El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

CICLO III:

Desarrollo de software

MisionTIC2022

El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

Sesión 13:

Desarrollo Software

Principios de programación Web Segura

Mision TIC 2022

Objetivos de la sesión

Al finalizar esta sesión estarás en capacidad de:

1. Explicar los principios de programación segura
2. Mitigar los ataques a aplicaciones web más comunes
3. Aplicar la validación de los datos de entrada

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Programación Web segura

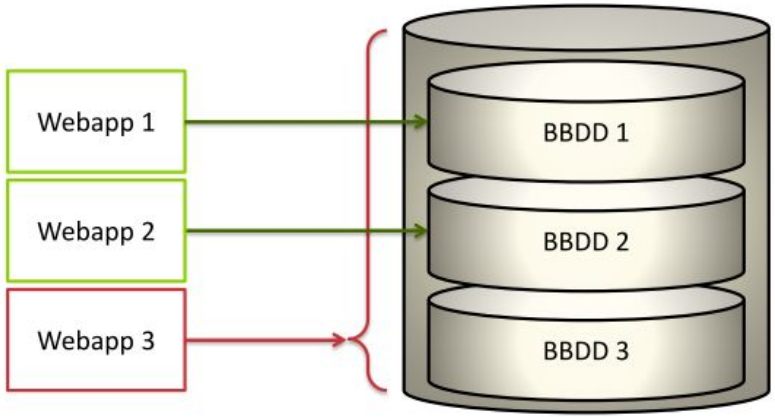
- La finalidad de la seguridad web es prevenir ataques de denegación de servicio, o de información modificada (y con frecuencia dañada) en sus páginas de inicio.
- La seguridad es la acción de proteger sitios web del acceso, uso, modificación, destrucción o interrupción, no autorizados.
- Para que la seguridad de sitios web sea eficaz, se requiere de gran capacidad de diseño a lo largo de la totalidad del sitio web: en la aplicación web, en la configuración del servidor web, en las políticas para crear y renovar contraseñas, y en el código del lado cliente.

MisiónTIC2022

Principios de Programación Web segura

1. Mínimo privilegio

Cada elemento debe tener los permisos estrictamente necesarios para efectuar las acciones que le corresponde y para los que han sido diseñados.



Principios de Programación Web segura

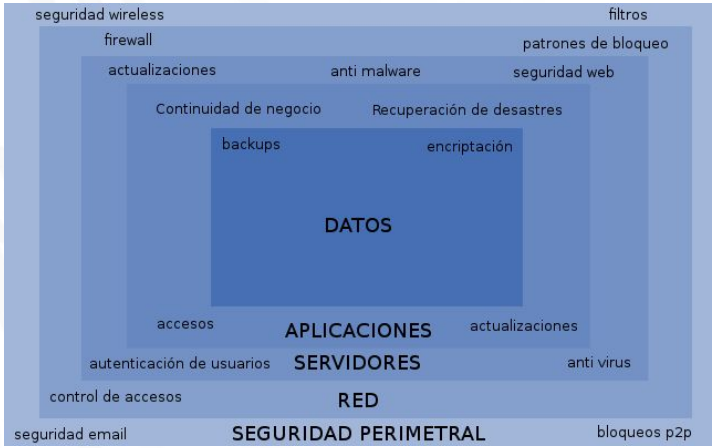
2. Mínima exposición

Minimizar el área de exposición de un sistema habilitando únicamente los servicios estrictamente necesarios.

Principios de Programación Web segura

3. Defensa en profundidad

Aplicar varias capas de protección a un mismo elemento y separar en varias áreas la arquitectura de la red con el fin de hacer más complicado el acceso a la información.



Principios de Programación Web segura

4. El eslabón más débil

La seguridad de un sistema está dada por su eslabón más débil, no sirve de nada fortalecer un área de un sistema si no se presta atención a las demás.

5. Proceso continuo

La seguridad debe estar en permanente evolución con el fin de adaptarse a las nuevas técnicas de ataque y amenazas.

