

A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the date.

3/10/2022

Sandbox User Manual

Student Id: 202124070

User manual index

About tool	2
What the tool is capable of?	3
How to use?	4
Opening the SandBox-202124070.exe file	4
Examples for restricting permissions using UI	8
Through Command Line	10
Examples for restricting permissions using commands	15
Permissions	17
Permissions used in the tool and their capabilities	17
Limitations of the tool	18
References	18

About tool

The Sandbox tool is implemented using C# and Windows forms for the UI. This tool provides a secure environment in which executable files can run with configuring various types of permissions. In addition, the tool can be run in two ways. First, can be executed by double-clicking on the .exe file, in which it will launch the tool with user interface. Second, by using command line, please refer the command line section for more details (page no 10).

What the tool is capable of?

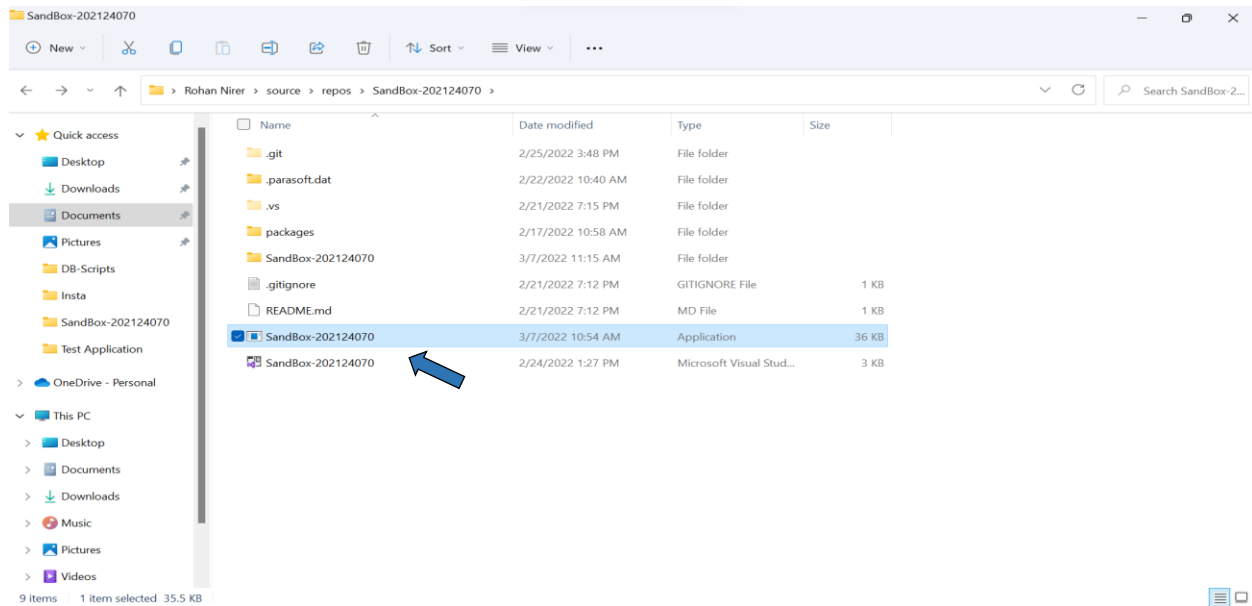
- The tool can be started in one of two ways: by running the SandBox-202124070.exe file, or by using the command line (details are provided in next section).
- The tool performs exactly like sandbox, means the application that opened through sandbox tool will not appear in the windows task manager, so it runs virtually.
- The tool can configure 8 different types of permissions (details are provided in the permissions sections).
- The tool can configure default permissions and run the untrusted application when we pass `-config default` in the command line (for more details refer page no 10).
- The tool can omit all the command keys when we pass `--help` in command line.
- The tool can successfully execute a .exe files which are compiled and built in C#.
- The tool will print some logs in the console while its running.

How to use?

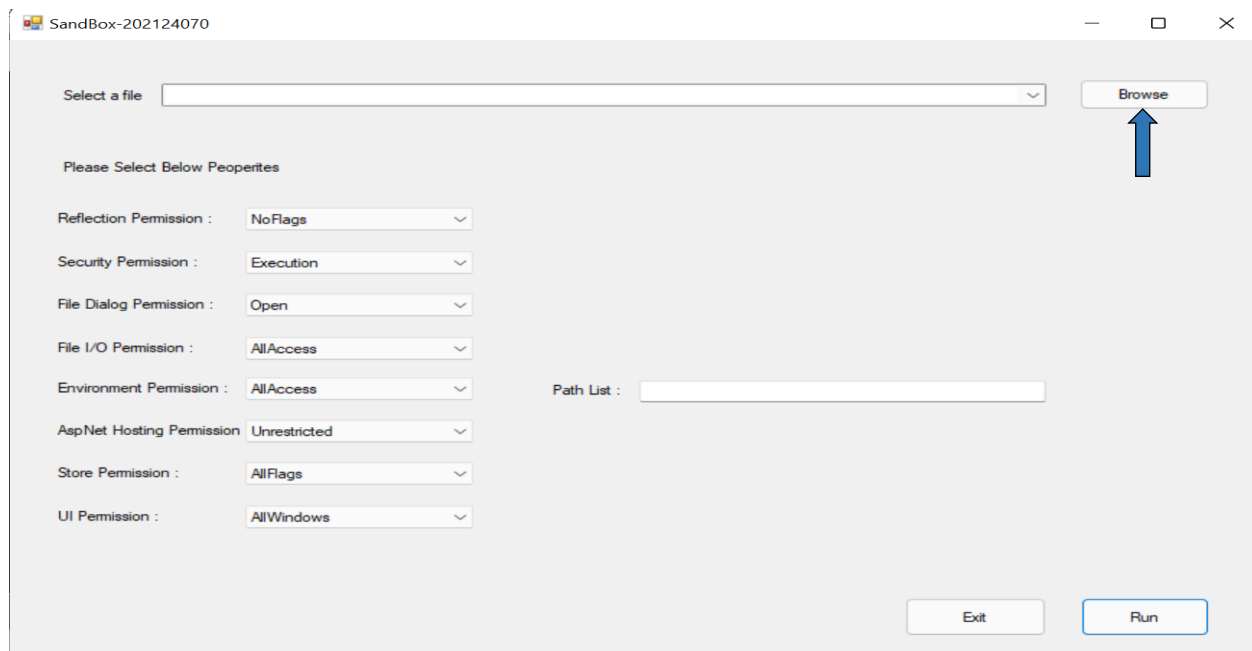
- Opening the SandBox-202124070.exe file.
- Through command line.

