**Práctica: Análisis de páginas Web**

Seleccionar páginas de su preferencia y realizar un testeo de vulnerabilidades de las mismas con ‘ , en Windows o Parrot.

**Objetivo:**

Que el alumno realice un análisis de las vulnerabilidades más comunes en páginas web conocidas.

**Desarrollos.**

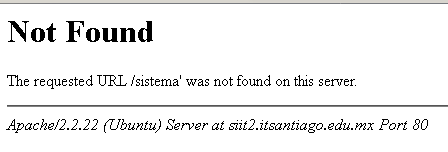
Instrucciones. -Realiza una bitácora donde se detecten las principales vulnerabilidades de una página web, registra y consulta el posible error y la solución del mismo o prevención.

**: Detección de erros:**

**Pagina:**



**Imagen del error:**



**Posible vulnerabilidad:** *Inyección SQL. Envió de información por GET. Sistema Operativo en el que está desarrollada o alojada la aplicación y el puerto.*

**Solución:**

*Puerto: 443 –Certificados $, enviar la información por POST-Hash cifrada, etc, etc, etc..*

* - - - - - - - - - -
* **Pagina:**
* 
* **Imagen del error:**
* 
* *Content-Security-Policy*
* **Posible vulnerabilidad:** *La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra los ataques de 'ClickJacking'.*
* **Solución:**
* *Asegurarse que estén configurados en todas las paginas web devueltas por el sitio/ aplicación*
* - - - - - - - - - -

**Pagina:**



**Imagen del error:**

*Desconfiguración del intercambio de recursos cruzados de origen (CORS).*

**Posible vulnerabilidad:**

*Descargas de datos del navegador web podría ser posible, debido a una desconfiguración del intercambio de recursos cruzados de origen (CORS) en el servidor web*

**Solución:**

*Asegurarse de que los datos sensibles no estén disponibles de manera no autenticada (usando la dirección IP lista-blanco). Configurar el encabezado HTTP ''''Access-Control-Allow-Origin" a un conjunto de dominios más restrictivo, o remover completamente todos los encabezados CORS, para permitir que el navegador web refuerce la política del mismo origen (SOP) de una manera más restrictiva.*

* - - - - - - - - - -

**Pagina:**



**Imagen del error:**



*(tokens) Anti-CSRF*

**Posible vulnerabilidad:**

*No se encontraron fichas (tokens) Anti-CSRF en un formulario HTML.*

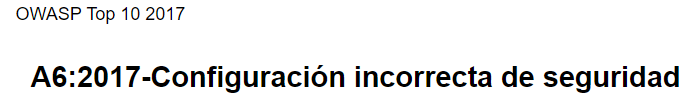
**Solución:**

* *Utilizar una biblioteca o marco comprobado que no acepte que ocurra esta debilidad o que proporcione construcciones que permitan que esta debilidad sea más sencilla de evita.*
* *Asegúrese de que el nonce no sea predecible (CWE-330).*
* *Utilizar el control de gestión de la sesión de ESAPI.*
* *No utilizar el método GET para ninguna de las solicitudes que puedan desencadenar un cambio de estado.*
* *Asegurarse de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante.*
* *Identificar las operaciones que sean especialmente peligrosas. Cuando el usuario desarrolla una operación peligrosa, envíar una solicitud de confirmación de forma separada para poder garantizar que el usuario tenga la intención de desarrollar esa operación.*

**Pagina:**



**Imagen del error:**



*CSP*

**Posible vulnerabilidad:**

* *Las siguientes directivas permiten fuentes comodín (o ancestros), no están definidas o están demasiado definidas:*

*marco-ancestros*

* *La(s) directiva(s): frame-ancestors se encuentran entre las directivas que no recurren a default-src, omitirlas/excluirlas es lo mismo que permitir cualquier cosa.*

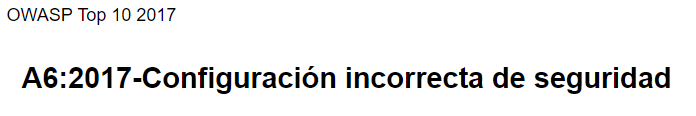
**Solución:**

* *Asegurarse de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado correctamente para establecer el encabezado de Política de seguridad de contenido.*
* - - - - - - - - - -

