3/7/2022

Sandbox User Manual

Student Id: 202124070

Rohan Mahesh Nirer
UNIVERSITY OF HULL

User manual index

About tool

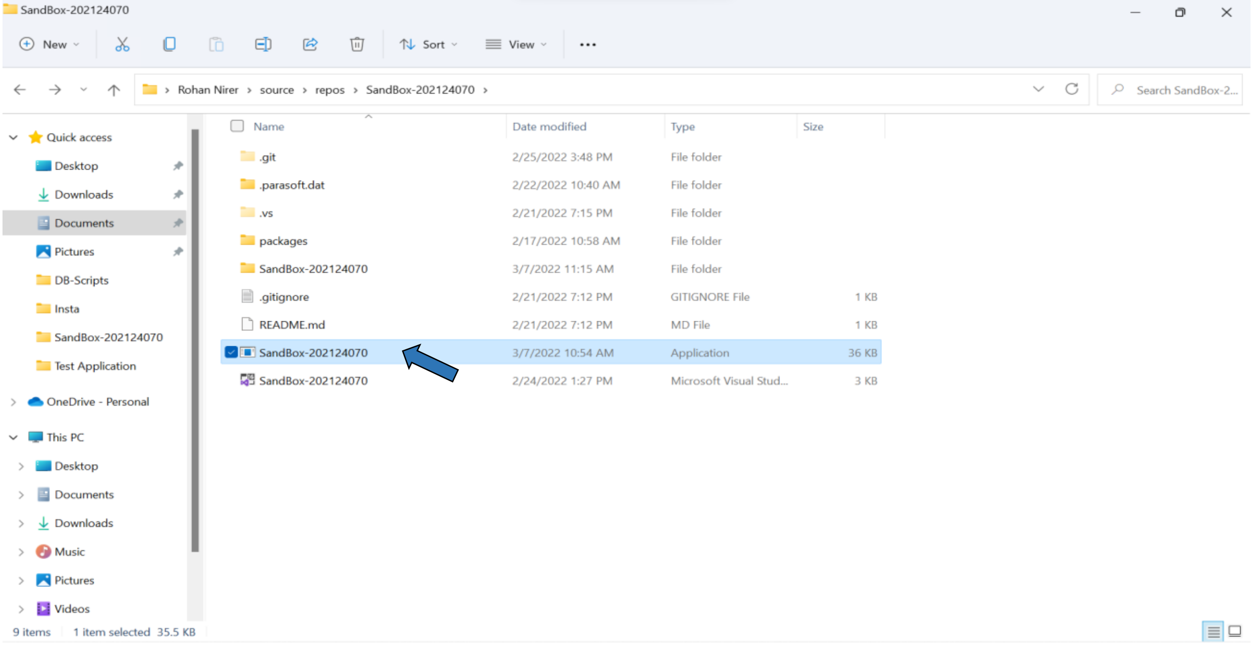
The Sandbox tool is implemented using C# and Windows forms for the UI. This tool provides a secure environment in which executable files can run with configuring various types of permissions. In addition, the tool can be run in two ways. First, can be executed by double-clicking on the .exe file, in 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 8).

How to use?

