ADMIN UNAM 2012

Amenazas a Aplicaciones Web

Ing. Mauricio Andrade Guzmán

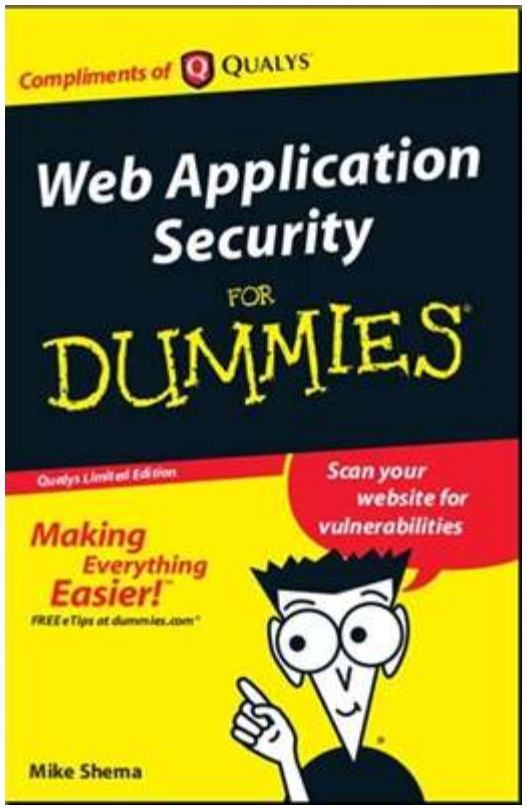
Subdirección de Seguridad de la Información/UNAM-CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM CERT

