POC - Exploit del Mundo Real

Análisis de Vulnerabilidades

Pacheco Franco Jesús Enrique

jesus.pacheco@bec.seguridad.unam.mx

11/Abril/2019

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.

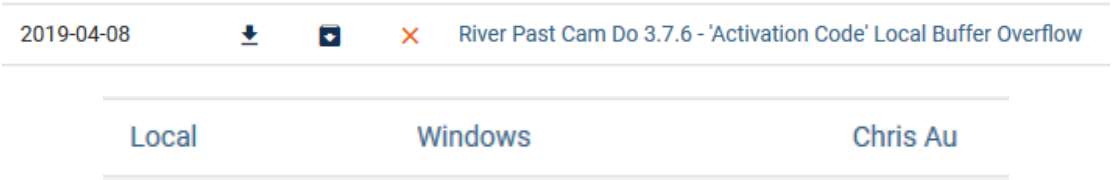
Obtención

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 catalogo 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.

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

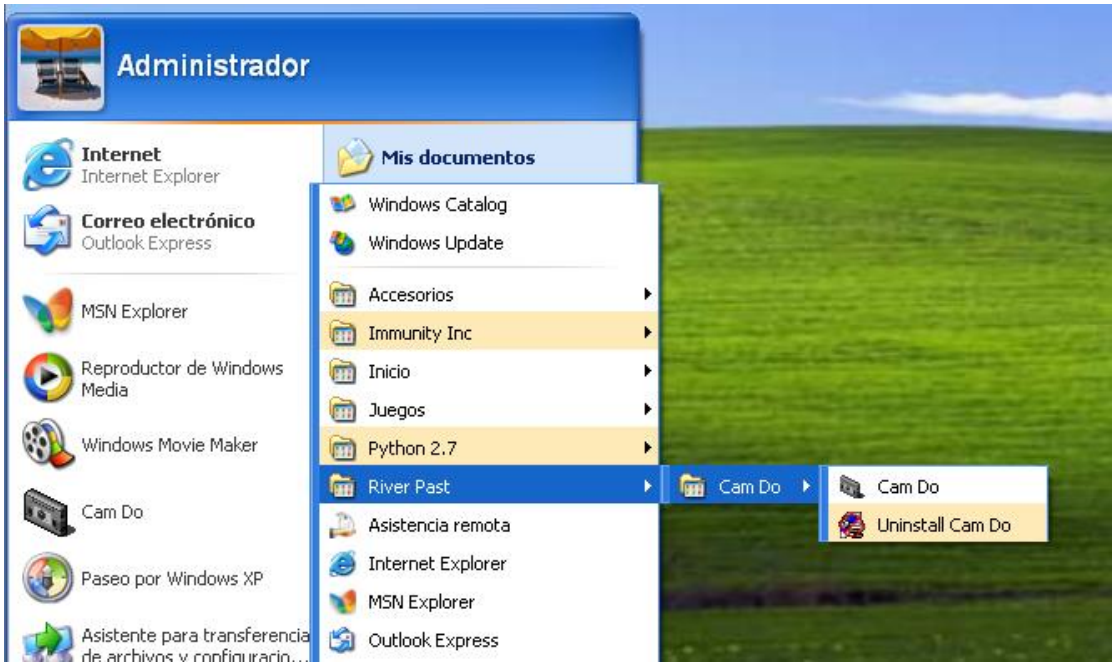
Para esta prueba de concepto el exploit a utilizar es el que se muestra a continuación.