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

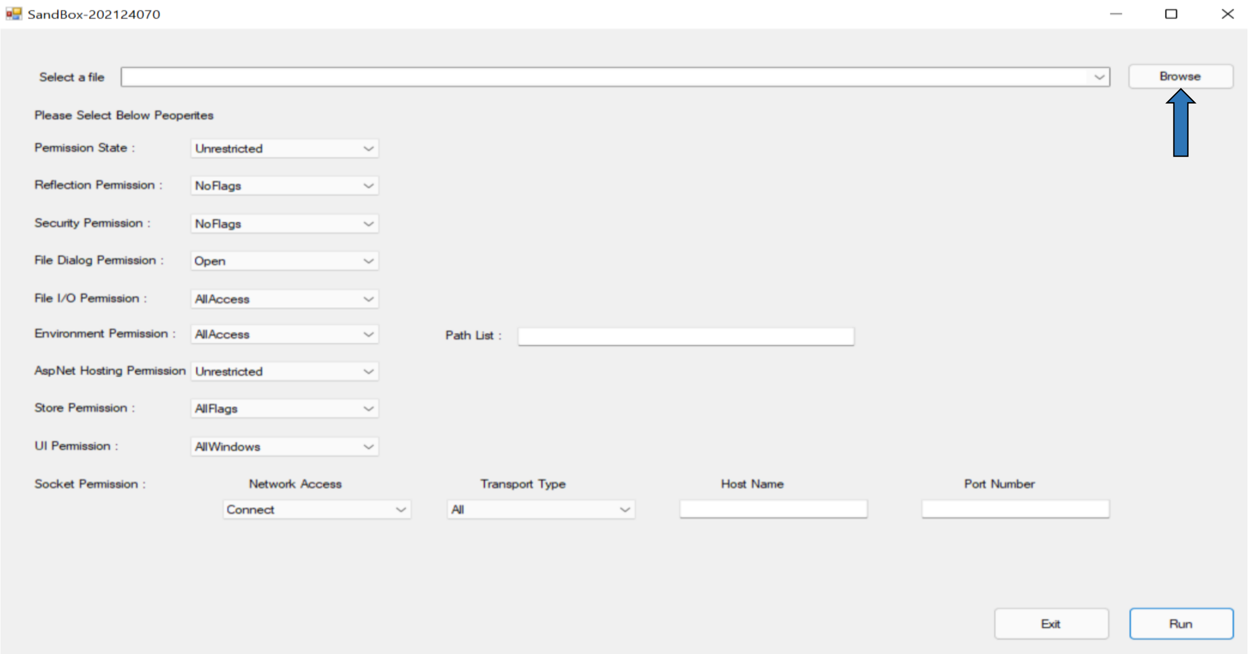
Opening the SandBox-202124070.exe file

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



Name	Date modified	Type	Size
.git	2/25/2022 3:48 PM	File folder	
.parasoft.dat	2/22/2022 10:40 AM	File folder	
.vs	2/21/2022 7:15 PM	File folder	
packages	2/17/2022 10:58 AM	File folder	
SandBox-202124070	3/7/2022 11:15 AM	File folder	
.gitignore	2/21/2022 7:12 PM	GITIGNORE File	1 KB
README.md	2/21/2022 7:12 PM	MD File	1 KB
SandBox-202124070	3/7/2022 10:54 AM	Application	36 KB
SandBox-202124070	2/24/2022 1:27 PM	Microsoft Visual Stud...	3 KB

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.