6. Proporcional

El nivel de seguridad de un sistema debe ser proporcional al valor de la información almacenada por estos.

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación Web segura

Técnicas de programación segura

Muchos de los problemas de seguridad web suelen ser el resultado de una programación errónea.

Mision TIC 2022

Principios de Programación Web segura – OWASP TOP 10

¿Qué es OWASP?

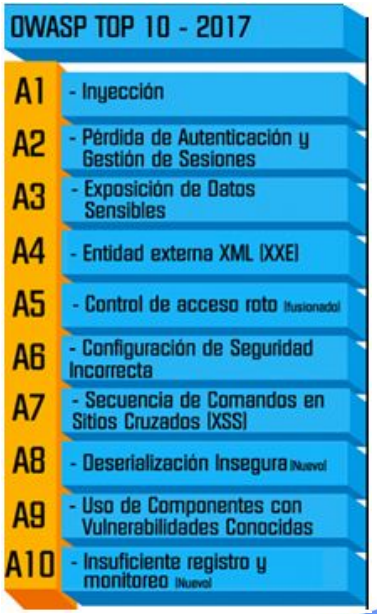
- Existen organizaciones dedicadas a proporcionar el análisis de vulnerabilidades y ofrecer herramientas para la auditoría, aprendizaje y prevención de las fallas de seguridad web con el fin de identificar los riesgos y errores de seguridad más relevantes en una aplicación web.
- OWASP es una organización conocida mundialmente que reúne una gran cantidad de profesionales de la seguridad informática para crear conocimiento con respecto a la seguridad web. OWASP es de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación Web segura – OWASP TOP 10

OWASP publica y revisa un documento con los diez riesgos de seguridad que considera más importantes en aplicaciones web de mayor a menor importancia.



MisiónTIC2022

Principios de Programación Web segura – Inyección SQL

- Las vulnerabilidades de Inyección SQL permiten a atacantes ejecutar código SQL arbitrario, autorizando implícitamente que se pueda acceder, modificar o borrar a los datos, independientemente de los permisos asignados a un usuario y/o libreria.
- Un ataque de inyección exitoso puede llevar a otros ataques, tales como falsificar identidades, crear nuevas con permisos de administración, acceder a todos los datos en el servidor o dañar/modificar los datos para hacerlos inutilizables.
- Esta vulnerabilidad se presenta siempre y cuando la entrada del usuario pasada por medio de la sentencia SQL pueda cambiar el significado de la misma.

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación Web segura – Inyección SQL

Tipos de ataques:

- **Ataque por error:** es el más común y el más fácil de explotar ya que es la misma aplicación la que va mostrando los errores de la base de datos al ejecutar las distintas consultas.
- **Ataque por unión:** un atacante que utiliza la unión SQL se une para mostrar los resultados de una tabla diferente. Por ejemplo, si un atacante está en una página de búsqueda, puede añadir los resultados de otra tabla.
- **Ataque ciego (blind):** es el más complicado y el más avanzado. El atacante envía varias consultas a la base de datos para evaluar cómo la aplicación analiza estas respuestas. Es decir, crea un oráculo con la aplicación permitiéndole encontrar respuesta a una serie de “queries”, de los que en últimas puede filtrar información.

Mision TIC 2022

Principios de Programación Web segura – Inyección SQL

Ejemplo: listar todos los usuarios con un nombre en particular (Nombre) que ha sido suministrado en un formulario HTML:

```
SELECT * FROM usuarios WHERE nombre = '" + Nombre + "';
```

- Si el usuario introduce su nombre real, todo funciona de forma correcta.
- Si es un atacante, éste podría cambiar por completo el comportamiento de ésta instrucción SQL, de la siguiente forma:

```
SELECT * FROM usuarios WHERE nombre = 'a';DROP TABLE usuarios; SELECT *
FROM informacion WHERE 't' = 't';
```