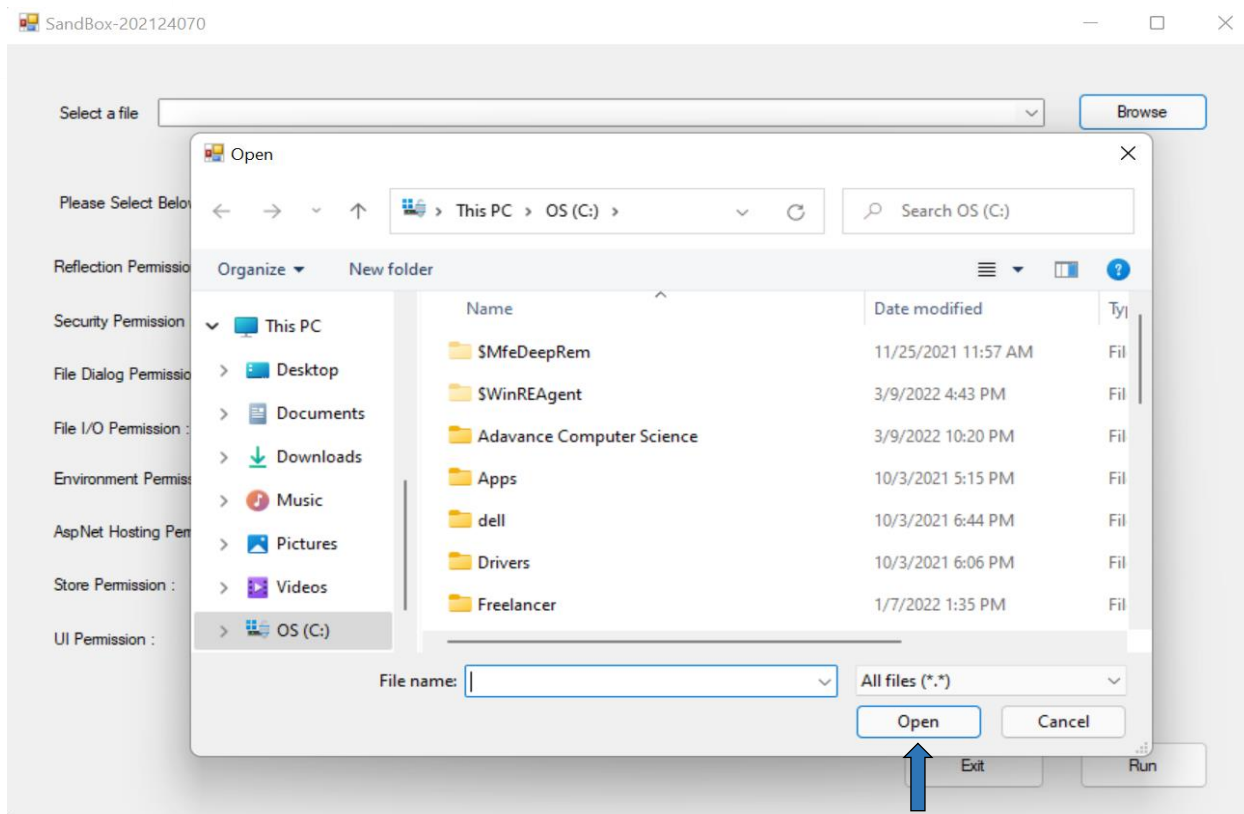
Opening the SandBox-202124070.exe file

1. Double click on the SandBox-202124070.exe.

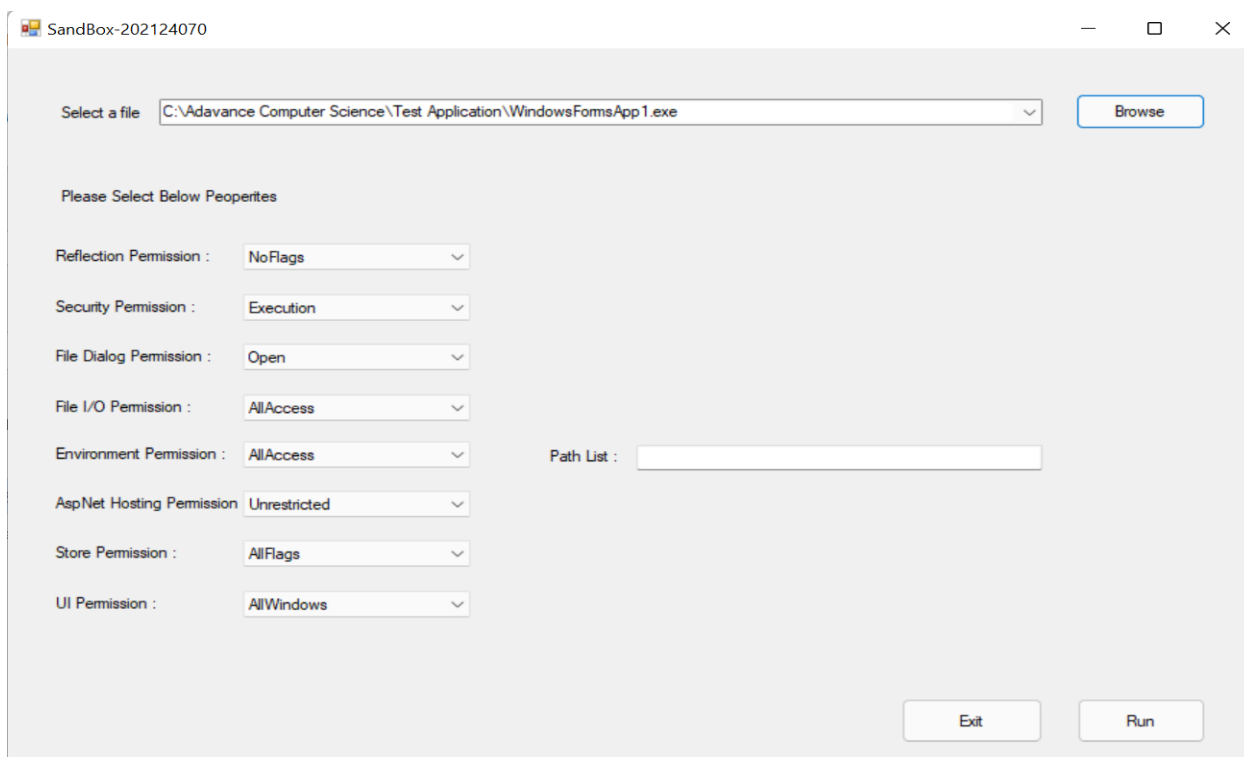


2. SandBox-202124070 window will open, as given below and click on Browse button and system files window will appear and select the file and click on Open button.

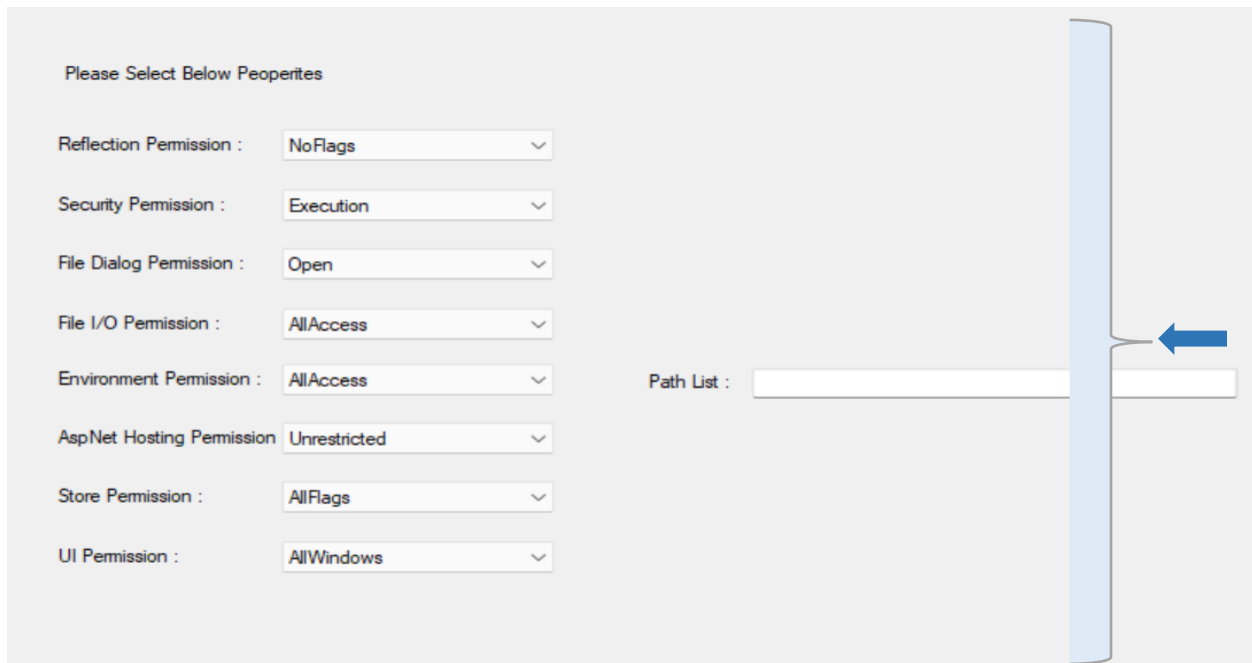




After selecting the file, the application window will look like as below, and the selected file and path will show in Select a file box.