**Pagina:**



**Imagen del error:**



*Falta el encabezado antisecuestro de clics*

**Posible vulnerabilidad:**

*La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra los ataques de 'ClickJacking'.*

**Solución:**

*Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que uno de ellos esté configurado en todas las páginas web devueltas por su sitio/aplicación.*

* - - - - - - - - - -

**Pagina:**



**Imagen del error:**



*Inclusión de archivos fuente de JavaScript entre dominios.*

**Posible vulnerabilidad:**

*La página incluye uno o más archivos de script de un dominio de terceros.*

**Solución:**

*Asegúrese de que los archivos fuente de JavaScript se carguen solo desde fuentes confiables y que los usuarios finales de la aplicación no puedan controlar las fuentes.*

* - - - - - - - - - -

**Pagina:**



**Imagen del error:**



*Divulgación de error de aplicación*

**Posible vulnerabilidad:**

*Esta página contiene un mensaje de error/advertencia que puede revelar información confidencial, como la ubicación del archivo que produjo la excepción no controlada. Esta información se puede utilizar para lanzar más ataques contra la aplicación web. La alerta podría ser un falso positivo si el mensaje de error se encuentra dentro de una página de documentación.*

**Solución:**

*Revisar el código fuente de esta página. Implementar páginas de error personalizadas. Considere implementar un mecanismo para proporcionar una referencia/identificador de error único al cliente (navegador) mientras registra los detalles en el lado del servidor y no los expone al usuario.*

* - - - - - - - - - -

**Pagina:**



**Imagen del error:**



*Divulgación de la marca de hora*

**Posible vulnerabilidad:**

*Una marca de tiempo ha sido divulgada por el servidor de la aplicación/el navegador – Unix*

**Solución:**

*Confirmar manualmente que los datos de marca de hora no son sensibles, y que los datos no pueden ser agregados a patrones explotables de divulgación.* - - - - - - - - - -

**Pagina:**



**Imagen del error:**



*Envenenamiento por galletas*

**Posible vulnerabilidad:**

*Esto se denomina ataque de envenenamiento de cookies y se vuelve explotable cuando un atacante puede manipular la cookie de varias maneras. En algunos casos, esto no será explotable; sin embargo, permitir que los parámetros de URL establezcan los valores de las cookies generalmente se considera un error.*

**Solución:**

*Si se deben establecer algunos parámetros de la cadena de consulta en los valores de las cookies, asegurarse de filtrar los puntos y comas que pueden servir como delimitadores de pares de nombre/valor.*

- - - - - - - - - -

**Pagina:**

**Imagen del error:**

**Posible vulnerabilidad:**

**Solución:**

* - - - - - - - - - -

**Pagina:**

**Imagen del error:**

**Posible vulnerabilidad:**

**Solución:**

* - - - - - - - - - -

**Pagina:**

**Imagen del error:**

**Posible vulnerabilidad:**

**Solución:**

* - - - - - - - - - -

**Pagina:**

**Imagen del error:**

**Posible vulnerabilidad:**

**Solución:**

* - - - - - - - - - -

**Conclusiones.**

Las vulnerabilidades en las páginas web pueden ser explotadas por ciberdelincuentes y hackers para acceder a información confidencial, robar datos personales o financieros, o incluso tomar el control total del sitio web.

Por lo tanto, es importante que los desarrolladores y administradores de páginas web tomen medidas para identificar y corregir las vulnerabilidades en su sitio web. Esto puede incluir la implementación de medidas de seguridad adecuadas, como el uso de contraseñas seguras, la actualización regular del software y el uso de medidas de autenticación de usuario, entre otras.

Además, es importante que los usuarios tomen medidas para proteger su información personal en línea. Esto puede incluir el uso de contraseñas seguras y únicas, el uso de software antivirus y el monitoreo regular de la actividad de la cuenta en línea.

**Integrantes del equipo:**

* Ismael Saucedo Martínez
* Marvin Meza Hurtado
* Arcadio Emmanuel Batres Ramirez
* Alan Osiel Ortega Díaz
* Omar Osvaldo Corral Villanueva