Principios de Programación Web segura – Inyección SQL

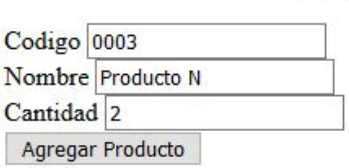
Ejemplo (continuación)

- Al cambiar Nombre por el texto en "negrilla“, seguiría siendo una instrucción SQL válida que borraría la tabla usuarios y seleccionaría todos los datos de la tabla información (poniendo al descubierto toda la información de todos los usuarios). Esto funciona por que la primera parte del texto inyectado (a';) completa la sentencia original (' es el símbolo para indicar una cadena literal en SQL).
- La forma de evitar este tipo de ataque es asegurar que cualquier dato de usuario que se pasa a un query SQL no cambie la naturaleza del mismo. Una manera es eludir ('escape') todos los caracteres en la entrada de usuario que tengan un significado especial en SQL.

```
SELECT * FROM users WHERE name = 'a\';DROP TABLE users;    SELECT *
  FROM userinfo WHERE \'t\' = \'t';
```

Principios de Programación Web segura – Inyección SQL

Tomando la Base de datos de la sesión anterior, se muestra un ejemplo de Inyección SQL.



Los datos ingresados serán concatenados y formarán una cadena con la sentencia sql de update:

```
insert into productos (codigo, nombre, cantidad) values('0003', 'Producto N', 2);
```

Ahora bien si en el campo de texto cantidad se digita la siguiente cadena:

```
insert into productos (codigo, nombre, cantidad) values('005', 'xx', '0');
```

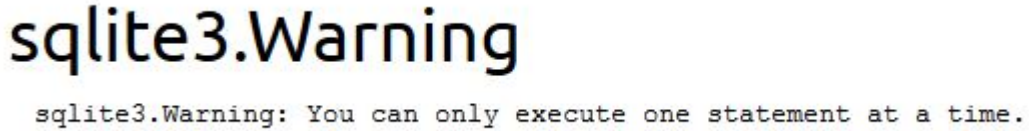
El resultado de la cadena sql será el siguiente:

```
insert into productos (codigo, nombre, cantidad) values('0003', 'Producto N', 2);
insert into productos (codigo, nombre, cantidad) values('005', 'xx', '0');
```

Principios de Programación Web segura – Inyección SQL

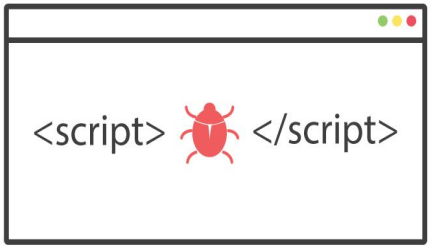
SQLite3 en su lógica tiene mecanismos implementados que no permiten que se ejecute con una sola instrucción más de en una secuencia, evitando con esto los ataques Inyección SQL. Lo que no sucede con otras bases de datos.

Este es el mensaje que se muestra al ejecutar:



Principios de Programación
Web segura – Inyección JavaScript

- Un ataque por inyección JavaScript tiene como propósito lograr inyectar en el contexto de un dominio un código Javascript con la finalidad de engañar al usuario o realizar una acción no deseada reemplazandolo.
- En este tipo de ataque, el afectado no es precisamente el servidor, como suele suceder en un ataque de Inyección SQL, sino que el objetivo directo es el usuario.
- Si el ataque se realiza con éxito y se utiliza suplantación de identidad, se podrán ejecutar las acciones deseadas en el servidor afectado y al que se puede acceder desde una página web.



Principios de Programación
Web segura – Inyección JavaScript

- Para comprobar si hay vulnerabilidad en una aplicación web a este ataque, se debe escribir en el campo de texto el siguiente código que permitirá una alerta en el navegador cuando se ejecute:

```
<script>
   alert()
</script>
```

- Pueden darse dos formas de ejecución:
  - En el instante en que se envía el formulario
  - Que se almacene en una base de datos, y se ejecute al cargar el contenido de esta.