3. Select the permissions properties from the dropdowns, if user does not enter any Path List the application will pick default value from the system.

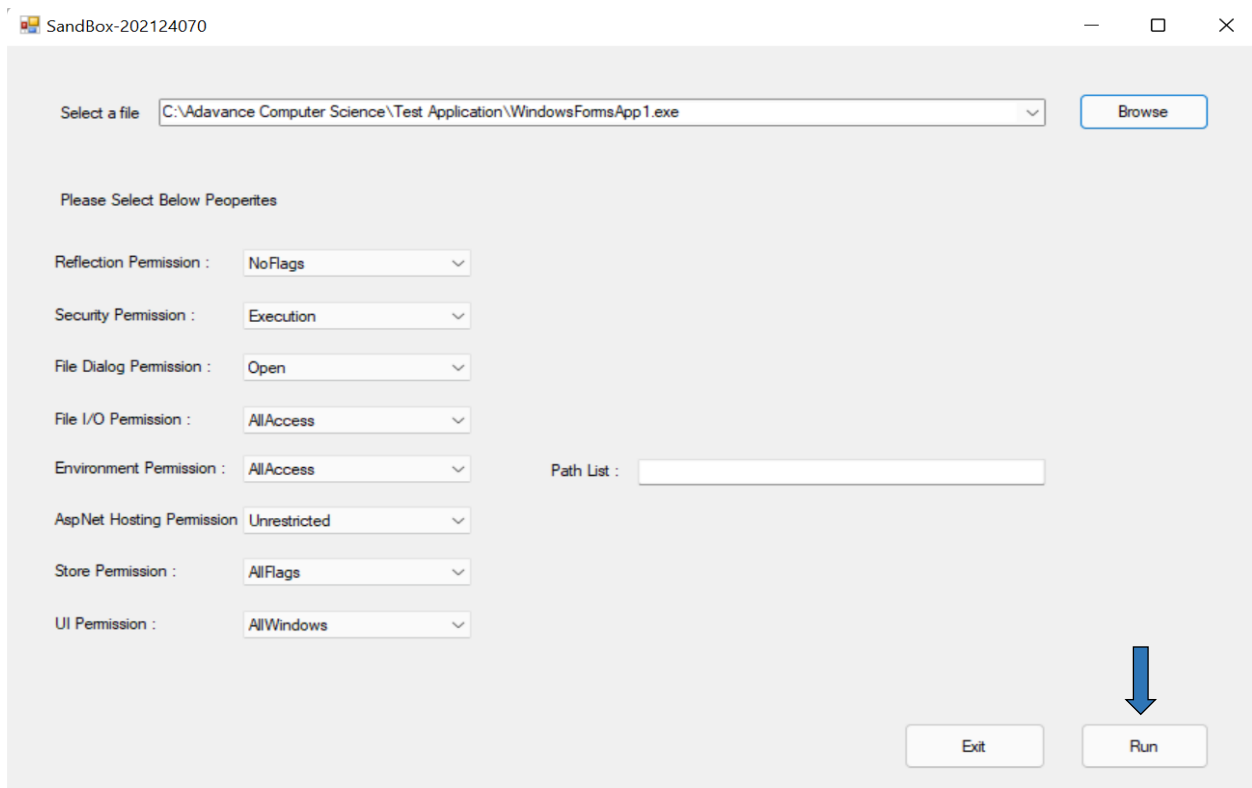


Please Select Below Properties

Reflection Permission :	NoFlags	▼
Security Permission :	Execution	▼
File Dialog Permission :	Open	▼
File I/O Permission :	AllAccess	▼
Environment Permission :	AllAccess	▼
AspNet Hosting Permission	Unrestricted	▼
Store Permission :	AllFlags	▼
UI Permission :	AllWindows	▼

Path List :

