Curso de Programación en PHP

Nivel I

Facultad de Ciencia y Tecnología - Oro Verde - v2.1

Capítulo 6: Seguridad en PHP

Seguridad en formularios de sesión

Command Injection

Hosting compartido

Algunas opciones más de php.ini

Session Fixation

Es uno de los temas más avanzados y existen tres formas (métodos) de obtener un identificador de sesión válido en una aplicación Web:

- **Predicción**
- **Fuerza bruta**
- **Captura**

Session Fixation (continuación)

Existen tres formas (métodos) de obtener un identificador de sesión válido en una aplicación Web:

Predicción refiere a adivinar un identificador de sesión válido. Con el mecanismo de sesiones de PHP, el identificador de sesión es aleatorio, por lo que se hace poco probable que sea el punto más débil en su implementación.

Captura de un identificador de sesión válido. Esto puede hacerse mediante XSS, sniffing, etc. Consiste en interceptar el tráfico entre el cliente y el servidor web y extraer así los identificadores de session generados. También pueden extraerse las credenciales de acceso del usuario que se loguea.

La **fuerza bruta** consiste en lanzar ataques que prueben credenciales de accesos contra un formulario web. Una forma de mitigar esto sería que dicho formulario permita *tres* intentos de login y luego redirija la navegación a otro script o pida un captcha.

Clase 12: Seguridad en formularios de sesión

Ejemplo de mitigar la fijación de sesión

```
<?php

session_start();

if (!isset($_SESSION['initiated']))
{
    session_regenerate_id();
    $_SESSION['initiated'] = true;
}
```

Clase 12: Seguridad en formularios de sesión

Session Hijacking (secuestro)

Viene a reforzar la identificación del cliente para evitar el robo del ***id*** de sesión, con lo cual utilizaremos información del header de http para obtener un identificador adicional del cliente que accede a nuestro sitio Web.

$_SERVER['HTTP_USER_AGENT']

Mozilla/5.0 (Windows NT 5.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1

Clase 12: Seguridad en formularios de sesión

Session Hijacking (continuación)

Ejemplo de mitigar la session Hijacking

proceso.php

```
<?php

session_start();

// Después de hacer un buen login
...

$_SESSION['HUA'] = md5($_SERVER['HTTP_USER_AGENT']);
```

Clase 12: Seguridad en formularios de sesión

Session Hijacking (continuación)

Ejemplo de mitigar la session Hijacking

chequear.php

```
<?php

session_start();

// Después de hacer otros chequeos
...

if ($_SESSION['HUA'] != md5($_SERVER['HTTP_USER_AGENT'])) {
    header("Location: /login/includes/logout.php");
}
```

Capítulo 6: Seguridad en PHP

~~Seguridad en formularios de sesión~~

Command Injection

Hosting compartido

Algunas opciones más de php.ini

Command Injection

La inyección de comandos se puede llevar a cabo desde inclusiones dinámicas no controladas.

Ejecutando comandos del sistema operativo con las funciones exec(), shell_exec(), passthru() y system().

Ejemplo:

```
echo exec('whoami');
$ultima_fila = system('dir c: ', $directorios);
```

Clase 12: Command Injection

Command Injection (continuación)

Para mitigar la ejecución de comandos del SO debemos modificar la opción disable_functions del archivo php.ini.

disable_functions = exec, passthru, shel_exec, system

Capítulo 6: Seguridad en PHP

~~Seguridad en formularios de sesión~~

~~Command Injection~~

Hosting compartido

Algunas opciones más de php.ini

Clase 12: Hosting compartido

Hosting compartido

Almacenamiento de archivos de sesión

Directorios de base para abrir archivos desde PHP

Exposición de los archivos en el servidor Web

Clase 12: Hosting compartido

Hosting compartido (continuación)

Almacenamiento de archivos de sesión

Mayor exposición de los archivos de sesión que se guardan en **/tmp** para todos los sitios que residen en un servidor.

Clase 12: Hosting compartido

Hosting compartido (continuación)

Exposición de los archivos en el servidor

Mayor exposición de los archivos del proyecto en el servidor. Se pueden realizar un script para obtener los archivos de nuestro proyecto u otros alojados en el mismo servidor.

Capítulo 6: Seguridad en PHP

~~Seguridad en formularios de sesión~~

~~Command Injection~~

~~Hosting compartido~~

Algunas opciones más de php.ini

Clase 12: Algunas opciones más de php.ini

Algunas opciones más de php.ini

Activar el reconocimiento de etiquetas reducidas en PHP.

short_open_tag = On

Activar el reconocimiento de etiquetas tipo asp en PHP.

asp_tags = On

Clase 12: Algunas opciones más de php.ini

Algunas opciones más de php.ini (continuación)

Desactivar la exposición de la firma (signature) de PHP en la cabecera http de nuestro servidor Web.

expose_php = Off

Clase 12: Algunas opciones más de php.ini

Algunas opciones más de php.ini (continuación)

Establecer el tamaño máximo de memoria que puede consumir un script.

memory_limit = 128

Clase 12: Algunas opciones más de php.ini

Algunas opciones más de php.ini (continuación)

Permitir la subida de archivos desde http usando un script PHP.

file_uploads = On

Especificar un directorio temporario para los archivos subidos al servidor utilizando http y PHP.

upload_tmp_dir = /tmp

Clase 12: Algunas opciones más de php.ini

Algunas opciones más de php.ini (continuación)

Especificar el tamaño máximo de los archivos a subir utilizando http y un script PHP.

upload_max_filesize = 2M

Especificar una cantidad máxima de archivos a subir al servidor http.

max_file_uploads = 20

Clase 12: Algunas opciones más de php.ini

Algunas opciones más de php.ini (continuación)

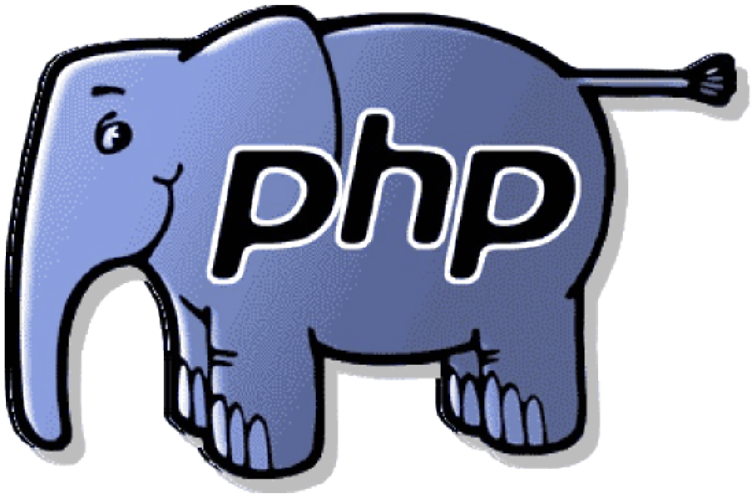
Especificar la ruta donde se guardaran los datos de las distintas sesiones que se creen en el servidor.

session.save_path = /tmp

Especificar el tiempo de vida de una sesión.

session.cookie_lifetime = 120

¿Dudas?



¿Consultas?

Información de contacto

Vía Web:

http://www.gugler.com.ar

http://campusvirtual.gugler.com.ar

Vía Mail:

contacto@gugler.com.ar

soporte@gugler.com.ar

capacitacion@gugler.com.ar

cursos@gugler.com.ar

Versión 2.1