Agenda

- Aplicaciones web
- Principales amenazas
- Prevención y buenas prácticas
- Demo



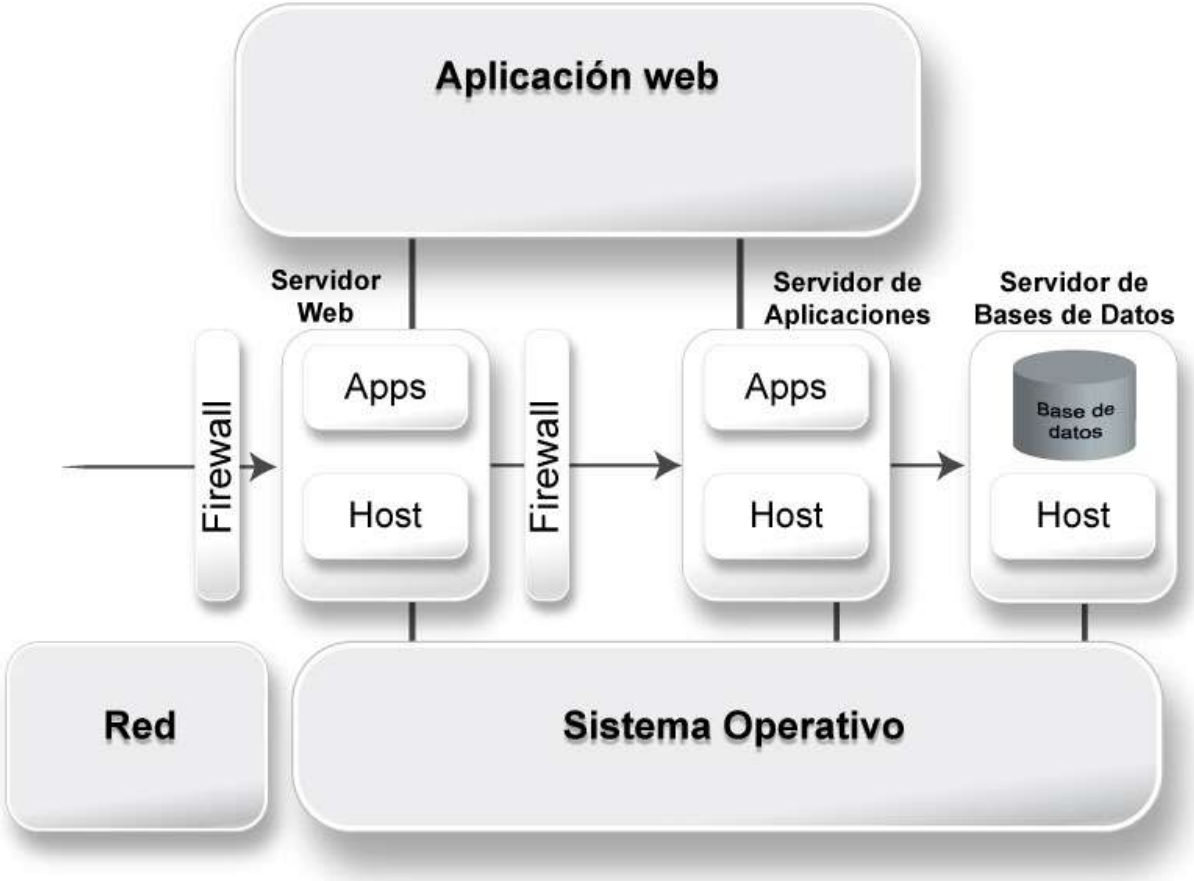
Aplicación web

WIKIPEDIA
La enciclopedia libre

PostgreSQL

WORDPRESS.COM

Esquema general de una aplicación web



Aplicaciones web

- Las aplicaciones web manejan grandes cantidades de **información** y su uso está creciendo.
- La seguridad comienza desde la planeación y diseño de cualquier proyecto de desarrollo.
- Es muy importante capacitar al personal involucrado con una cultura de seguridad.
- Es conveniente mantenerse informado y actualizado de las vulnerabilidades existentes y cómo prevenirlas.

