UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Tarea 1

Maestro

Miguel Ángel Salazar

Matricula

1702824

Alumno

Fernando Martínez Bautista

Vulnerabilidades de aplicaciones web

Las vulnerabilidades de las aplicaciones web pueden ser explotadas por diversos medios y dependiendo del área de negocio en la cual se encuentre esta tendrá una mayor o menor cantidad de porcentaje a ser objetivo de malas intenciones. El sitio de seguridad y hackeo ético whitehat (https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-FINAL.pdf) da un informe detallado de los sectores más expuestos y menciona una lista de vulnerabilidades más comunes.

1. Insufficient transport layer protection
2. Information leakage
3. Cross site scripting
4. Content spoofing
5. Brute forcé

INSUFFICIENT TRANSPORT LAYER PROTECTION

Una capa de transporte transmite información de TCP O UDP. En esta capa podemos encontrar problemas de autenticación de integridad y de confidencialidad. Algunos de los ataque más conocidos en esta capa son las denegaciones de servicio debidas a protocolos de transportes. Un ejemplo claro y rápido seria que mientras existe una denegación de servicio a una página web un incauto usuario intente ingresar pero su ip es secuestrada y redirigida a una página que no es la que buscaba una vez ahí intenta ingresar con su usuario y contraseña, lo cual ya le dio al secuestrador de la ip toda la información ingresada.

INFORMATION LEAKAGE

Fuga de información es una debilidad de la aplicación en la que una aplicación revela datos confidenciales, como detalles técnicos de la aplicación web, el entorno o los datos específicos del usuario. Los datos sensibles pueden ser utilizados por un atacante para explotar la aplicación web de destino, su red de alojamiento o sus usuarios. Por lo cual la fuga de datos sensibles debe ser muy limitada o nula siempre que sea posible. La fuga de información, en su forma más común, es el resultado de una o más de las siguientes condiciones: Error al borrar los comentarios de HTML / Script que contienen información sensible, configuraciones de aplicaciones o servidores incorrectas o diferencias en las respuestas de página para datos válidos contra datos no válidos.

CROSS SITE SCRIPTING

XSS es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador. Sucede cuando un usuario mal intencionado envía código malicioso a la aplicación web y se coloca en forma de un hipervínculo para conducir al usuario a otro sitio web, mensajería instantánea o un correo electrónico. Así mismo, puede provocar una negación de servicio (DDos).

CONTENT SPOFFING

El spoofing de contenido es una técnica de ataque usada para engañar a un usuario para qué crea que cierto contenido que aparece en un sitio Web es legítimo y no de una fuente externa.

BRUTE FORCE

Un ataque de fuerza bruta puede manifestarse de muchas maneras diferentes, pero consiste principalmente en que un atacante configure valores predeterminados, haga peticiones a un servidor usando esos valores y luego analice la respuesta. En aras de la eficiencia, un atacante puede usar un ataque de diccionario o un ataque tradicional de fuerza bruta (con clases dadas de caracteres por ejemplo: alfanumérico, especial, caso (en) sensible). Considerando un método dado, el número de intentos, la eficiencia del sistema que realiza el ataque y la eficiencia estimada del sistema atacado, el atacante puede calcular aproximadamente cuánto tiempo tardará en someter todos los valores predeterminados elegidos.

Una vez leyendo este contenido lo que menos uno querría seria estar navegando en internet, pero como usuario solo nos queda tener en cuenta que en algún momento vamos a estar expuestos y solo nos queda aprender de las recomendaciones de los expertos.

http://projects.webappsec.org/w/page/13246936/Information%20Leakage

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/915/A5.pdf?sequence=5

https://seguridadenredesleonardochaparro.wordpress.com/2014/11/23/vulnerabilidades-mas-comunes-de-las-distintas-capas-del-modelo-tcpip/

https://www.seguridad.unam.mx/%C2%BFqu%C3%A9-es-y-c%C3%B3mo-opera-un-ataque-de-cross-site-scripting-xss

https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-FINAL.pdf

https://www.seguridad.unam.mx/%C2%BFqu%C3%A9-es-y-c%C3%B3mo-opera-un-ataque-de-cross-site-scripting-xss

https://www.owasp.org/index.php/Brute_force_attack