4. Now click on the Run button to execute the executable file which you have selected.



SandBox-202124070

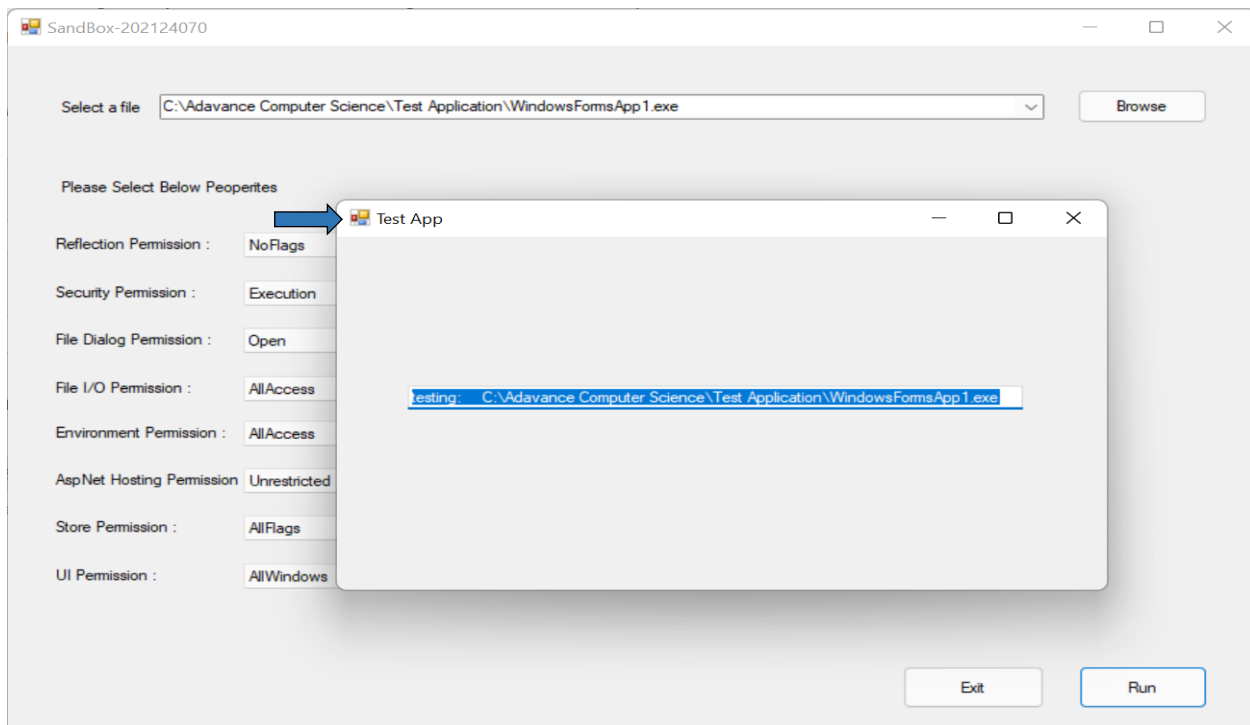
Select a file

Please Select Below Properties

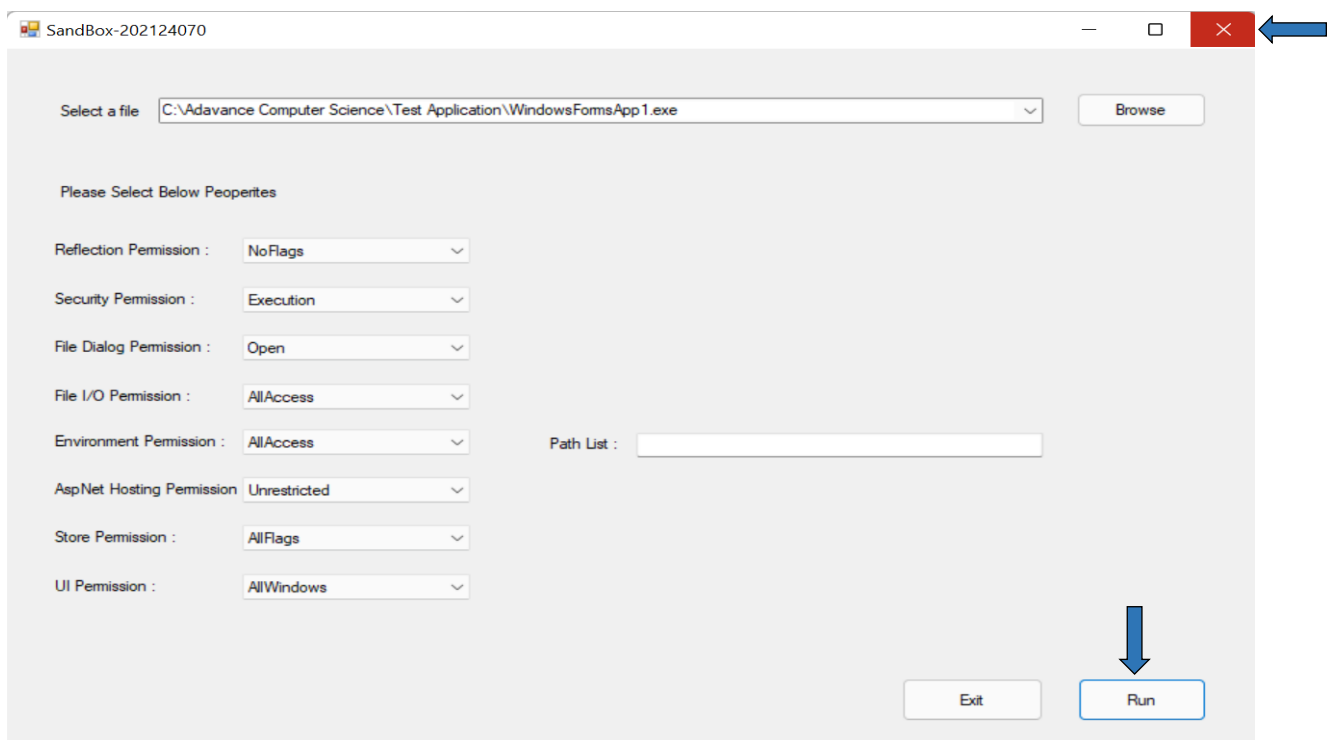
Reflection Permission :	NoFlags	▼
Security Permission :	Execution	▼
File Dialog Permission :	Open	▼
File I/O Permission :	AllAccess	▼
Environment Permission :	AllAccess	▼
AspNet Hosting Permission	Unrestricted	▼
Store Permission :	AllFlags	▼
UI Permission :	AllWindows	▼

Path List :