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación
Web segura – Inyección JavaScript

Tipos de ataques

Dependiendo de cómo envían el código malicioso:

- **No permanente:** Estos no almacenan el código malicioso en el servidor sino que lo pasan y presentan directamente a la víctima. Este ataque se lanza desde una fuente externa, mediante email o un sitio de terceros.
- **Permanente:** El código malicioso ya ha traspasado todo el proceso de validación y está almacenado en una Base de Datos. Puede ser un comentario, un archivo log, un mensaje de notificación, o cualquier otro tipo de proceso del sitio web que solicite algún input al usuario. Cuando esta información se presenta en el sitio web, el código malicioso se ejecuta.

MisionTIC2022

Principios de Programación
Web segura – Inyección JavaScript

Ejemplo: Usuario logueado siempre en un foro del que es admin. A la hora de cambiar la contraseña se realiza una petición con GET a la web:

```
foro.com/id=admin&changepassword=nuevacontraseña
```

El ataque consistirá en enviarle al usuario lo siguiente:

```
paginavulnerable.com#catalogo=<script>window.location=foro.com/id='
admin'&changepassword='a2g4g5';</script>
```

Este script redirige a la página foro y cambia la contraseña. Claro está que si no está logueado no funcionará.

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación Web segura – Monster Mitigations

- Estrategias de mitigación aplicables y efectivas para prevenir y solucionar las vulnerabilidades del OWASP Top 10.
- Adaptando estas estrategias de mitigación a cada aplicación, la misma será más segura.
- Se dividen en estrategias de mitigación específicas para cada error y, en generales, aplicables a todas las vulnerabilidades

Mision TIC 2022

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación Web segura – Monster Mitigations

M1 – Establecer y controlar las entradas

- Medida efectiva utilizada para defenderse de ataques comunes.
- Se refiere a revisar la validez de los datos antes de ser procesados.
- Evita que se procesen datos maliciosos o incorrectos a la aplicación.
- Previene el uso de datos maliciosos para la generación de contenidos o comandos.

MisionTIC2022

Principios de Programación Web segura – Monster Mitigations

M1 – Establecer y controlar las entradas

Buenas prácticas:

- Nunca confiar en el usuario.
- Considerar todas las posibles entradas.
- Los atacantes pueden modificar la petición HTTP.
- Centralizar las validaciones.
- Siempre validar del lado del servidor.
- Rechazar datos no válidos.

Ataques que se pueden prevenir:

- Inyección SQL
- Secuencia de Comandos en Sitios Cruzados (XSS)

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Principios de Programación Web segura – Monster Mitigations

M2 – Establecer y controlar las salidas

- Medida más efectiva para defenderse de secuencia de comandos en sitios cruzados (XSS).
- Se refiere a neutralizar los datos potencialmente peligrosos antes de utilizarlos en la generación de contenidos.
- Evita el uso de datos maliciosos durante la creación de contenidos o comandos.

Mision TIC 2022

Principios de Programación Web segura – Monster Mitigations

M2 – Establecer y controlar las salidas

Buenas prácticas:

- Nunca utilizar datos no confiables.
- Colocar un “Escape” a los datos antes de ser utilizados:
  - Etiquetas y atributos HTML
  - JavaScript
  - CSS y Style
  - URL
  - XML
- Utilizar librerías aceptadas como OWASP Enterprise Security API(ESAPI)

Ataques que se pueden prevenir:

- Secuencia de Comandos en Sitios Cruzados (XSS).
- Inyección SQL

Principios de Programación Web segura – Monster Mitigations

M3 – Asegurar el ambiente: permisos y privilegios

- Definir y mantener una configuración segura de la aplicación, frameworks, librerías, servidor Web, base de datos y plataformas.
- Aplicar defensa en profundidad.

