Actividad 9: Explotación y Mitigación de Remote File Inclusion (RFI)

Tema: *Inclusión de archivos remotos*

Objetivo: *Ejecutar código remoto y mitigarlo bloqueando URLs externas*

¿Qué es RFI?

RFI (**Remote File Inclusion**, Inclusión Remota de Archivos) es una vulnerabilidad de seguridad que ocurre cuando una aplicación web permite la inclusión de archivos desde una URL externa sin una validación adecuada. Esto puede permitir la ejecución de código malicioso en el servidor objetivo, comprometiendo la seguridad del sistema.

Código vulnerable

Crear el archivo **vulnerable**: `rfi.php`

El siguiente código PHP es vulnerable a RFI:

```
<?php
$file = $_GET['file'];
include($file);
?>
```

El código permite que un atacante incluya un archivo arbitrario desde una fuente externa. Si el archivo contiene código malicioso, se ejecutará en el servidor víctima. Puede llevar a la ejecución remota de comandos, robo de datos y comprometer el servidor.

Explotación de RFI

Subir un archivo malicioso *exploit.php* en un servidor controlado por el atacante:

```
<?php
echo "¡Servidor comprometido!";
// Código malicioso, como una web shell o un backdoor
?>
```

Ejecutarlo a través de la aplicación vulnerable (en nuestro caso en el mismo *localhost*):

```
http://localhost/rfi.php?file=http://localhost/exploit.php
```

Si el código del atacante se ejecuta en el servidor víctima, significa que la aplicación es vulnerable.

Posibles efectos del ataque:

- Acceso no autorizado al servidor.
- Robo de datos sensibles.
- Modificación o eliminación de archivos del sistema.
- Instalación de malware o puertas traseras (*backdoors*).

Mitigación de RFI

*** Bloquear la inclusión de URLs externas**

En lugar de permitir cualquier entrada sin validación, se debe bloquear la inclusión de archivos remotos:

```
<?php
// Obtener el parámetro 'file' de la URL
$file = $_GET['file'] ?? '';

// Bloquear URLs externas
if (filter_var($file, FILTER_VALIDATE_URL)) {
    die("Incluir archivos remotos está prohibido.");
}

// Incluir el archivo sin más restricciones (Aún vulnerable a LFI)
include($file);
?>
```

Sin embargo, esta solución no es suficiente, ya que aún permite archivos locales maliciosos.

*** Restringir las rutas de inclusión**

Limitar la inclusión de archivos solo a un directorio específico dentro del servidor:

```
<?php
// Obtener el parámetro 'file' de la URL
$file = $_GET['file'] ?? '';

// Lista blanca de archivos permitidos
$whitelist = ['allowed.php', 'config.php'];

if (!in_array($file, $whitelist)) {
    die("Acceso denegado.");
}

// Incluir solo archivos de la lista blanca
include($file);
?>
```

*** Usar rutas absolutas y sanitización**

Asegurar que solo se incluyan archivos desde una ubicación específica:

```
<?php
// Obtener el parámetro 'file' de la URL
$file = $_GET['file'] ?? '';
```

```
// Directorio base permitido
$base_dir = "/var/www/html/includes/";

// Normalizar la ruta y obtener solo el nombre del archivo
$real_path = realpath($base_dir . $file);
$clean_file = basename($real_path);

// Verificar que el archivo esté dentro del directorio permitido
if (!$real_path || strpos($real_path, $base_dir) !== 0) {
    die("Acceso denegado.");
}

// Incluir solo archivos dentro del directorio seguro
include($real_path);
?>
```

*** Deshabilitar *allow_url_include* en *php.ini***

Para prevenir la inclusión remota de archivos en PHP:

```
allow_url_include = Off
```

Esta opción debe configurarse en el servidor y previene ataques RFI globalmente.

*** Validación estricta de entradas**

Nunca confiar en los datos de entrada del usuario. Usar listas blancas, validaciones y escapes adecuados.

Comando para deshabilitar la seguridad en PHP 8.2 (sólo para pruebas)

Realizar antes de cada actividad para deshabilitar la seguridad y así poder trabajar la vulnerabilidad correctamente.

Ejecutar el siguiente comando en la terminal **como root** para modificar *php.ini* y así deshabilitar todas las restricciones:

```
sudo sed -i 's/^disable_functions.*/disable_functions =/' /etc/php/8.2/apache2/php.ini && \
sudo sed -i 's/^allow_url_include.*/allow_url_include = On/' /etc/php/8.2/apache2/php.ini &&
\
sudo sed -i 's/^allow_url_fopen.*/allow_url_fopen = On/' /etc/php/8.2/apache2/php.ini && \
sudo sed -i 's/^open_basedir.*/;open_basedir =/' /etc/php/8.2/apache2/php.ini && \
sudo systemctl restart apache2
```

¿Qué hace este comando?

1. Elimina todas las funciones deshabilitadas (*disable_functions vacío*).
2. Habilita la inclusión de archivos remotos (*allow_url_include = On*).
3. Habilita *file_get_contents()* para URLs externas (*allow_url_fopen = On*).
4. Desactiva *open_basedir* para permitir la ejecución en cualquier directorio.
5. Reinicia Apache para aplicar los cambios.