Select a file

Please Select Below Peopertes

Permission State : Unrestricted

Reflection Permission : NoFlags

Security Permission : NoFlags

File Dialog Permission : Open

File I/O Permission : AllAccess

Environment Permission : AllAccess

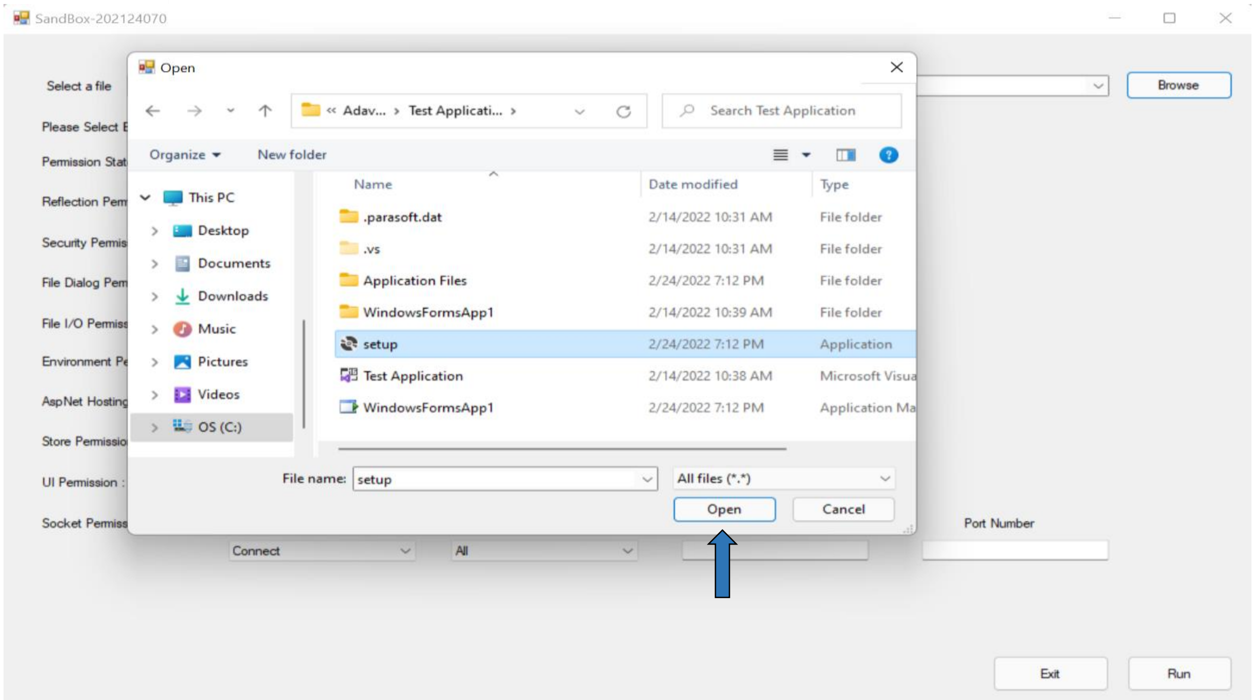
Path List :

AspNet Hosting Permission Unrestricted

Store Permission : AllFlags

UI Permission : AllWindows

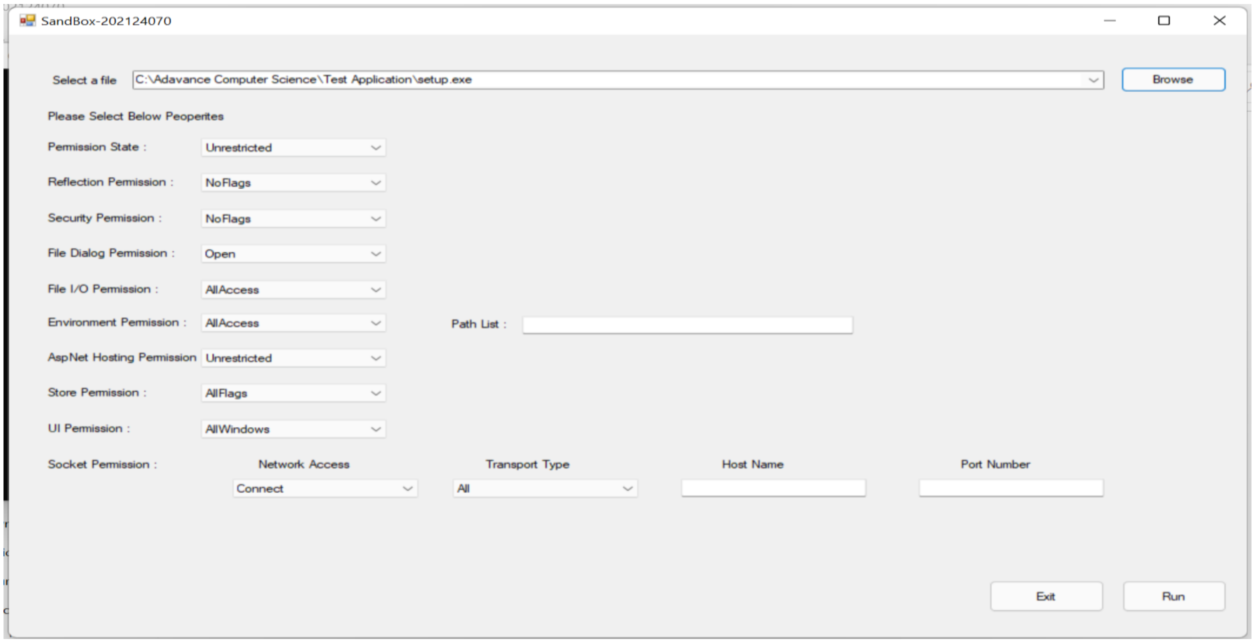
Socket Permission : Network Access Connect Transport Type All Host Name Port Number