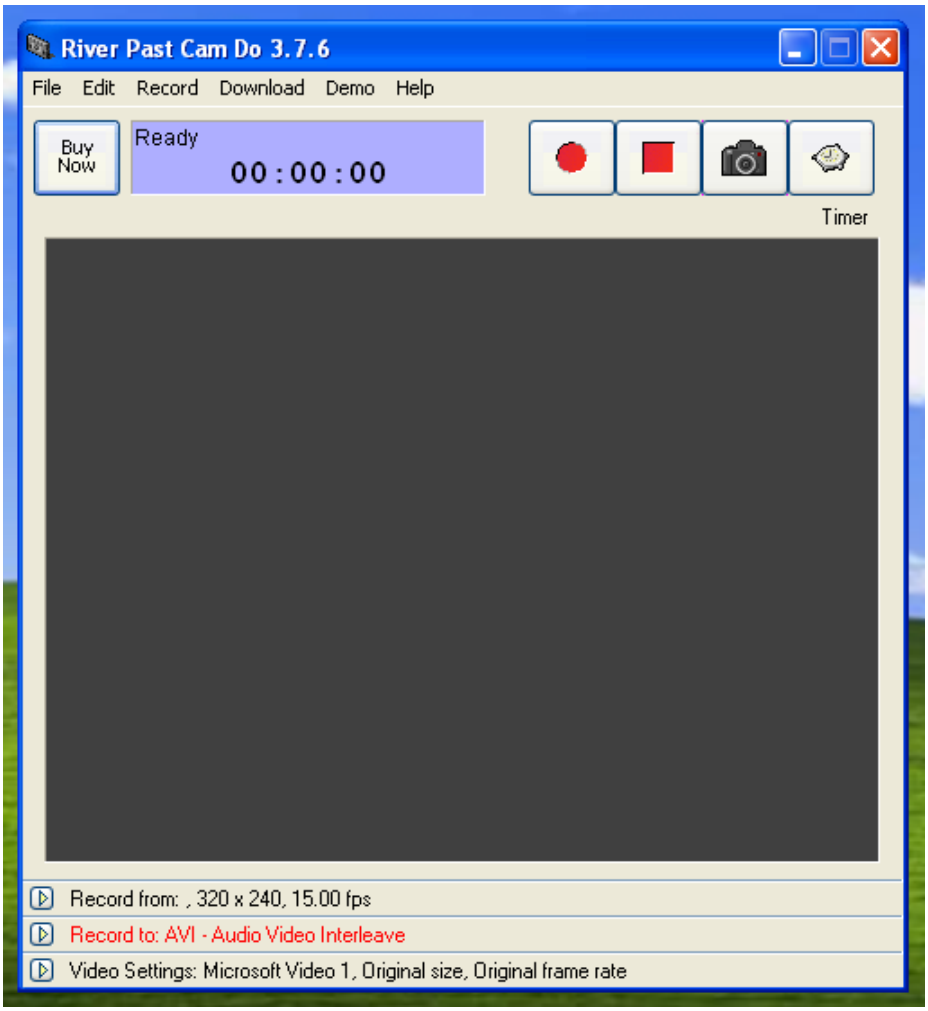
https://www.exploit-db.com/exploits/46670

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 bufferoverflow en el código de activación del producto.

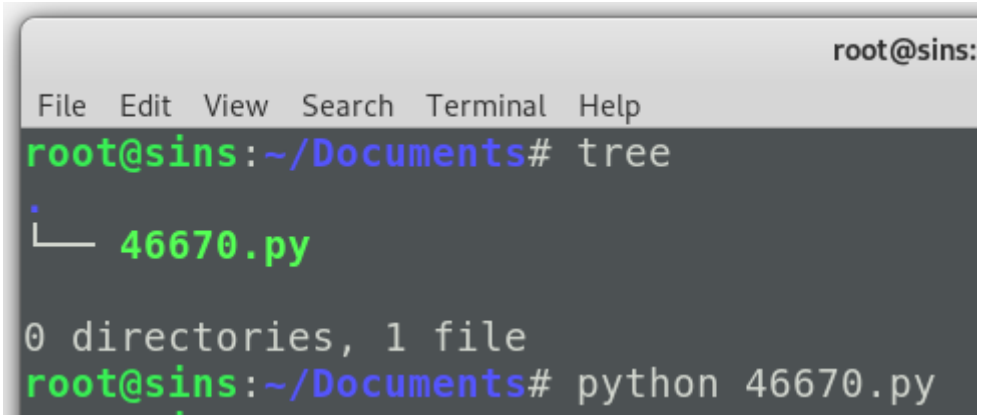


Ruta al programa vulnerable instalado.

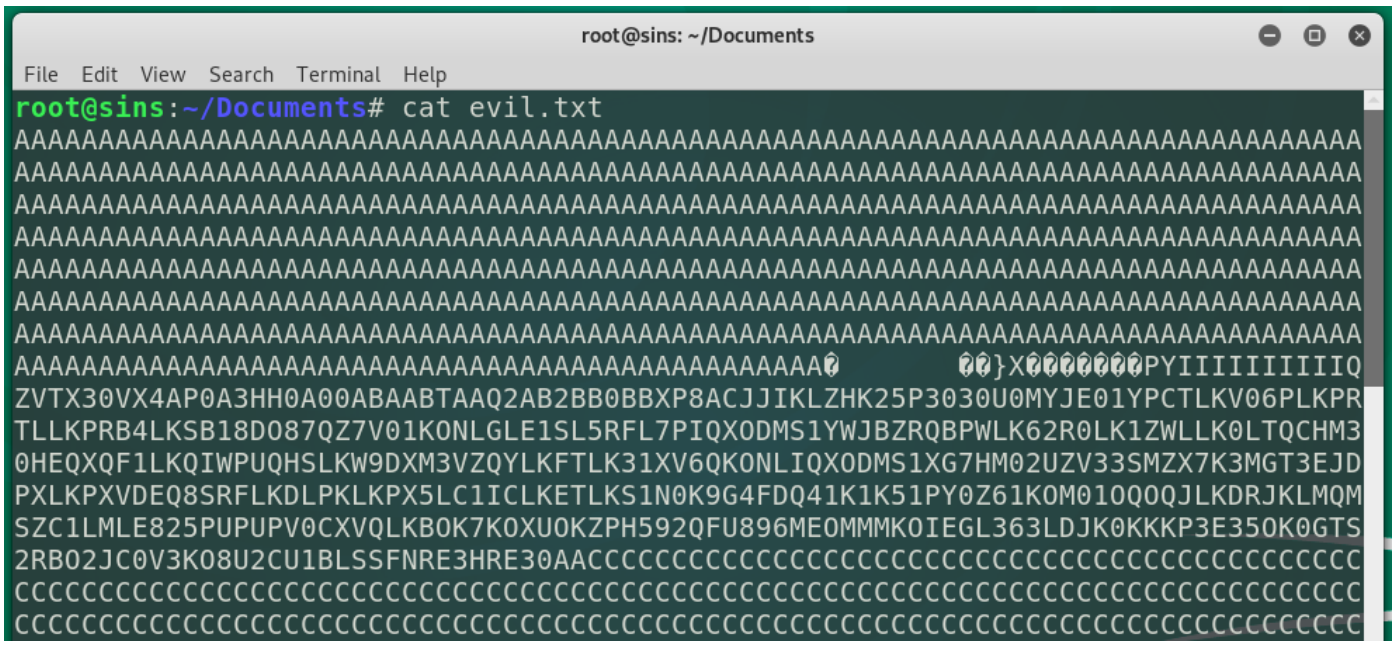


Pantalla del programa en ejecución.

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 bufferoverflow.

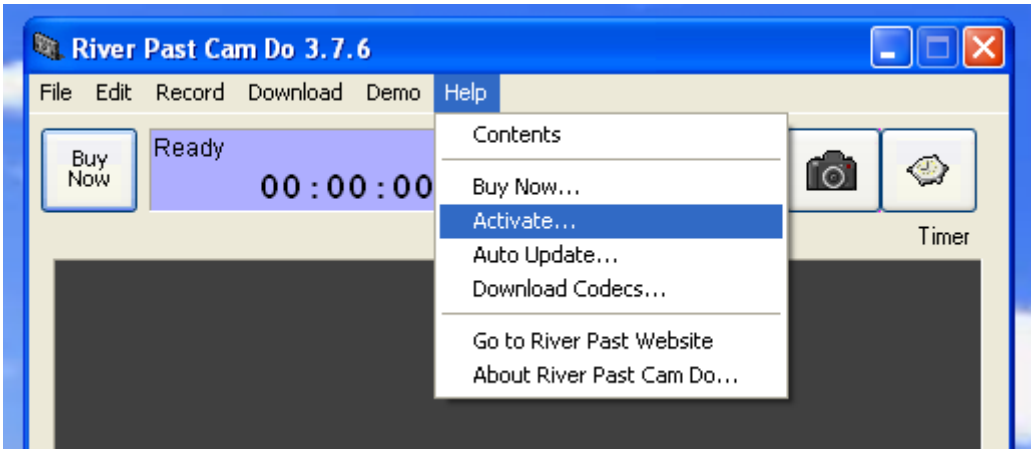


Generación de cadena maliciosa.