Riesgos en aplicaciones web

- **Riesgo**.
  - Probabilidad de que ocurra un evento
  - Consecuencias que pueden presentarse cuando ocurre.

Ej.

  - Evento: Fallo inesperado en el comportamiento de una aplicación web.

  - Consecuencias: Exposición accidental de información confidencial.

Amenazas y vulnerabilidades

- **Amenaza**. Probable causa de un evento no deseado que puede resultar en daño para un sistema o una organización.

Ej.

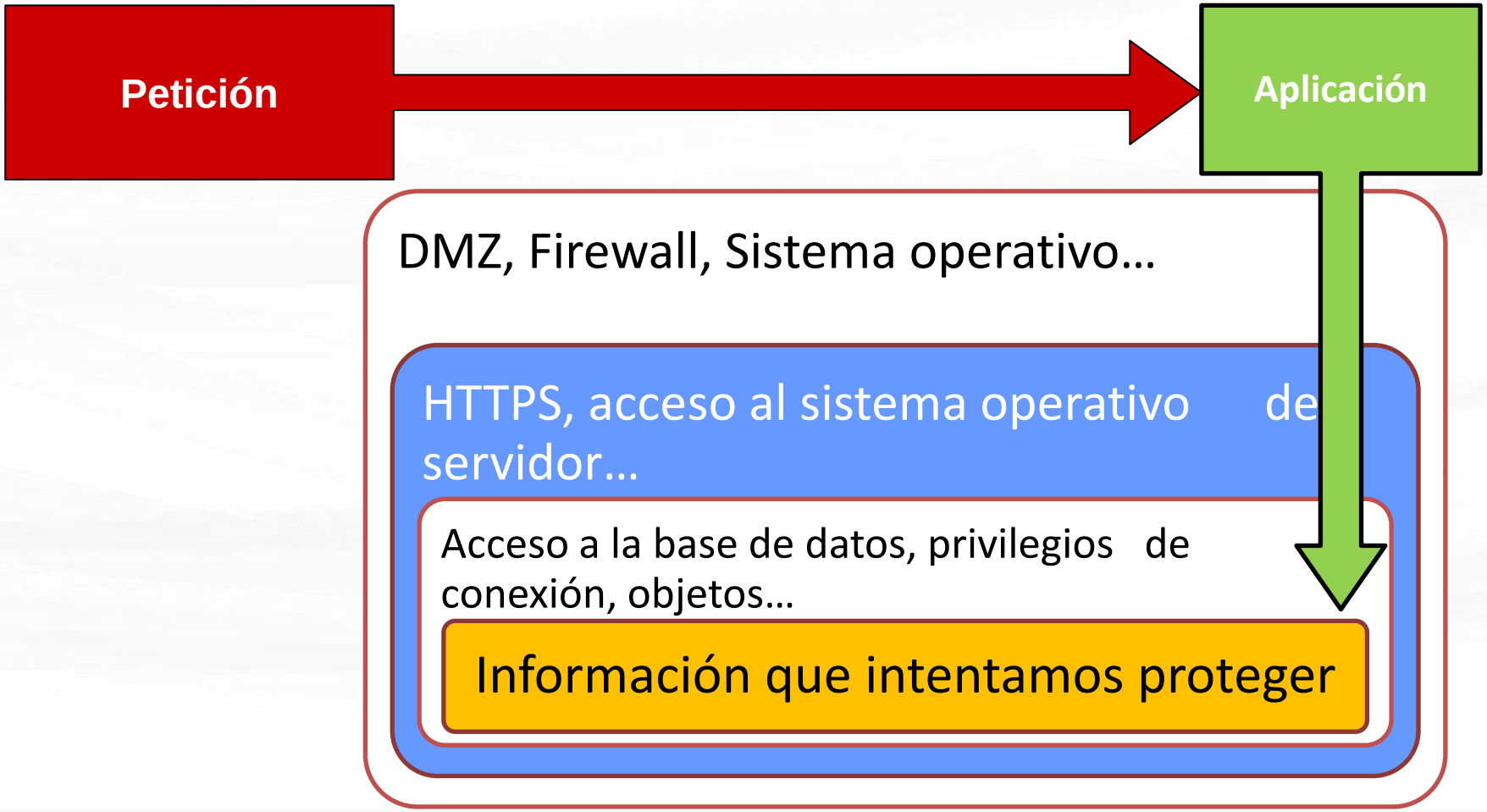
  - Que los usuarios de la aplicación escriban su contraseña y la guarden bajo el teclado.

