

informatizate

<http://www.informatizate.net>

Consideraciones de Seguridad en el Diseño de Aplicaciones Web

Victor Hugo Lamadrid Mendoza

Analista Programador Web [GILAT Peru](#)

Ing. Informático
Miembro Fundador de [informatizate](#)

[victor_lamadrid\(at\)informatizate\(dot\)net](mailto:victor_lamadrid(at)informatizate(dot)net)

Agosto 16 del 2004.



Esta es la primera parte de una serie de artículos que tratan aspectos a tener en cuenta en el diseño de aplicaciones web en cuanto a seguridad, en esta entrega se presenta una vista general de los problemas que se presentan para el diseño de una aplicación web segura.

Introducción

Las aplicaciones web presentan un conjunto complejo de aspectos de seguridad que deben ser cubiertos por los arquitectos, diseñadores y desarrolladores. Las aplicaciones más seguras y resistentes al hacking son aquellas en las cuales la seguridad se tuvo en cuenta durante todo su proceso de desarrollo.

Consideraciones de Diseño para Aplicaciones Web

Las aplicaciones web presentan a los diseñadores y desarrolladores muchos desafíos. La naturaleza del protocolo HTTP como un protocolo sin estado implica que el seguimiento de la sesión para cada usuario pasa a ser responsabilidad de la aplicación. Además, la aplicación debe permitir identificar a un usuario usando algún mecanismo de autenticación. Dado que todas las subsecuentes decisiones de autorización estarán basadas en la identidad del usuario, es esencial que el proceso de autenticación sea seguro y que el mecanismo de manejo de sesión del usuario autenticado esté igualmente bien protegido. El diseño de los mecanismos de autenticación segura y administración de sesión son solo un par de consideraciones con las que los diseñadores y desarrolladores de aplicaciones web tendrán que lidiar. Otro desafío se presenta en el paso de datos de entrada y salida a través de redes públicas. Prevenir la manipulación de parámetros y el acceso a datos sensibles son otros de los aspectos a dar prioridad.

Algunos de los problemas a tratar con prácticas de diseño seguro se muestran en la Figura 1.

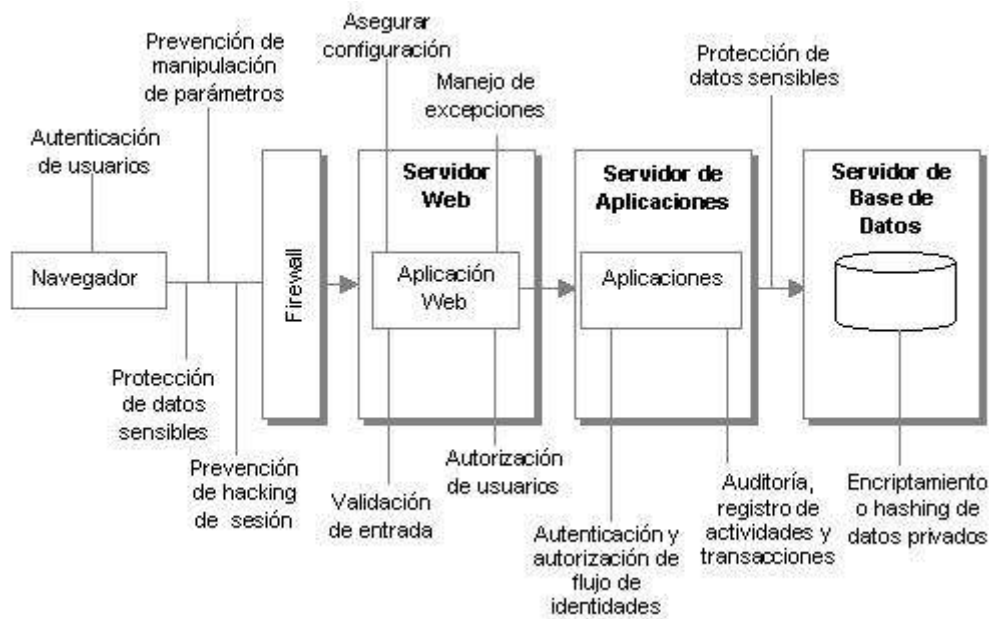


Figura 1. Consideraciones en un diseño seguro para una aplicación web.

Las consideraciones en el diseño se pueden organizar por categorías considerando las vulnerabilidades de la aplicación. La experiencia muestra que un diseño pobre en estas áreas, en particular, conducen a vulnerabilidades de seguridad. La Tabla 1 lista las categorías de vulnerabilidades y para cada una resalta los problemas potenciales que pueden darse debido a un mal diseño.

