Universidad Autónoma del Estado de Hidalgo
Escuela Superior de Tizayuca

Licenciatura En Tecnologías de la Información

Sexto Semestre

Optativa 1 (Pruebas de Software (Software Testing))

Ramírez Corona Eder Geovanni

Seguridad en Paginas Web, Pishing e Inyecciones SQL

Meza Solís Lady Guadalupe

Numero de Cuenta: 435443

Seguridad en Páginas Web

El propósito de la seguridad web es prevenir ataques de cualquier clase. Mas formalmente, la seguridad es la acción/práctica de proteger sitios web del acceso, uso, modificación, destrucción o interrupción, no autorizados.

La seguridad de sitios web eficaz requiere de esfuerzos de diseño a lo largo de la totalidad del sitio web: en tu aplicación web, en la configuración del servidor web, en tus políticas para crear y renovar contraseñas, y en el código del lado cliente.

Amenazas contra la seguridad de sitios web

Cross-Site Scripting (XSS)

XSS es un término que se usa para describir una clase de ataques que permiten al atacante inyectar scripts de lado cliente, a través del sitio web, hasta los exploradores de otros usuarios. Como el código inyectado va del servidor del sitio al explorador, se supone de confianza, y de aquí que pueda hacer cosas como enviar al atacante la cookie de autorización al sitio del usuario. Una vez que el atacante tiene la cookie pueden iniciar sesión en el sitio como si fuera el verdadero usuario y hacer cualquier cosa que pueda hacer éste. Dependiendo de que sitio sea, esto podría incluir acceso a los detalles de su tarjeta de crédito, ver detalles de contactos o cambiar contraseñas, etc.

Amenazas contra la seguridad de sitios web

Cross-Site Scripting (XSS)

Vulnerabilidades XSS	
Reflejada	**Persistente**
Ocurre cuando contenido del usuario que se pasa al servidor se devuelve inmediatamente y sin modificar par que los muestre el explorador.	Es aquella en la que el script malicioso se almacena en el sitio web y luego más tarde se vuelve a presentar en pantalla sin modificar para que otros usuarios lo ejecuten involuntariamente.

Amenazas contra la seguridad de sitios web

Cross-Site Scripting (XSS)

La mejor defensa contra las vulnerabilidades XSS es eliminar o deshabilitar cualquier etiqueta que pueda contener instrucciones para ejecutar código. En el caso del HTML esto incluye etiquetas como <script>, <object>, <embed>, y <link>.

El proceso de modificar los datos del usuario de manera que no puedan utilizarse para ejecutar scripts o que afecten de otra forma la ejecución del código del servidor, se conoce como "desinfección de entrada" (input sanitization).

Suplantación de Identidad - Phishing

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito.

Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar.

A quien practica el phishing se le llama phisher.

Suplantación de Identidad - Phishing

Tipos de ataques de phishing

El denominador común de todos los ataques de phishing es el uso de un pretexto fraudulento para adquirir datos valiosos.

Suplantación de Identidad - Phishing

Spear phishing

Mientras la mayoría de las campañas de phishing envían correos electrónicos masivos al mayor número posible de personas, el spear phishing es un ataque dirigido. Spear phishing ataca a una persona u organización específica, a menudo con contenido personalizado para la víctima. Requiere un reconocimiento previo al ataque para descubrir nombres, cargos, direcciones de correo electrónico y similares. Los hackers buscan en Internet para relacionar esta información con lo que han averiguado sobre los colegas profesionales del objetivo, junto con los nombres y las relaciones profesionales de los empleados clave en sus organizaciones. Con esto, el autor del phishing crea un correo electrónico creíble.

Suplantación de Identidad - Phishing

Phishing de clonación

En este ataque, los delincuentes hacen una copia, o clonan, correos electrónicos legítimos enviados anteriormente que contienen un enlace o un archivo adjunto. Luego, el autor del phishing sustituye los enlaces o archivos adjuntos con contenido malicioso disfrazado para hacerse pasar por el auténtico. Los usuarios desprevenidos hacen clic en el enlace o abren el adjunto, lo que a menudo permite tomar el control de sus sistemas. Luego el autor del phishing puede falsificar la identidad de la víctima para hacerse pasar por un remitente de confianza ante otras víctimas de la misma organización.

Suplantación de Identidad - Phishing

419/Estafas nigerianas

Un extenso correo electrónico de phishing de alguien que afirmaba ser un príncipe nigeriano es una de las estafas más antiguas de Internet. Según Wendy Zamora, jefe de contenido de Malwarebytes Labs, “el phishing del príncipe nigeriano procede de una persona que afirma ser un funcionario del gobierno o miembro de una familia real que necesita ayuda para transferir millones de dólares desde Nigeria. El correo electrónico se marca como "urgente" o "privado" y su remitente solicita al destinatario que proporcione un número de cuenta bancaria para remitir los fondos a un lugar seguro”.

El número “419” está asociado con esta estafa. Hace referencia a la sección del código penal nigeriano que trata sobre fraude, los cargos y las penas para los infractores.

