

RFI, LFI, CSRF,... WTF?!



Pedro Laguna
pedlagdur@gmail.com

Rafael Vargas
rafavargas@ieee.org

Agenda

- Zero-day
- Remote File Inclusion
 - Shell Remotas
- Local File Inclusion
 - Canonicalización
- Cross Site Request Forgery

Atención/Disclaimer

- En la realización de esta charla ningún desarrollador de Open Source fue maltratado o humillado.
- Algunas vulnerabilidades que vamos a mostrar no están arregladas y son actualmente explotables.
- Los desarrolladores serán avisados tras la charla.



Zero-day

- Vulnerabilidad publicada **sin conocimiento previo** de los responsables del software.
- No es una practica recomendable.
- A las chicas le gustan los hackers malotes... ;)



Remote File Inclusion

- RFI para los amigos.
- Permite la carga de un fichero remoto en el contexto de la aplicación.
- Adquiere valor cuando este código es interpretado y ejecutado.
- Especial hincapié en **lenguajes no compilados**.



RFI en PHP

- Requiere de una configuración deficiente en el fichero php.ini
 - `allow_url_fopen = On`
- También influye una programación descuidada
 - Variables sin inicializar
 - Carga de ficheros de manera dinámica
- `include()`, `require()`, `include_once()`, `require_once()` son nuestras amigas/enemigas

Shells Remotas

- Permiten ejecutar comandos en la aplicación víctima.
- Existen multitud de shells disponibles, a destacar:

- C99

- R75

- <?

```
system($_GET['cmd']);
```

```
?>
```



RFI en ASP.NET

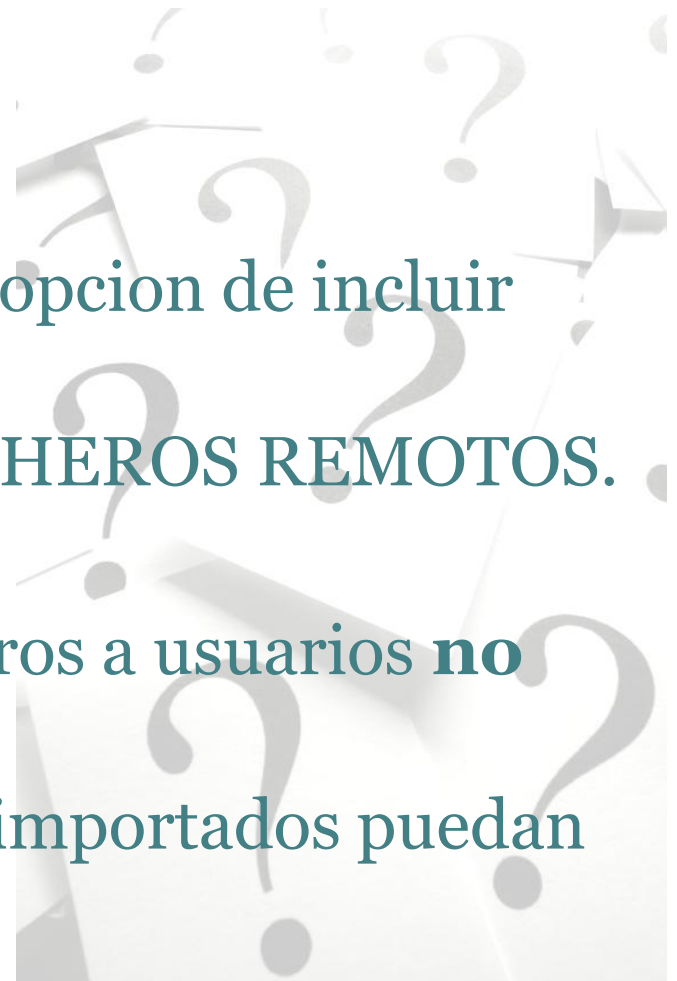
- Distinto de la definición original.
- Suelen darse menos casos por su diseño y forma de trabajar.
- Igualmente destructivo.
- Delegar el control de acceso en el .NET Framework es la causa más común.

Demo



¿Soluciones RFI?

- PHP:
 - Si usamos PHP desactivar la opción de incluir ficheros remotos.
 - Obviamente... **NO USAR FICHEROS REMOTOS.**
- ASP.NET:
 - No permitir “importar” ficheros a usuarios **no autenticados.**
 - No permitir que los ficheros importados puedan **ser ejecutados.**



Local File Inclusion

- LFI para los amigos.
- Permite la inclusión de ficheros a los que tenga acceso local la aplicación.
- Paginas de plantilla las más vulnerables.
- El problema es el desarrollador, no la plataforma.



LFI en PHP

- De nuevo nuestras amigas:
 - `include()`
 - `include_once()`
 - `require()`
 - `require_once()`
- Pueden imponernos la extensión, pero podemos ignorarla: (`magic_quotes_gpc = Off`)
 - `include($_GET['pagina'] . ".txt");`
`// ?pagina=/etc/passwd%00`

LFI en ASP.NET

- Handlers (.ashx) de descarga.
- También en los de imágenes o parecidos.
- No validar el padre del contenido al que se accede.
 - Errores de canonicalización.
 - Uso de wildcards.