Name	Date modified	Type
.parasoft.dat	2/14/2022 10:31 AM	File folder
.vs	2/14/2022 10:31 AM	File folder
Application Files	2/24/2022 7:12 PM	File folder
WindowsFormsApp1	2/14/2022 10:39 AM	File folder
setup	2/24/2022 7:12 PM	Application
Test Application	2/14/2022 10:38 AM	Microsoft Visua
WindowsFormsApp1	2/24/2022 7:12 PM	Application Ma

File name: setup

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.



Select a file C:\Adavance Computer Science\Test Application\setup.exe

Please Select Below Peoperites

Permission State : Unrestricted

Reflection Permission : NoFlags

Security Permission : NoFlags

File Dialog Permission : Open

File I/O Permission : AllAccess

Environment Permission : AllAccess

Path List :

AspNet Hosting Permission Unrestricted

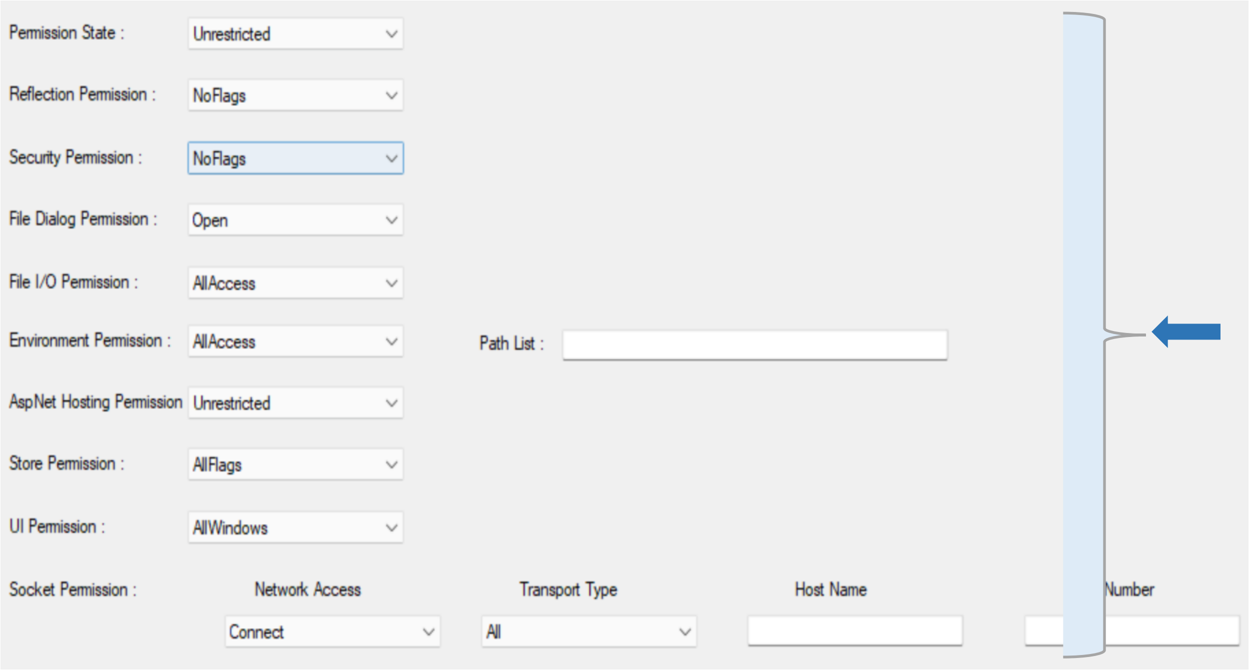
Store Permission : AllFlags

UI Permission : AllWindows

Socket Permission :

Network Access	Transport Type	Host Name	Port Number
Connect	All		

3. Select the permissions properties from the dropdowns, if user does not enter any Path List, Host Name or Port Number the application will pick default value from the system.
   Default value for Path list is same as selected file path and hostname is localhost and port number is 8080.