- **Vulnerabilidad**. Punto débil de un activo o grupo de activos que pueden ser explotadas por una o varias amenazas.

Ej.

  - Error en la validación de los datos del usuario.

La aplicación es parte del perímetro de seguridad

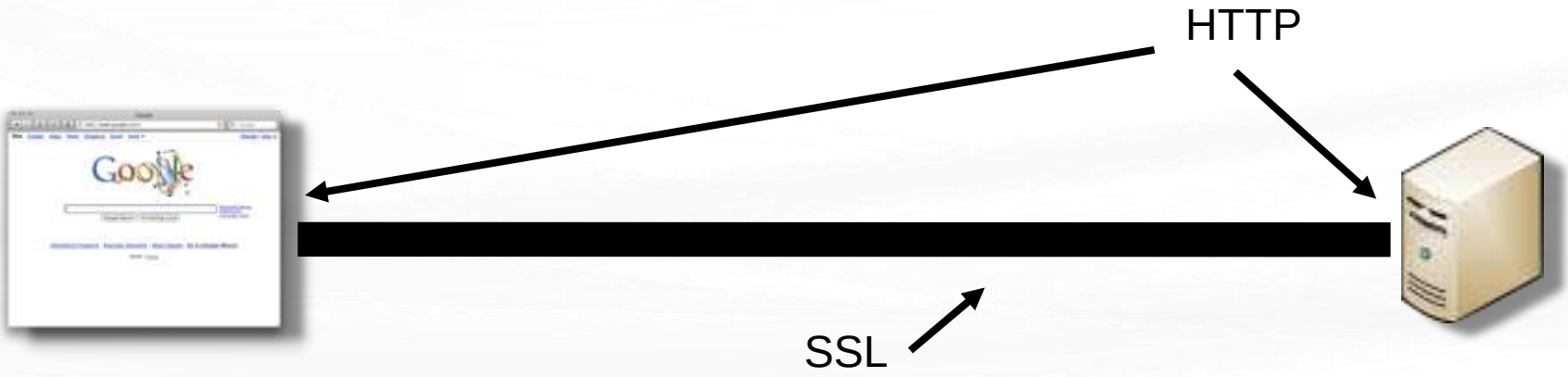


Consideraciones para el sistema operativo

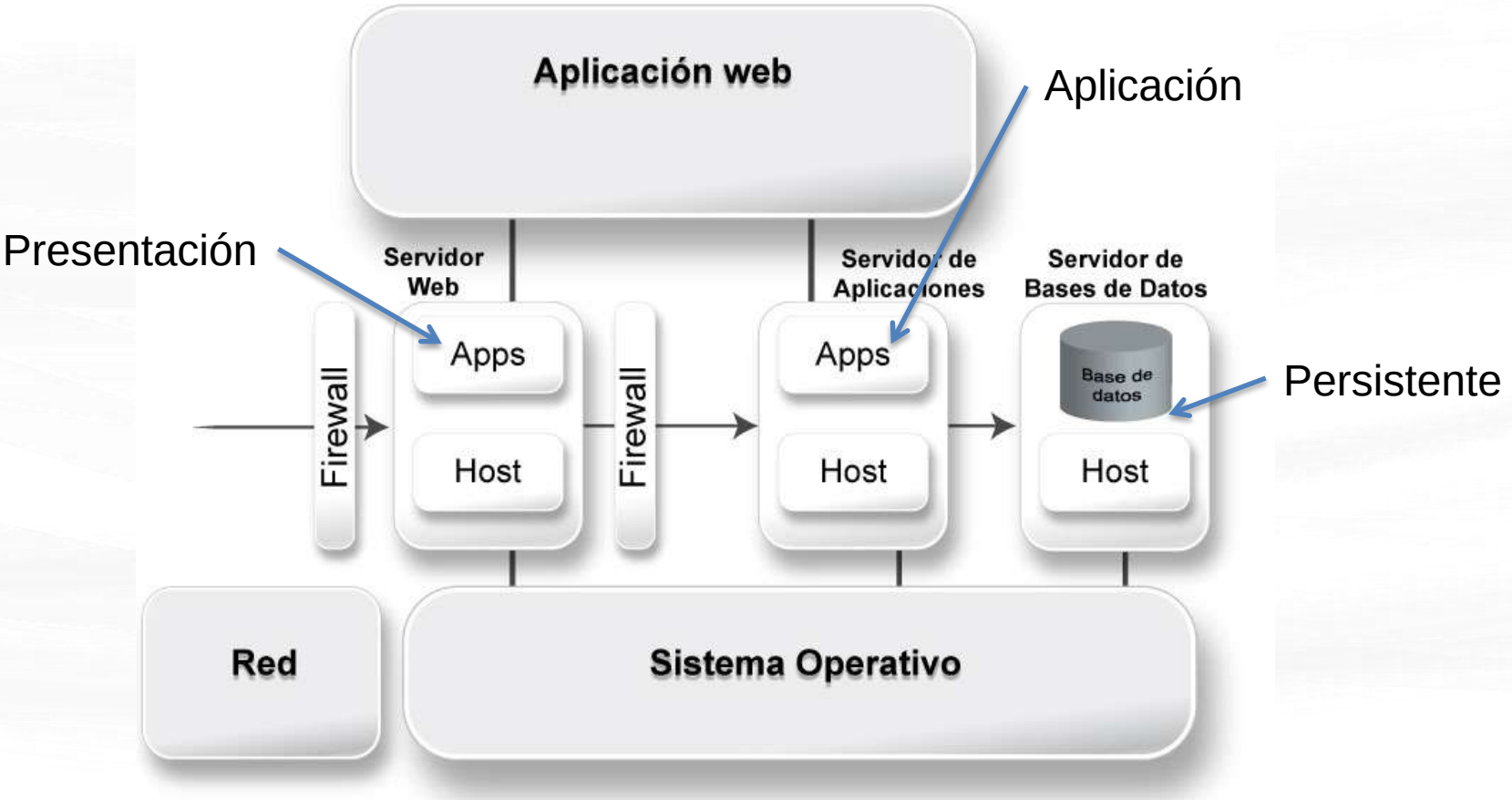
- Parches y actualizaciones
- Cuentas de usuario
- Archivos y directorios
- Puertos y protocolos
- Servicios
- Bitácoras

HTTPS

- **Importante**: protege sólo la información en transito entre el sitio web y los usuarios.



Regresemos al esquema general



Características de aplicaciones web

- Usando servicios tipo Web 2.0 o redes sociales
- Instalando gestores de contenido
- Desarrollo a la medida

Web 2.0 y redes sociales

- Compartir información
- Mapas
- Fotos
- Autenticación
- Colaboración
- Documentos
- Comentarios
- Búsquedas

Riesgos de usar Web 2.0 y redes sociales

- **Privacidad de la información**. La información de los usuarios está en un servidor externo.
- **Errores de configuración**. Pueden quitar funcionalidad a nuestra aplicación.
- **Disponibilidad**. El servicio se puede caer sin previo aviso.
- **SPAM**. La moderación de contenido puede ser un problema.
- Se aceptan los riesgos del proveedor para los usuarios.
  - Fuga de información
  - Robo de sesión
  - …

Gestores de contenidos

- Blogs
- Wikis
- Foros
- Cursos
- Cientos de funcionalidades adicionales a través de plugins

Riesgos de gestores de contenido (CMS)

- **Vulnerabilidades conocidas**. Al ser aplicaciones populares, la mirada está puesta en ellos.
- **Configuraciones predeterminadas**. Una instalación sin cuidado puede exponer la aplicación.
- **Vulnerabilidades en el servidor**. El sistema operativo debe estar preparado para un ambiente de producción.
- **Versiones sin actualizar**. Constantemente se liberan parches que deben ser aplicados.

Desarrollo a la medida

- Puede ser una mezcla de las anteriores
- Mayor versatilidad
- Intervienen las tres capas de la aplicación
- Permite automatizar procesos complejos
- Costo mayor

Riesgos de un desarrollo de la medida

- Errores de validación de entrada
- Configuración insegura
- Gestión de sesión de usuarios
- Autenticación débil
- Fallas de seguridad en la interacción con la base de datos
- Uso inseguro de bibliotecas del sistema
- Uso inseguro de llaves criptográficas
- …

Top Ten de OWASP (owasp.org)

1. Inyección
2. XSS (Cross Site Scripting)
3. Pérdida de Autenticación y Gestión de Sesiones
4. Referencia Insegura a Objetos
5. CSRF (Falsificación de Peticiones en Sitios Cruzados)
6. Defectuosa configuración de seguridad
7. Almacenamiento Criptográfico Inseguro
8. Falla de Restricción de Acceso a URL
9. Protección Insuficiente en la capa de Transporte
10. Redirecciones y Reenvíos no validados

1. Inyección

- Ejemplo. Ejecución de código sql sin validar:
  - String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") +"'";

http://example.com/app/accountView?id=' or '1'='1

2. XSS

- Ejemplo. Construcción de etiquetas HTML:

- http://www.sitio.com.mx/v1/lib/autocomplete/lib/search.php?Base=information_schema.tables&campoBase=table_name&q=%_ <marquee bgcolor="white"> Hola a todos</marquee>

Protección y prevención

- En la organización
  - Contar con una metología de desarrollo
  - Documentación
  - Capacitación

- Buenas prácticas
  - Al codificar
  - Administrar el servidor
  - Bases de datos

Instalación de un WAF como medida de protección

- Un WAF (Web Application Firewall) protege cada petición entrante a la aplicación, identificando comportamiento sospechoso.

- Ofrece una protección inmediata contra muchos ataques sin modificar el código fuente.

SDL

- Security Development Lifecycle (Microsoft)

Pruebas a las aplicaciones

- Permite encontrar vulnerabilidades en la funcionalidad y seguridad de la aplicación web.
- Permiten monitorear aspectos importantes en la codificación de la aplicación.
- Algunas herramientas:
  - Backtrack
  - Samurai WTF

DEMO

Mauricio Andrade
Mario Martínez

adminunam@seguridad.unam.mx

Seguridad en Aplicaciones Web

¡Gracias por su atención!