LINEA DE SEGURIDAD

LFI en servidores web

- Por defecto, los servidores web se instalan con una cuenta de usuario del sistema.
- Este usuario puede acceder a cualquier fichero del sistema:
 - C:\Windows\repair\SAM
 - /etc/passwd
- Deben limitarse sus privilegios.
 - Los de ejecución.
 - Los de lectura y escritura.



Canonicalización

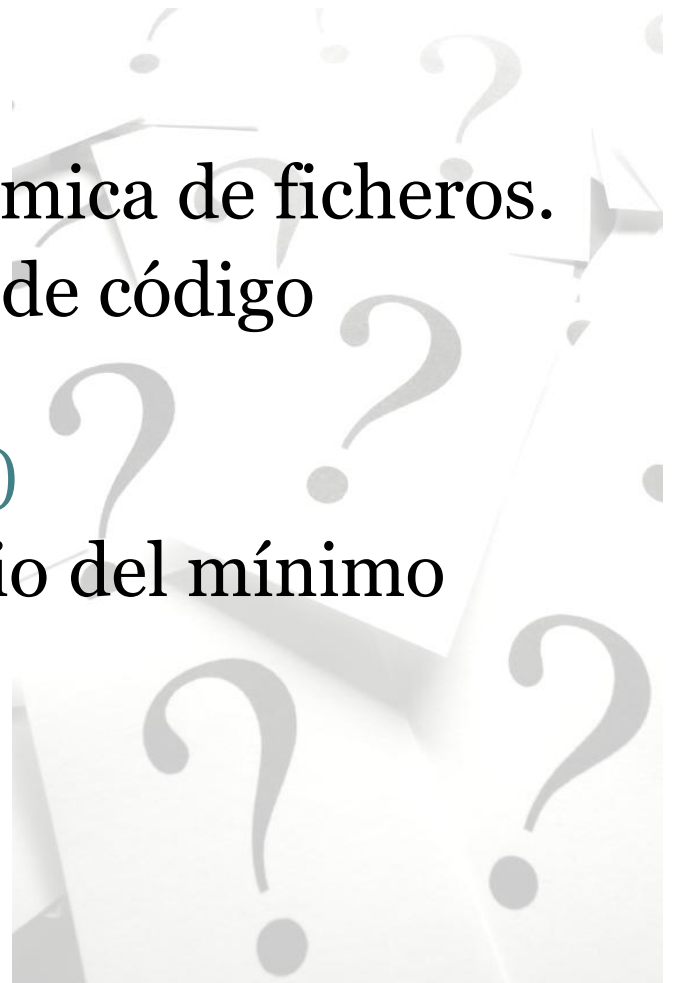
- Problema del cambio de base.
- Hay 10 tipos de personas, los que saben binario y los que no.
 - $10_{(2)} == 2_{(10)}$
- Rutas relativas versus rutas absolutas.
 - `C:\Windows\notepad.exe`
 - `..\..\..\..\Windows\notepad.exe`
 - Algunos se olvidaron del viejo `cd ..` de DOS.
- El problema del `String.Format`

DEMO



¿Soluciones LFI?

- Limitar uso de descarga dinámica de ficheros.
- Asegurar la ruta de carga desde código
 - `basename()` (PHP)
 - `FileInfo.Directory` (ASP.NET)
- Asegurar el servidor, principio del mínimo privilegio
 - `mod_chroot`
 - Permisos en carpetas



Cross Site Request Forgery

- CSRF ó XSRF para los amigos.
- Íntimamente relacionado con XSS.
- Sustentado en la mala (nula) verificación de la procedencia de las peticiones.
- Necesita un usuario autenticado en la aplicación para realizar las acciones privilegiadas.

Ejemplos CSRF

- La manera más fácil de realizar un ataque CSRF es mediante la etiqueta ``
 - ``
- El navegador realiza una petición para traerse la “imagen”.
- Se pueden realizar ataques más complejos mediante JavaScript incrustado en cualquier página.

DEMO



¿Soluciones CSRF?


- Comprobar la cabecera Referer del navegador.
 - Fácilmente “spoofeable”.
- Enviar todos los parámetros mediante POST
 - Se puede igualmente vulnerar, pero es mas complicado y tedioso.
- Llevar un parámetro mediante campos hidden y comprobarlo en servidor.
 - Mucho mas complejo para modificar.

Más información

- Equilibrio Inestable
<http://www.equilibrioinestable.com/>
- Vargas & Software Development
<http://rafavargas.wordpress.com/>
- El lado del mal
<http://elladodelmal.com/>
- Google & Wikipedia ;)



¿Preguntas? ¿Sugerencias?
¿Hackear hotmail? ;)



Pedro Laguna
pedlagdur@gmail.com

Rafael Vargas
rafavargas@ieee.org