Categoría de vulnerabilidad	Problema Potencial
Validación de entrada	Ataque ejecutado mediante inserción de cadenas de texto maliciosas en Query Strings, campos de formularios, cookies, y cabeceras HTTP. Esto incluye ejecución de comandos, cross-site scripting (XSS), SQL injection, y ataques para desborde de buffer (buffer overflow attacks).
Autenticación	Suplantación de identidad, password cracking, elevación de privilegios y acceso no autorizado.
Autorización	Acceso a datos confidenciales o restringidos, ejecución de operaciones no autorizadas.
Administración de configuración	Acceso no autorizado a interfaces de administración, alteración de datos de configuración, acceso no autorizado a cuentas de usuario y perfiles de cuentas de usuarios.
Datos sensibles	Acceso a información confidencial
Administración de sesiones	Captura de identificadores de sesión
Encriptamiento	Acceso a datos confidenciales o credenciales de cuenta o a ambos.
Manipulación de parámetros	Ejecución de comandos, elevación de privilegios, Denegación de servicios, etc.
Manejo de Excepciones	Denegación de servicios y acceso a información de detalle en el nivel de sistema.
Auditoría y registro de actividades	Falla para registro de pruebas de intrusión, acciones realizadas por el intruso y dificultades en diagnosticar problemas.

Tabla 1. Vulnerabilidades en Aplicaciones Web y problemas potenciales debido a un mal diseño.

Consideraciones de Despliegue

Durante la fase de diseño, se deberían revisar los procedimientos y políticas de seguridad corporativa junto con la infraestructura sobre la cual será desplegada la aplicación. Frecuentemente, el entorno de destino no es flexible, el diseño de la aplicación debe reflejar esas restricciones. Compensaciones en el diseño se requieren algunas veces, por ejemplo, tener en cuenta restricciones de protocolo o puerto, o topologías de despliegue específicas. Identificar estas restricciones con anticipación en la fase de diseño evita toparse con sorpresas posteriormente e involucra a los miembros de los equipos de red e infraestructura para ayudarnos en el proceso.

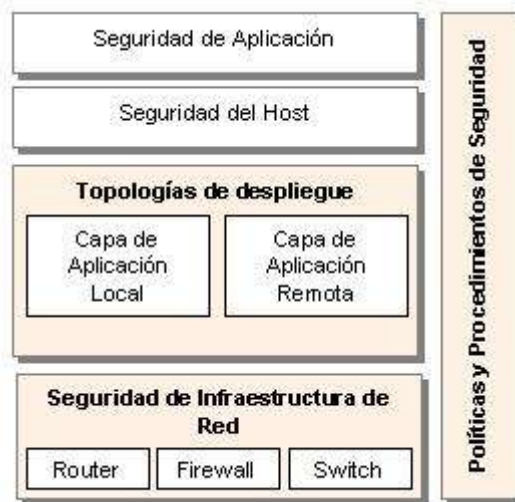


Figura 2. Consideraciones de despliegue.

Políticas y Procedimientos de Seguridad

Las políticas de seguridad determinan que es lo que les está permitido hacer a la aplicación y usuarios de aplicación. Más importante aún, éstas definen restricciones que determinan que es lo que no puede hacer una aplicación o usuario. Identificar y trabajar dentro del ámbito cubierto por las políticas de seguridad corporativa mientras se diseña la aplicación asegura un correcto despliegue.

Componentes de infraestructura de red

Se debe familiarizar con la estructura de red del entorno destino y los requerimientos de seguridad de la red en términos de reglas de filtro, restricciones de puertos, protocolos soportados, etc.

Identificar como las políticas de los firewalls afectarían el diseño y despliegue de la aplicación. Puede darse el caso de la existencia de firewalls delante del o los servidores de base de datos. Estos pueden afectar los posibles puertos de comunicación a usar y, por lo tanto, las opciones de autenticación desde el servidor web a los servidores de aplicaciones y de bases de datos. Por ejemplo el modo de autenticación Windows requiere el uso de puertos adicionales.

Topologías de despliegue

La topología de despliegue de la aplicación y la necesidad de tener una capa de aplicación remota es uno de los puntos clave a considerar e incorporar en el diseño. Si se tiene una capa de aplicación remota, se debe tomar en cuenta como asegurar la red entre los servidores para tratar las amenazas como escucha o alteración de datos, por lo que se deben proporcionar mecanismos de protección y aseguramiento de integridad de datos sensibles.

También es importante tener en cuenta los flujos de identidades e identificar las cuentas que serán usadas para autenticación en la red cuando la aplicación conecte a servidores remotos. Un enfoque común es el uso de una cuenta lo menos privilegiada y el uso de una cuenta espejo o duplicada en el servidor remoto con el mismo password. Otra alternativa es el uso de una cuenta de dominio, la cual facilita la administración, pero con el costo adicional de configurar el uso de la misma en toda la red. La presencia de un firewall o de dominios separados sin relaciones de confianza algunas veces hacen que la única opción viable sea el uso de cuentas locales.

Intranet, Extranet e Internet

Cada uno de estos escenarios de aplicación presenta desafíos en su diseño. Puntos a tener en cuenta pueden ser:

- ¿Cómo fluirá la identidad de los llamadores por las múltiples capas de la aplicación para poder obtener acceso a los recursos del back-end?
- ¿Dónde se realizará la autenticación?

Hasta la próxima entrega.

Referencias

<http://msdn.microsoft.com/library/spa/default.asp?url=/library/spa/vbcon/html/vbconintroductiontowebformssecurity.asp>

<http://msdn.microsoft.com/library/spa/default.asp?url=/library/SPA/vsent7/html/vxconDesigningForSecurability.asp>

<http://msdn.microsoft.com/library/SPA/vbcon/html/vbconBestSecurityPracticesForWebApplications.asp?frame=true>