimo el riesgo de ser víctimas de los delincuentes.

Todo usuario que desee aumentar su seguirdad en la red debe realizarse las siguientes preguntas, estos cuestionamientos contribuyen a aumentar la precausión y puede disminuir ser victimas de un ataque digital.
A. Confidencialidad: ¿Quienes deberían tener acceso al documento?
B. Autorización: ¿Los permisos que tiene el usuario para trabajar con el documento?
C. Responsabilidad: ¿Lo que va a hacer el destinatario con el documento?
D. Integridad: ¿Cómo sabes si el documento ha sido alterado?
E. Autenticidad: ¿Cómo se sabe de dónde proviene el documento?

## Referencias bibliográficas


- Pareja D. (2019).Uno de cada 10 sitios web, infectados con códigos maliciosos. Recuperado de https://www.riesgoscero.com/blog/uno-de-cada-10-sitios-web-infectados-con-codigos-maliciosos
- Guru de la informática (2017) Herramientas para la ingeniería inversa de Adobe Flash. Recuperado de https://gurudelainformatica.es/herramientas-para-la-ingenieria-inversa-de-adobe-flash
- MDN Web Docs (2020) Cross-site scripting. Recuperado de https://developer.mozilla.org/es/docs/Glossary/Cross-site_scripting
- Panda Security (2020) Exploit. Recuperado de: https://www.pandasecurity.com/es/security-info/exploit/#

San Marcos

**www.usanmarcos.ac.cr**

San José, Costa Rica