UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Licenciatura en Seguridad de las Tecnologías de Información

DISEÑO ORIENTADO A OBJETOS

Tarea 3

Profesor: Miguel Salazar.

Alumno: Uziel Elías Peñuela Rodríguez.
Matricula: 1734995.

San Nicolás de los Garza, Nuevo León., a 4 de Septiembre de 2017.

Investigación a modo ensayo de los riesgos/aspectos de seguridad con html y/o javascript.

Ejecución remota del código

Como el nombre sugiere, esta vulnerabilidad permite que un usuario malévolo ejecute código arbitrario a nivel servidor y recupere cualquier información deseada que este contiene.

Ocasionalmente, es difícil descubrir esta vulnerabilidad durante el periodo de testeo de la aplicación web, estos problemas se descubren a menudo mientras que se hace una revisión del código de fuente.

Ataque SQL

Los ataques SQL Injection explotan una vulnerabilidad en la validación de las entradas a la base de datos de una aplicación. Una inyección SQL consiste en inyectar un código SQL invasor dentro de otro código SQL para alterar su funcionamiento normal haciendo que se ejecute el código invasor en la base de datos.

La mayoría de aplicaciones webs consisten en un conjunto de operaciones con la base de datos, por ejemplo, en un foro para crear nuevos comentarios se insertan registros en la base de datos y para listar las entradas se seleccionan registros en la base de datos. Estas operaciones reciben el nombre de **CRUD** (Create, Retrieve, Update y Delete). Las aplicaciones son un conjunto de módulos separados que interaccionan entre sí a través de los enlaces y los formularios. Por lo tanto es normal que el desarrollador enlace las distintas páginas utilizando variables que después utilizará para hacer las consultas pertinentes a la base de datos.