# Desarrollo Seguro de Aplicaciones 2016

## Servicio Vulnerable (CTF)


### Autores.

Juan Fernández Sosa(265/1), Martín Daniel Cantarini (272/0) y Nicolas Ferrario(310/7)


### Dependencias.

No se utilizan

### Vulnerabilidad.

La vulnerabilidad desarrollada es del tipo File Upload. Un usuario sube un archivo malicioso al servidor, para ejecutar, por ejemplo, un comando del sistema operativo.

**Como setear un flag.**

El flag debe ser establecido en un archivo de texto. En nuestro caso, el archivo será almacenado dentro del directorio donde se guardan las imágenes que se suben desde la aplicación.

Por defecto, en nuestra aplicación, las imágenes se almacenarán en una carpeta llamada "imagenes" del servidor que debe ser creada con permisos de escritura para los usuarios, en caso de querer modificar esto, se debe cambiar el archivo carga.php la variable "$target_path".

**Forma de explotarlo.**

Para explotar esta vulnerabilidad lo que se hace es subir un archivo php con código malicioso, interceptar el request, modificar el valor del Content Type como si fuese una imagen para engañar al script y así que lo pueda almacenar. Una vez almacenado, se accede al archivo desde la URL y al abrirlo se ejecutará el comando que se encuentra en él.

Una de las maneras de explotar la vulnerabilidad es:

*1-* Nos dirigimos a la aplicación: *index.php* donde completamos (no es obligatorio) los campos "ubicación", "descripción", y seleccionamos una imagen. Si enviamos el formulario obtendremos un mensaje de éxito donde aparecerá un link a la imagen. Dirigiéndonos a ese link, podemos ver que la URL es algo del estilo SERVIDOR/CARPETA_IMAGENES/archivo.jpeg/png

Uno podría preguntarse si es vulnerable a ataques del tipo File Upload y tratar de ejecutar un comando, por ejemplo “ls” para obtener el listado de archivos en esa carpeta.

2- Sabiendo esto, se crea un archivo con extensión php, cuyo contenido sea:

//exploit.php

```
<?php
        system(“ls”);
?>
```

*// el comando a ejecutar, para encontrar el flag será “ls” si el archivo de texto que contiene el flag se encuentra dentro de la carpeta donde se almacenan las imágenes; o “ls ../” si se encuentra en el directorio padre.*

3- Cuando queremos enviar en el formulario nuestro archivo malicioso, vamos a obtener un mensaje de error, ya que sistema solo deja subir archivos en formato jpeg o png. Para poder subirlo es necesario utilizar alguna herramienta para interceptar y modificar los headers y parámetros que se envían por POST. En nuestro caso utilizamos la herramienta para reenviar peticiones que incluye el software de OWASAP-ZAP, pero también se pueden usar otras como el complemento de firefox Tamper Data.

En primer lugar es necesario tener instalado el software OWASAP-ZAP y luego nos dirigimos al formulario, en el cual ya seleccionamos el script php que queremos subir y presionamos enviar, si está configurado el proxy correctamente como localhost, OWASAP-ZAP reconocerá el request http y podremos reenviar la petición modificando los parámetros que enviamos a través de post.

El parámetro que debemos modificar es **Content-Type: text/php** por **Content-Type: image/jpeg** presionamos “send” y obtenemos la respuesta una vez realizado ese nuevo request. En caso de éxito, se mostrará un mensaje indicando que el archivo se subió correctamente y un link a ese archivo con la url correspondiente.

4- Si vamos al link se ejecutará el script mostrando la salida del comando ingresado en él. Si el comando fue “ls” nos mostrará el listado de los archivos presente en el directorio donde se almacenan las imágenes, allí se encontrará el archivo del flag.

5- Ubicado el archivo del flag, accedemos a través de la URL a él para obtener el flag.

**Video explicativo:**

https://www.youtube.com/watch?v=xje9zRwTOk0