Facultad de Tecnologías de información y comunicación

Escuela de Ingeniería de Sistemas Informáticos

Tarea

Nombre del curso: Programación

Alumno: Carlos Daniel Hernández Bonilla  
Carnet: 20170111182

San José, 5/25/2018

Tipos de ataque de código

Inyección de código/code injection:

Son ataques que tratan de inyectar código que es interpretado por la aplicación. Este tipo de ataques inyecta código fuente como SQL, SSI, HTML

Los ataques se dan mucho por no validar apropiadamente las entradas y salidas de datos, falta de responsabilidad en acciones o denegación de acceso. Una inyección puede incluso tomar control total de un nodo.

## SQL injection:

## Bajo esto se busca **acceder a una base de datos mediante PHP** (o el lenguaje elegido)****,** y una vez dentro, sacar, modificar y/o borrar los datos**.

## Para ello, se tiende a buscarle las cosquillas a cualquier cosa de consulta, y se escribe código PHP en su defecto.

**Cross Site Scripting (XSS):**

Se basan en insertar código o script en el sitio web de la víctima, y hacer que el visitante al ingresar al sitio web lo ejecute y así robar sesiones o datos vulnerables.

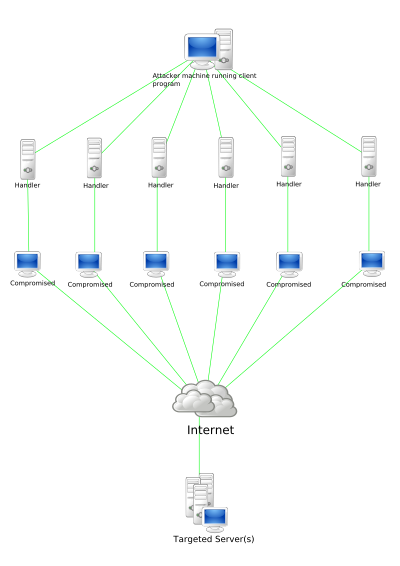
Entre sus funciones esta presentar la información en un [navegador web](https://es.wikipedia.org/wiki/Navegador_web) u otro contenedor de [páginas web](https://es.wikipedia.org/wiki/P%C3%A1ginas_web). Pero no solo se limita a sitios web disponibles en [Internet](https://es.wikipedia.org/wiki/Internet), ya que puede haber aplicaciones locales vulnerables a XSS o incluso el navegador en sí.

Ataques a Fuerza:

Crean procesos automatizados que mediante prueba y error logran dar con el usuario y contraseña, generándolos al azar. Este ataque se puede dar en cualquier página que requiera hacer un login para ingresar, aunque hoy en día son muchas las técnicas utilizadas para evitarlo.

**Denegación del servicio (DDoS):**

Denegación de servicio es el que se realiza cuando millones de sistemas atacan a un único objetivo, provocando la denegación del servicio, de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema fuerza el cierre del mismo, haciendo inaccesible el ingreso a los usuarios legítimos.



Fuga de información:

Una fuga de información es un tipo de ataque que es creado por una persona cercana a la organización, que es ajena a información confidencial y que solo debería ser accesible para integrantes del mismo. Puede ser un incidente tanto interno como externo y a la vez intencional o no.

# Bibliography

Attribution-ShareAlike, C. C. (30 de July de 2015). *OWASP*. Obtenido de https://www.owasp.org/index.php/Inyecci%C3%B3n\_de\_C%C3%B3digo

Bornik, S. (13 de abril de 2015). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

*Colombia Digital*. (3 de Mayo de 2017). Obtenido de https://colombiadigital.net/actualidad/articulos-informativos/item/4801-tipos-de-ataque-y-como-prevenirlos.html

*Palo Yglesias*. (2018). Obtenido de https://www.pabloyglesias.com/mundohacker-sql-injection/

*TechTarget*. (2018). Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio