# Beyond good ol' Run key, Part 77

This is one more about hh.exe program that is used when you open the .chm files.

The hh.exe functionality is implemented by the hhctrl.ocx library. When hh.exe is started it tries to find the hhctrl.ocx library by checking the following Registry value:

```
HKCR\CLSID\{52A2AAAE-085D-4187-97EA-8C30DB990436}\InprocServer32
```

The library that the value points to is then loaded.

If the library doesn't exist, or the loading didn't succeed the hh.exe gives it another go and attempts to load the library using the hard-coded name hhctrl.ocx and relying on the LoadLibrary function (and as a result is a subject to side-loading attacks).

As such, there seem to be at least 2 opportunities here:

- Drop c:\WINDOWS\hhctrl.ocx and delete the HKCR\CLSID\{52A2AAAE… value so running hh.exe will sideload the c:\WINDOWS\hhctrl.ocx
- Replace the value of the HKCR\CLSID\{52A2AAAE… to point to your own lib and run hh.exe – this will load the lib of choice

Both can be used as a LOLBin / Persistence trick (or a combo).

This entry was posted in **Anti-***, **Autostart (Persistence)**, **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.