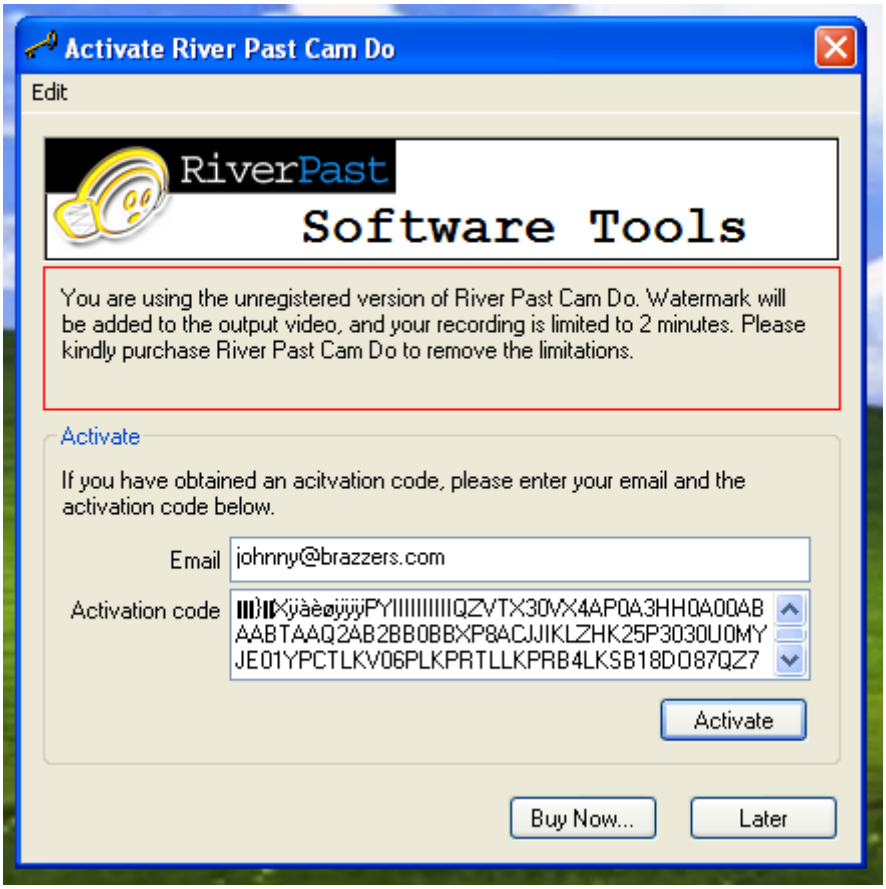


Contenido de la cadena maliciosa.

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.

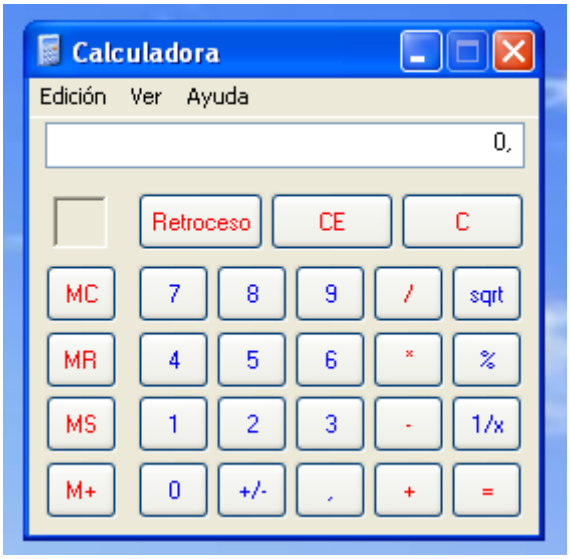


Accediendo a la sección de activación.



Colocación de la cadena maliciosa.

Al dar clic en Activate se cerrará la el programa actual y se abrirá la calculadora como resultado del bufferoverflow.



Calculadora abierta con bufferoverflow.