5. After clicking on Run button, the selected application will open, as given below.

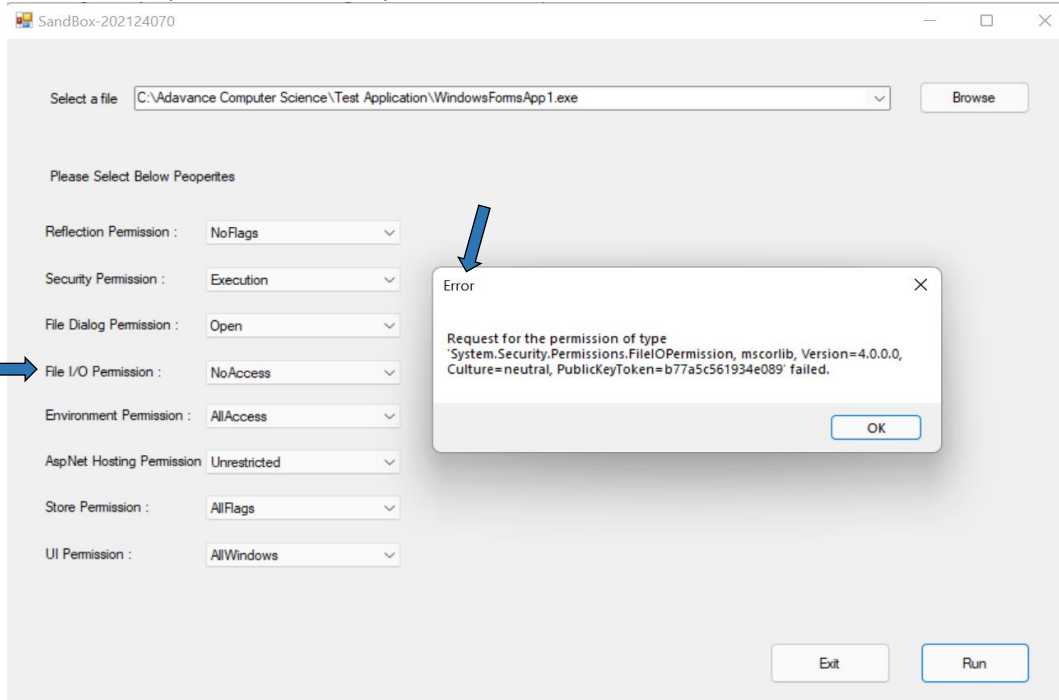


6. To terminate the Sandbox tool, click on exit button or you can click on red close button in the title bar.

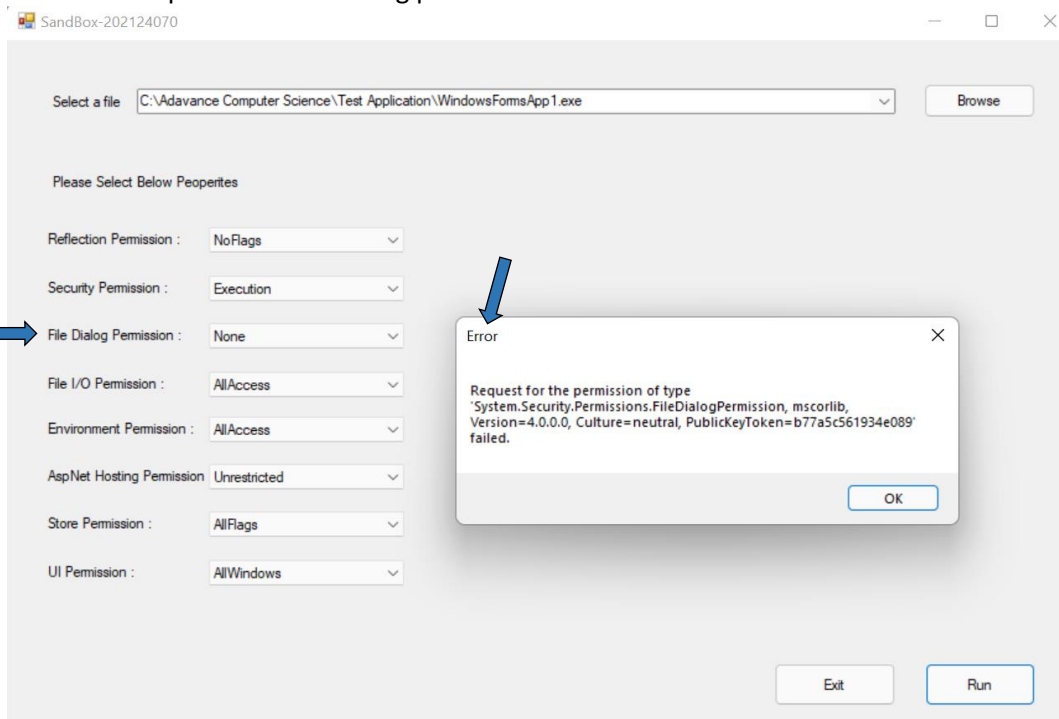


Examples for restricting permissions using UI

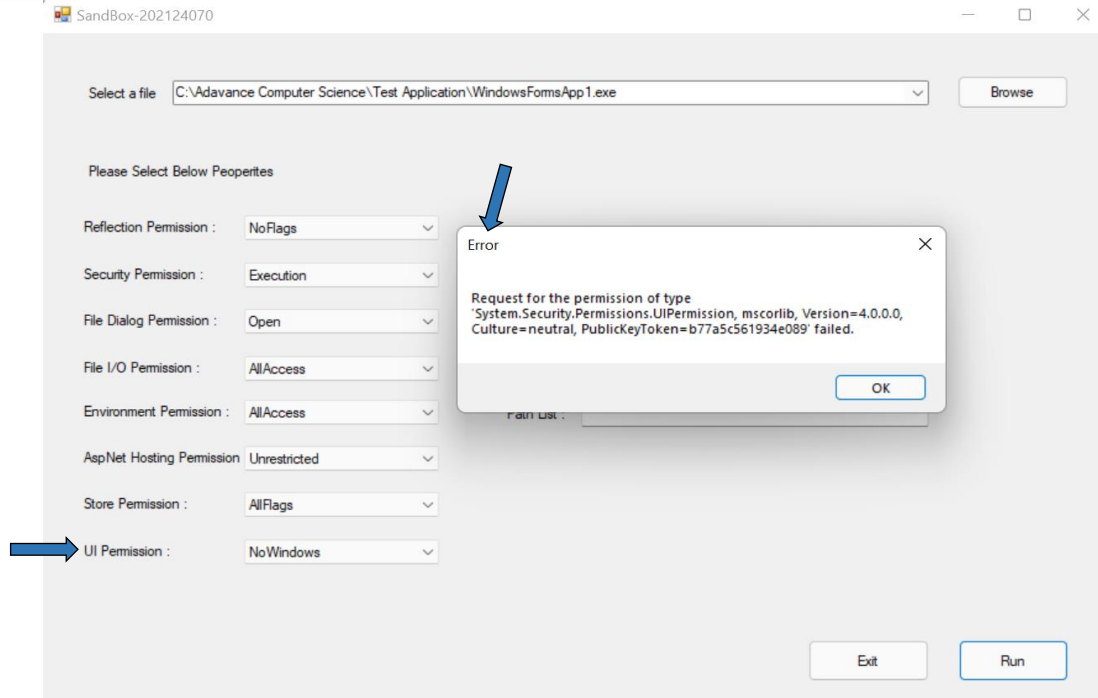
1. Example where file I/O permission is set to No Access.



2. Example where file dialog permission is set to None.



3. Example where ui permission is set to No Windows.



Through Command Line

1. Open the command prompt in the directory of SandBox-202124070.exe file.

```

C:\Windows\System32\cmd.exe

C:\Users\rnire\source\repos\SandBox-202124070>dir
Volume in drive C is OS
Volume Serial Number is EC03-9A46

Directory of C:\Users\rnire\source\repos\SandBox-202124070

02/22/2022  10:40 AM  <DIR>          .
03/02/2022  07:23 PM  <DIR>          ..
02/21/2022  07:12 PM                301 .gitignore
02/22/2022  10:40 AM                .parasoft.dat
02/17/2022  10:58 AM                packages
02/21/2022  07:12 PM                95 README.md
02/28/2022  08:17 PM                SandBox-202124070
02/18/2022  11:54 AM       28,672 SandBox-202124070.exe
02/24/2022  01:27 PM        2,428 SandBox-202124070.sln
               4 File(s)        31,496 bytes
               5 Dir(s)    245,328,920,576 bytes free

C:\Users\rnire\source\repos\SandBox-202124070>

```

2. To run the application and ask for the help with commands, enter in the command prompt `SandBox-202124070.exe --help`. It will provide all the command keys for the permissions and example of using application in commands as given below. Please check Permissions detail section for more details (page no 12).

```

C:\Users\rnire\source\repos\SandBox-202124070\SandBox-202124070\bin\AnyCPU>SandBox-202124070.exe --help
SandBox Tool

-- Usage --
SandBox-202124070.exe -exepath "path" -config default or "..config details.."
Ex: SandBox-202124070.exe -exepath "C:\TestApplication\WindowsFormsApp.exe" -config "-ps 1,-rp 0,-sp 1024,-fdp 2,-fiop 1,-anhp 300,-strp 0,-uip 1"

-- Commands Details --

ReflectionPermission : -rp
7-AllFlags
2-MemberAccess
0-NoFlags
4-ReflectionEmit
8-RestrictedMemberAccess
1-TypeInformation

SecurityPermission : -sp
16383-AllFlags
1-Assertion
8192-BindingRedirects
1024-ControlAppDomain
256-ControlDomainPolicy
32-ControlEvidence
64-ControlPolicy
512-ControlPrincipal
16-ControlThread
8-Execution
4096-Infrastructure
0-NoFlags
2048-RemotingConfiguration
4-SkipVerification
2-UnmanagedCode

FileDialogPermission : -fdp
0-None
1-Open
3-OpenSave
2-Save

```

```

C:\Windows\System32\cmd.exe

FileIOPermission : -fiop
15-AllAccess
4-Append
0-NoAccess
8-PathDiscovery
1-Read
2-Write

AspNetHostingPermission : -anhp
500-High
300-Low
400-Medium
200-Minimal
100-None
600-Unrestricted

StorePermission : -strp
32-AddToStore
247-AllFlags
1-CreateStore
2-DeleteStore
128-EnumerateCertificates
4-EnumerateStores
0-NoFlags
16-OpenStore
64-RemoveFromStore

UIPermission : -uip
0-NoWindows
1-SafeSubWindows
3-AllWindows
2-SafeTopLevelWindows

```

3. To run the tool with untrusted code and default tool permissions use the

`SandBox-202124070.exe -exepath "path" -config default`

The `-exepath` states that you're passing the untrusted code file path in "path" (path should be in double quotes) and `-config` states the permission configuration and default used to run the tool with default permissions.

```

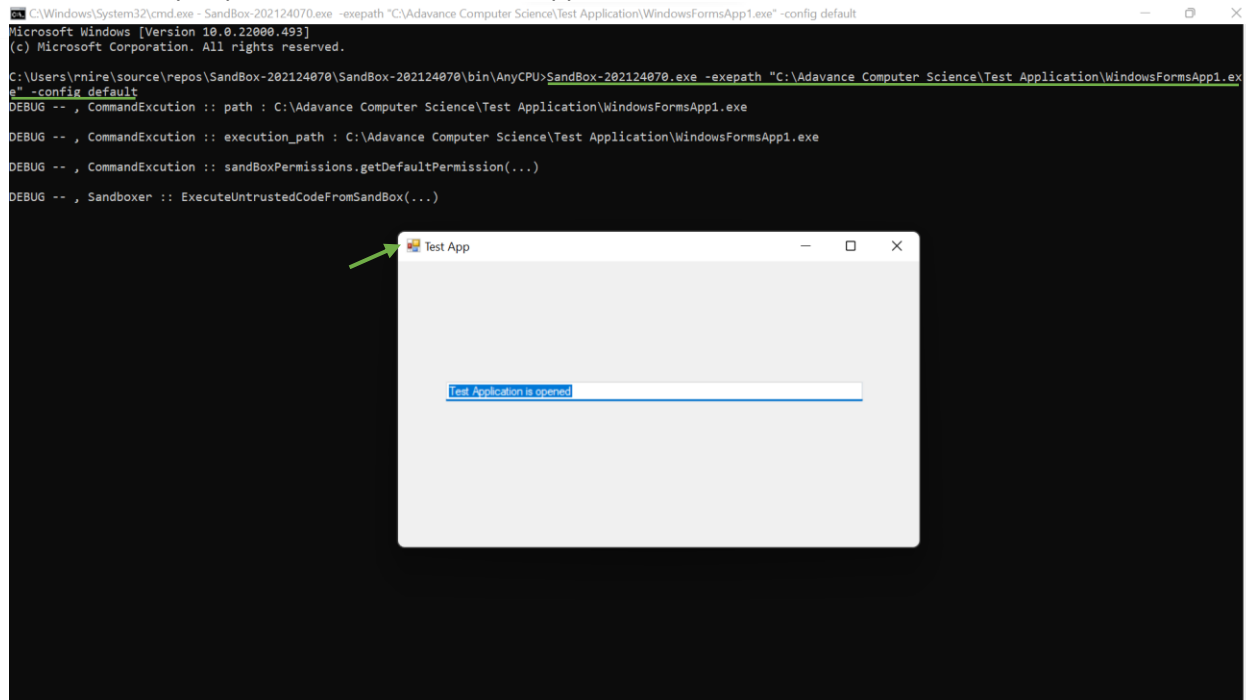
C:\Windows\System32\cmd.exe

Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rnire\source\repos\SandBox-202124070\SandBox-202124070\bin\AnyCPU>SandBox-202124070.exe -exepath "C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config default

```

Once you press enter the untrusted application will run.



4. In order to set the permissions instead of using tool default permissions, you need to pass them like `-config "-rp 0,-sp 1024,-fdp 2,-fiop 1,-anhp 300,-strp 0,-uip 1"`. The entire command will look like, `SandBox-202124070.exe -exepath "C:\AdvanceComputerScience\TestApplication\WindowsFormsApp1.exe" -config "-rp 0,-sp 1024,-fdp 2,-fiop 1,-anhp 300,-strp 0,-uip 1"`

Note: the permissions keys must be passed in the double quotes, and they will be comma separated without any space.

Below are the permission keys and their values.

-rp: Reflection Permission

- 7-AllFlags
- 2-MemberAccess
- 0-NoFlags
- 4-ReflectionEmit
- 8-RestrictedMemberAccess
- 1-TypeInformation

-sp: Security Permission

- 16383-AllFlags
- 1-Assertion
- 8192-BindingRedirects
- 1024-ControlAppDomain
- 256-ControlDomainPolicy
- 32-ControlEvidence
- 64-ControlPolicy
- 512-ControlPrincipal

16-ControlThread
8-Execution
4096-Infrastructure#
0-NoFlags
2048-RemotingConfiguration
4-SkipVerification
2-UnmanagedCode

-fdp: File Dialog Permission

0 - None
1-Open
3-OpenSave
2-Save

-fiop: File IO Permission

15-AllAccess
4-Append
0-NoAccess
8-PathDiscovery
1-Read
2-Write

-anhp: Asp.Net Hosting Permission

500-High
300-Low
400-Medium
200-Minimal
100-None
600-Unrestricted

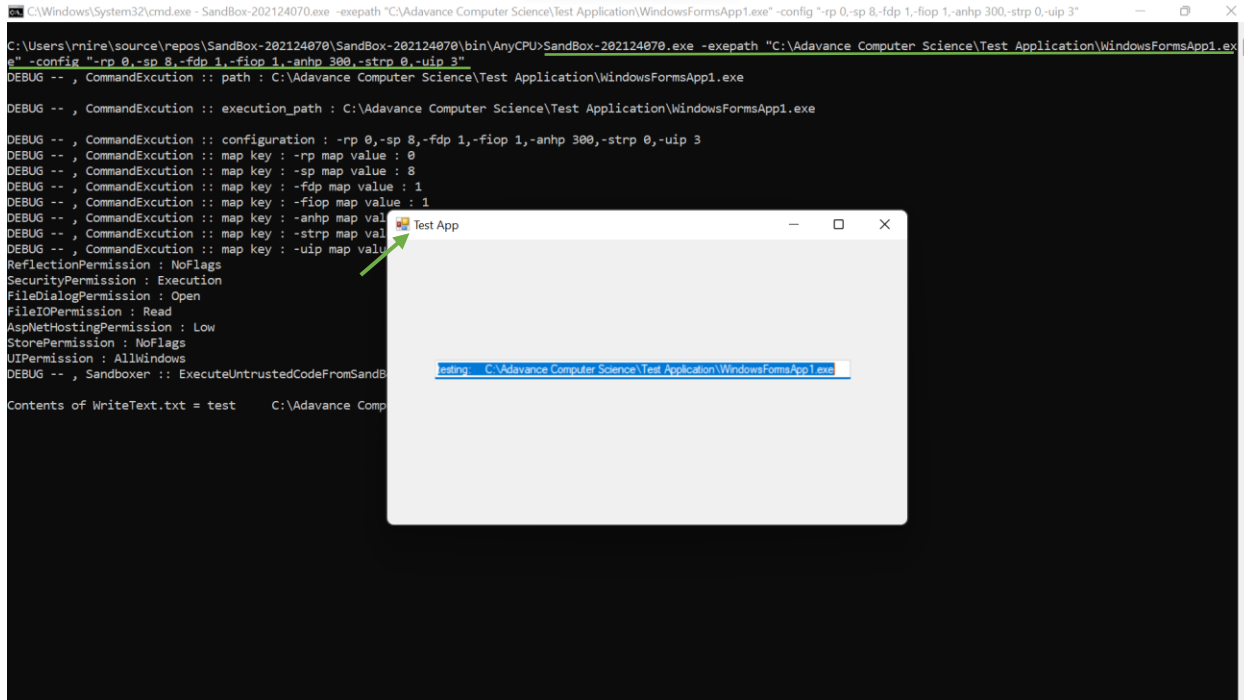
-strp: Store Permission

32-AddToStore
247-AllFlags
1-CreateStore
2-DeleteStore
128-EnumerateCertificates
4-EnumerateStores
0-NoFlags
16-OpenStore
64-RemoveFromStore

-uip: UI Permission

0-NoWindows
1-SafeSubWindows
3-AllWindows
2-SafeTopLevelWindows

After entering the command press enter to run the tool and the application will execute, as shown below.

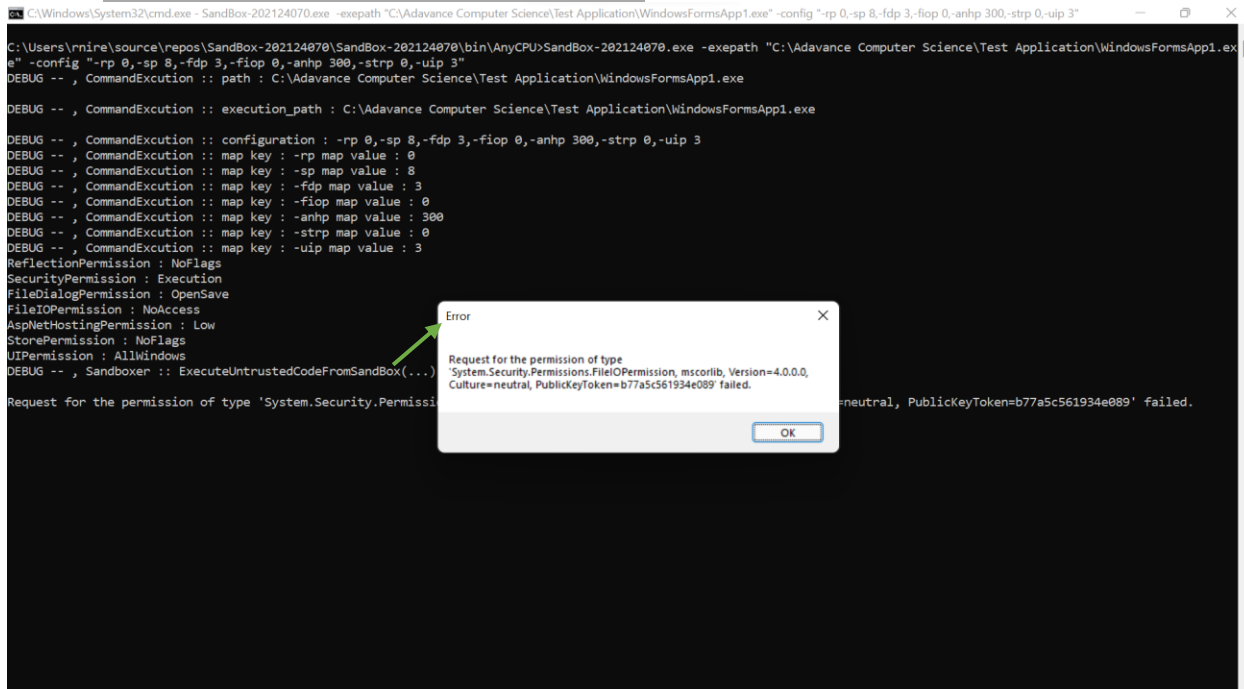


```
C:\Windows\System32\cmd.exe - SandBox-202124070.exe -exepath "C:\Advantage Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0;-sp 8;-fdp 1;-fiop 1;-anhp 300;-strp 0;-uiop 3"
C:\Users\rnire\source\repos\SandBox-202124070\SandBox-202124070\bin\AnyCPU>SandBox-202124070.exe -exepath "C:\Advantage Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0;-sp 8;-fdp 1;-fiop 1;-anhp 300;-strp 0;-uiop 3"
DEBUG -- , CommandExcution :: path : C:\Advantage Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExcution :: execution_path : C:\Advantage Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExcution :: configuration : -rp 0;-sp 8;-fdp 1;-fiop 1;-anhp 300;-strp 0;-uiop 3
DEBUG -- , CommandExcution :: map key : -rp map value : 0
DEBUG -- , CommandExcution :: map key : -sp map value : 8
DEBUG -- , CommandExcution :: map key : -fdp map value : 1
DEBUG -- , CommandExcution :: map key : -fiop map value : 1
DEBUG -- , CommandExcution :: map key : -anhp map value : 300
DEBUG -- , CommandExcution :: map key : -strp map value : 0
DEBUG -- , CommandExcution :: map key : -uiop map value : 3
ReflectionPermission : NoFlags
SecurityPermission : Execution
FileDialogPermission : Open
FileIOPermission : Read
AspNetHostingPermission : Low
StorePermission : NoFlags
UIPermission : AllWindows
DEBUG -- , Sandboxer :: ExecuteUntrustedCodeFromSandBox
Contents of WriteText.txt = test C:\Advantage Computer Science\Test Application\WindowsFormsApp1.exe
```

Examples for restricting permissions using commands

1. Example where file I/O permission is set to 0 (No Access).

Used command: `SandBox-202124070.exe -exepath "C:\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 3,-fiop 0,-anhp 300,-strp 0,-uip 3"`

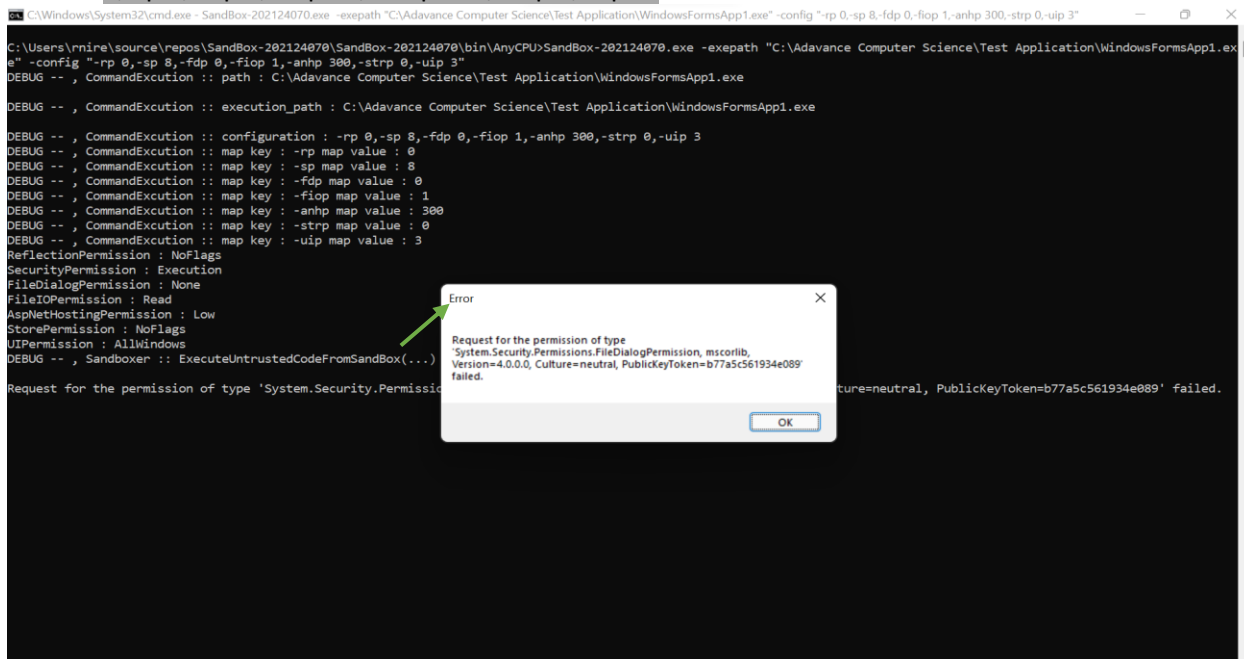


```
C:\Windows\System32\cmd.exe - SandBox-202124070.exe -exepath "C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 3,-fiop 0,-anhp 300,-strp 0,-uip 3"

C:\Users\rnire\source\repos\SandBox-202124070\SandBox-202124070\bin\AnyCPU>SandBox-202124070.exe -exepath "C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 3,-fiop 0,-anhp 300,-strp 0,-uip 3"
DEBUG -- , CommandExecution :: path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExecution :: execution_path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExecution :: configuration : -rp 0,-sp 8,-fdp 3,-fiop 0,-anhp 300,-strp 0,-uip 3
DEBUG -- , CommandExecution :: map key : -rp map value : 0
DEBUG -- , CommandExecution :: map key : -sp map value : 8
DEBUG -- , CommandExecution :: map key : -fdp map value : 3
DEBUG -- , CommandExecution :: map key : -fiop map value : 0
DEBUG -- , CommandExecution :: map key : -anhp map value : 300
DEBUG -- , CommandExecution :: map key : -strp map value : 0
DEBUG -- , CommandExecution :: map key : -uip map value : 3
ReflectionPermission : NoFlags
SecurityPermission : Execution
FileDialogPermission : OpenSave
FileIOPermission : NoAccess
AspNetHostingPermission : Low
StorePermission : NoFlags
UIPermission : AllWindows
DEBUG -- , Sandboxer :: ExecuteUntrustedCodeFromSandbox(...)
Request for the permission of type 'System.Security.Permissions.FileIOPermission, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' failed.
```

2. Example where file dialog permission is set to 0 (None).

Used command: `SandBox-202124070.exe -exepath "C:\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 0,-fiop 15,-anhp 300,-strp 0,-uip 3"`

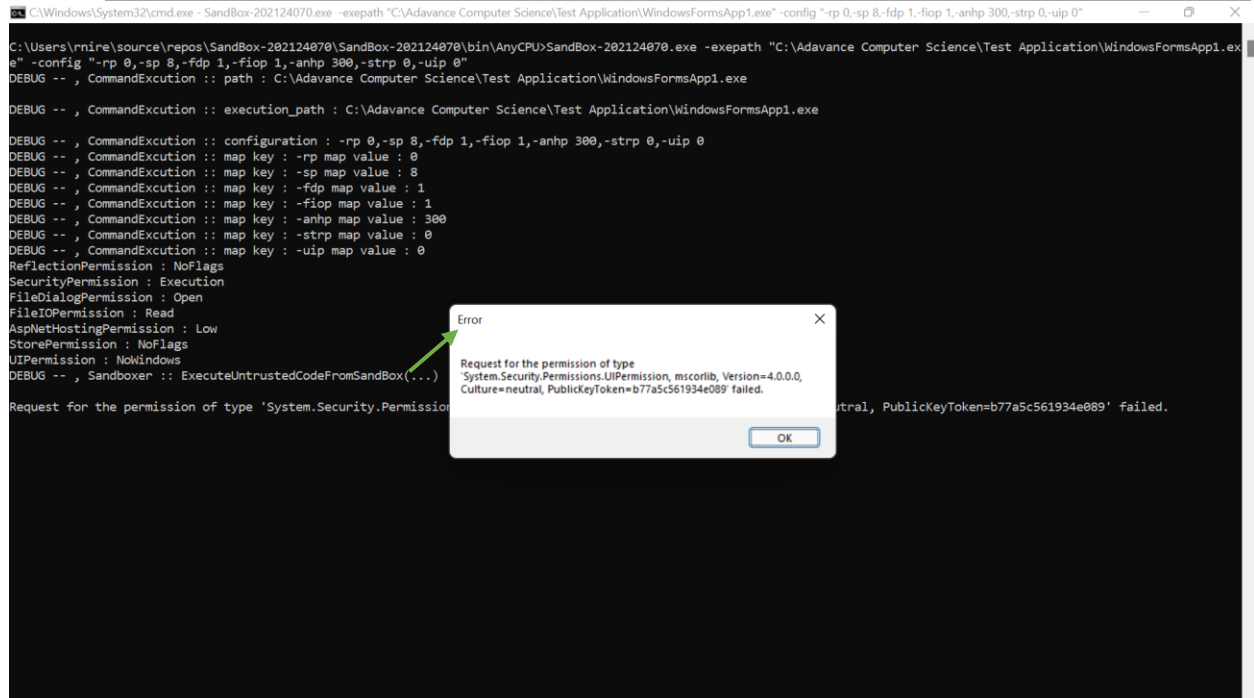


```
C:\Windows\System32\cmd.exe - SandBox-202124070.exe -exepath "C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 0,-fiop 15,-anhp 300,-strp 0,-uip 3"

C:\Users\rnire\source\repos\SandBox-202124070\SandBox-202124070\bin\AnyCPU>SandBox-202124070.exe -exepath "C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 0,-fiop 15,-anhp 300,-strp 0,-uip 3"
DEBUG -- , CommandExecution :: path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExecution :: execution_path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExecution :: configuration : -rp 0,-sp 8,-fdp 0,-fiop 15,-anhp 300,-strp 0,-uip 3
DEBUG -- , CommandExecution :: map key : -rp map value : 0
DEBUG -- , CommandExecution :: map key : -sp map value : 8
DEBUG -- , CommandExecution :: map key : -fdp map value : 0
DEBUG -- , CommandExecution :: map key : -fiop map value : 15
DEBUG -- , CommandExecution :: map key : -anhp map value : 300
DEBUG -- , CommandExecution :: map key : -strp map value : 0
DEBUG -- , CommandExecution :: map key : -uip map value : 3
ReflectionPermission : NoFlags
SecurityPermission : Execution
FileDialogPermission : None
FileIOPermission : Read
AspNetHostingPermission : Low
StorePermission : NoFlags
UIPermission : AllWindows
DEBUG -- , Sandboxer :: ExecuteUntrustedCodeFromSandbox(...)
Request for the permission of type 'System.Security.Permissions.FileDialogPermission, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' failed.
```


3. Example where ui permission is set to 0 (No Windows).

Used command: `Sandbox-202124070.exe -exepath "C:\Advance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 1,-fiop 1,-anhp 300,-strp 0,-uip 0"`



```
C:\Windows\System32\cmd.exe - Sandbox-202124070.exe -exepath "C:\Advance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 1,-fiop 1,-anhp 300,-strp 0,-uip 0"

C:\Users\rnire\source\repos\Sandbox-202124070\Sandbox-202124070\bin\AnyCPU>Sandbox-202124070.exe -exepath "C:\Advance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-rp 0,-sp 8,-fdp 1,-fiop 1,-anhp 300,-strp 0,-uip 0"
DEBUG -- , CommandExecution :: path : C:\Advance Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExecution :: execution_path : C:\Advance Computer Science\Test Application\WindowsFormsApp1.exe
DEBUG -- , CommandExecution :: configuration : -rp 0,-sp 8,-fdp 1,-fiop 1,-anhp 300,-strp 0,-uip 0
DEBUG -- , CommandExecution :: map key : -rp map value : 0
DEBUG -- , CommandExecution :: map key : -sp map value : 8
DEBUG -- , CommandExecution :: map key : -fdp map value : 1
DEBUG -- , CommandExecution :: map key : -fiop map value : 1
DEBUG -- , CommandExecution :: map key : -anhp map value : 300
DEBUG -- , CommandExecution :: map key : -strp map value : 0
DEBUG -- , CommandExecution :: map key : -uip map value : 0
ReflectionPermission : NoFlags
SecurityPermission : Execution
FileDialogPermission : Open
FileIOPermission : Read
AspNetHostingPermission : Low
StorePermission : NoFlags
UIPermission : NoWindows
DEBUG -- , Sandboxer :: ExecuteUntrustedCodeFromSandbox(...)
Request for the permission of type 'System.Security.Permissions.UIPermission, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' failed.
```

Permissions

In this section will be describing all the permission used in the tool and what are their capabilities.

Permissions used in the tool and their capabilities

- ***DnsPermission***: Controls rights to access Domain Name System (DNS) servers on the network. The default permissions allow all local and Intranet zone applications to access DNS services, and no DNS permission for Internet zone applications.
- ***SqlClientPermission***: Enables the .NET Framework Data Provider for SQL Server to help make sure that a user has a security level sufficient to access a data source. The Permission State enumeration takes precedence over the AllowBlankPassword property. Therefore, if you set AllowBlankPassword to false, you must also set Permission State to None to prevent a user from making a connection using a blank password. For an example demonstrating how to use security demands, see Code Access Security and ADO.NET.
- ***WebPermission***: Controls rights to access HTTP Internet resources. The value of the state parameter is either PermissionState.None or PermissionState.Unrestricted, respectively yielding fully restricted or fully unrestricted access to all security variables. If you specify PermissionState.None, then you can give access to individual URIs using AddPermission.
- ***TypeDescriptorPermission***: Initializes a new instance of the TypeDescriptorPermission class with the specified permission flags.
- ***ReflectionPermission***: Controls access to non-public types and members through the System.Reflection APIs. Controls some features of the System.Reflection.Emit APIs and initializes a new instance of the Reflection Permission class with the specified access.
- ***SecurityPermission***: Describes a set of security permissions applied to code.
- ***FileDialogPermission***: Controls the ability to access files or folders through a File dialog box. This class cannot be inherited and initializes a new instance of the File Dialog Permission class with the specified access.
- ***FileIOPermission***: Controls the ability to access files and folders.
- ***EnvironmentPermission***: Controls access to system and user environment variables.
- ***AspNetHostingPermission***: Controls access permissions in ASP.NET hosted environments.

- *StorePermission*: Controls access to stores containing X.509 certificates.
- *UIPermission*: Controls the permissions related to user interfaces and the Clipboard.

Limitations of the tool

- In this tool only few of the permissions are considered.
- Through the command line we cannot set the Environment Permissions.
- The tool will only run the applications which is built in C# and have proper assemblies.
- When you are running some application using the UI screen of the tool, the screen may shrink in size.

References

- All the permissions are taken from the Microsoft official site, which are given below,

<https://docs.microsoft.com/en-us/dotnet/api/system.net?view=dotnet-plat-ext-6.0>

<https://docs.microsoft.com/en-us/dotnet/api/system.data.sqlclient.sqlclientpermission?view=dotnet-plat-ext-6.0>

<https://docs.microsoft.com/en-us/dotnet/api/system.security?view=net-6.0>

<https://docs.microsoft.com/en-us/dotnet/api/system.web.aspnethostingpermission?view=dotnet-plat-ext-6.0>

<https://docs.microsoft.com/en-us/dotnet/api/system.security.permissions?view=dotnet-plat-ext-6.0>

- For the sandbox referred from <https://docs.microsoft.com/en-us/previous-versions/dotnet/framework/code-access-security/how-to-run-partially-trusted-code-in-a-sandbox?redirectedfrom=MSDN>