Suplantación de Identidad - Phishing

Phishing telefónico

Con los intentos de phishing a través del teléfono, a veces llamados phishing de voz o “vishing,” el phisher llama afirmando representar a su banco local, la policía o incluso la Agencia Tributaria. A continuación, le asustan con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa. Normalmente le piden que pague con una transferencia bancaria o con tarjetas prepago, porque son imposibles de rastrear.

Phishing vía SMS, o “smishing,” es el gemelo malvado del vishing, que realiza el mismo tipo de estafa (algunas veces con un enlace malicioso incorporado en el que hacer clic) por medio de un mensaje de texto SMS.

Suplantación de Identidad - Phishing

¿Cómo identificar un ataque de phishing?

- El correo electrónico hace una oferta que parece demasiado buena para ser verdad.
- Reconoce al remitente, pero es alguien con quién no trata.
- El mensaje suena aterrador.
- El mensaje contiene archivos adjuntos inesperados o extraños.
- El mensaje contiene enlaces que parecen un poco extraños.

Suplantación de Identidad - Phishing

¿Cómo protegerse del phishing?

- No abra correos electrónicos de remitentes que no le sean familiares.
- No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.
- Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no está seguro, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en su navegador.
- Busque el certificado digital del sitio web.

Suplantación de Identidad - Phishing

¿Cómo protegerse del phishing?

- Si se le pide que proporcione información confidencial, compruebe que la URL de la página comienza con “HTTPS” en lugar de simplemente “HTTP”. La “S” significa “seguro”. No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS porque es más seguro. Los sitios HTTP, incluso los legítimos, son vulnerables para los hackers.
- Si sospecha que un correo electrónico no es legítimo, seleccione un nombre o parte del texto del mensaje y llévelo a un motor de búsqueda para ver si existe algún ataque de phishing conocido que utiliza los mismos métodos.
- Pase el cursor del ratón por encima del enlace para ver si es legítimo.

Inyecciones SQL

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

El origen de la vulnerabilidad radica en la incorrecta comprobación o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté incrustado en otro.

Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

Inyecciones SQL

Un ataque de inyección con éxito, podría falsificar identidades, crear nuevas identidades con derechos de administración, acceder a todos los datos en el servidor o destruir/modificar los datos para hacerlos inutilizables.

Inyecciones SQL

Por ejemplo, asumiendo que el siguiente código reside en una aplicación web y que existe un parámetro "nombreUsuario" que contiene el nombre de usuario a consultar, una inyección SQL se podría provocar de la siguiente forma:

El código SQL original y vulnerable es:

```
consulta := "SELECT * FROM usuarios WHERE nombre = '" + nombreUsuario + "';"
```

Inyecciones SQL

Si el operador escribe un nombre, por ejemplo "Pepe", nada anormal sucederá, la aplicación generaría una sentencia SQL similar a la siguiente, que es perfectamente correcta, en donde se seleccionarían todos los registros con el nombre "Pepe" en la base de datos:

```
SELECT * FROM usuarios WHERE nombre = 'Pepe';
```

Pero si un operador malintencionado escribe como nombre de usuario a consultar:

```
Alicia'; DROP TABLE usuarios; SELECT * FROM datos WHERE nombre LIKE '%
```

Inyecciones SQL

se generaría la siguiente consulta SQL, (el color verde es lo que pretende el programador, el azul es el dato, y el rojo, el código SQL inyectado):

```
SELECT * FROM usuarios WHERE nombre = 'Alicia';
DROP TABLE usuarios;
SELECT * FROM datos WHERE nombre LIKE '%';
```

En la base de datos se ejecutaría la consulta en el orden dado, se seleccionarían todos los registros con el nombre 'Alicia', se borraría la tabla 'usuarios' y finalmente se seleccionaría toda la tabla "datos", que no debería estar disponible para los usuarios web comunes.

Inyecciones SQL

En resumen, cualquier dato de la base de datos puede quedar disponible para ser leído o modificado por un usuario malintencionado.

Nótese por qué se llama "Inyección" SQL. Si se observa el código malicioso, de color rojo, se notará que está insertado en el medio del código bueno, el verde. Así, el código rojo ha sido "inyectado" dentro del verde.

Blind SQL injection

"Ataque a ciegas por inyección SQL", en inglés, Blind SQL injection, es una función y una técnica de ataque que utiliza la inyección SQL. Se evidencia cuando en una página web, por un fallo de seguridad, no se muestran mensajes de error al no producirse resultados correctos ante una consulta a la base de datos, mostrándose siempre el mismo contenido (es decir, solo hay respuesta si el resultado es correcto).

Blind SQL injection

Algunas formas de evitar la Inyección SQL

- Ruby on Rails
- Perl
- PHP
- Java

Más información en: https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL

Actividad Individual

Responde las siguientes preguntas:

1. ¿Para qué se usa una base de datos?
2. ¿Qué es una base de datos?
3. ¿Qué es una SQL?
4. ¿Qué es una SQL Injection?
5. ¿Cuáles son las consecuencias de las SQL injection?
6. ¿Cuáles son las técnicas de explotación?