Ataques que se puede prevenir:

- Acceso no autorizado a interfaces de administrador de servidores y bases de datos.
- Fuga de información.
- Cualquiera al que estén expuestos los componentes y librerías no actualizados

Principios de Programación Web segura – Monster Mitigations

M3 – Asegurar el ambiente: permisos y privilegios

Buenas prácticas:

- Aplicar las actualizaciones y parches de software y librerías en todos los ambientes.
- Cambiar o deshabilitar las contraseñas por default.
- No almacenar contraseñas dentro de la base de datos.
- Configurar y utilizar elementos con los menos privilegios posibles.
- Deshabilitar o quitar componentes innecesarios.
- Mantener separados los privilegios de administrador.
- Fallar de modo seguro sin exponer más información que la necesaria.

Principios de Programación Web segura – Monster Mitigations

M4 – Todos pueden ver el código

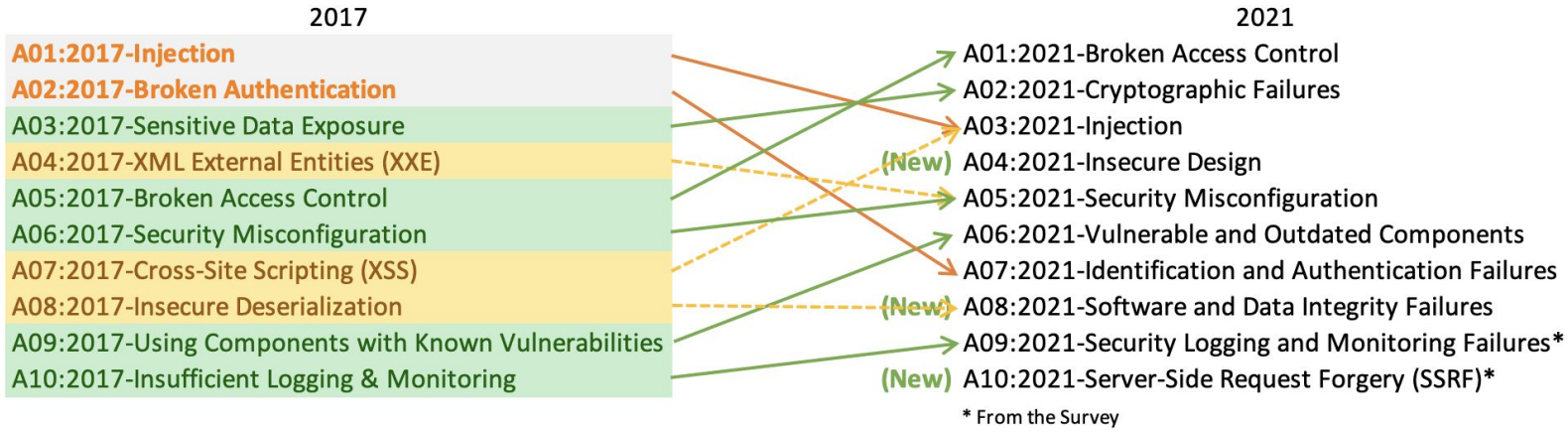
- No depender de la “seguridad por oscuridad”
- Siempre evaluar si el conocimiento del código o diseño hace vulnerable la aplicación.
- Nunca confiar en componentes externos.
- Tener en cuenta que aún el código compilado se puede “leer”.
- Cifrar o encriptar los datos sensibles.

Principios de Programación Web segura – Monster Mitigations

M5 – Usar librerías ya prediseñadas y no inventar las propias

- Aplica para: criptografía, autenticación, autorización, aleatoriedad, manejo de sesión y registro de bitácoras.
- Investigar cuales son los algoritmos más seguros en la actualidad y utilizarlos.
- Seleccionar lenguajes, librerías que faciliten el uso de los algoritmos anteriores.
- Alejarse de algoritmos “secretos” o propios.

Principios de Programación
Web segura – Propuesta OWASP Top 10 - 2021



El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

Ejercicios de práctica

Mision TIC 2022

El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

¡GRACIAS

POR SER PARTE DE ESTA EXPERIENCIA DE APRENDIZAJE!

Mision TIC 2022