Permission State : Unrestricted

Reflection Permission : NoFlags

Security Permission : NoFlags

File Dialog Permission : Open

File I/O Permission : AllAccess

Environment Permission : AllAccess

Path List :

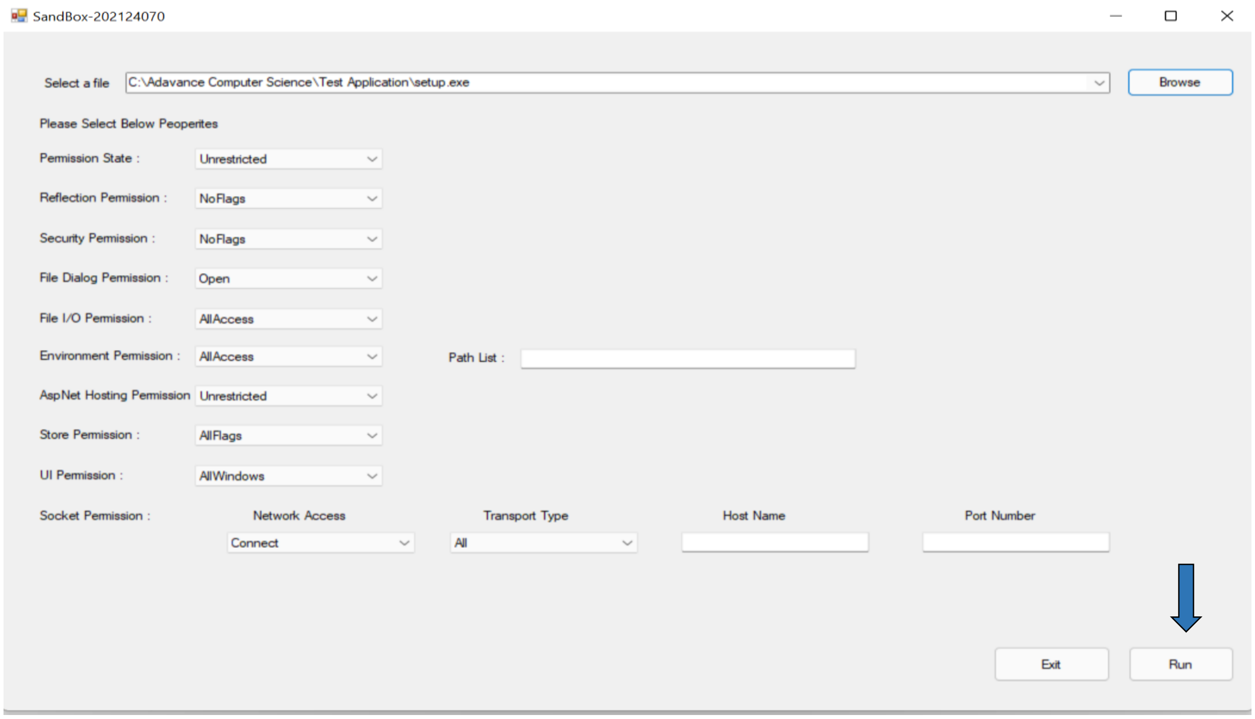
AspNet Hosting Permission Unrestricted

Store Permission : AllFlags

UI Permission : AllWindows

Socket Permission : Network Access Connect Transport Type All Host Name Number

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



SandBox-202124070

Select a file C:\Adavance Computer Science\Test Application\setup.exe

Please Select Below Peopertes

Permission State : Unrestricted

Reflection Permission : NoFlags

Security Permission : NoFlags

File Dialog Permission : Open

File I/O Permission : AllAccess

Environment Permission : AllAccess

Path List :

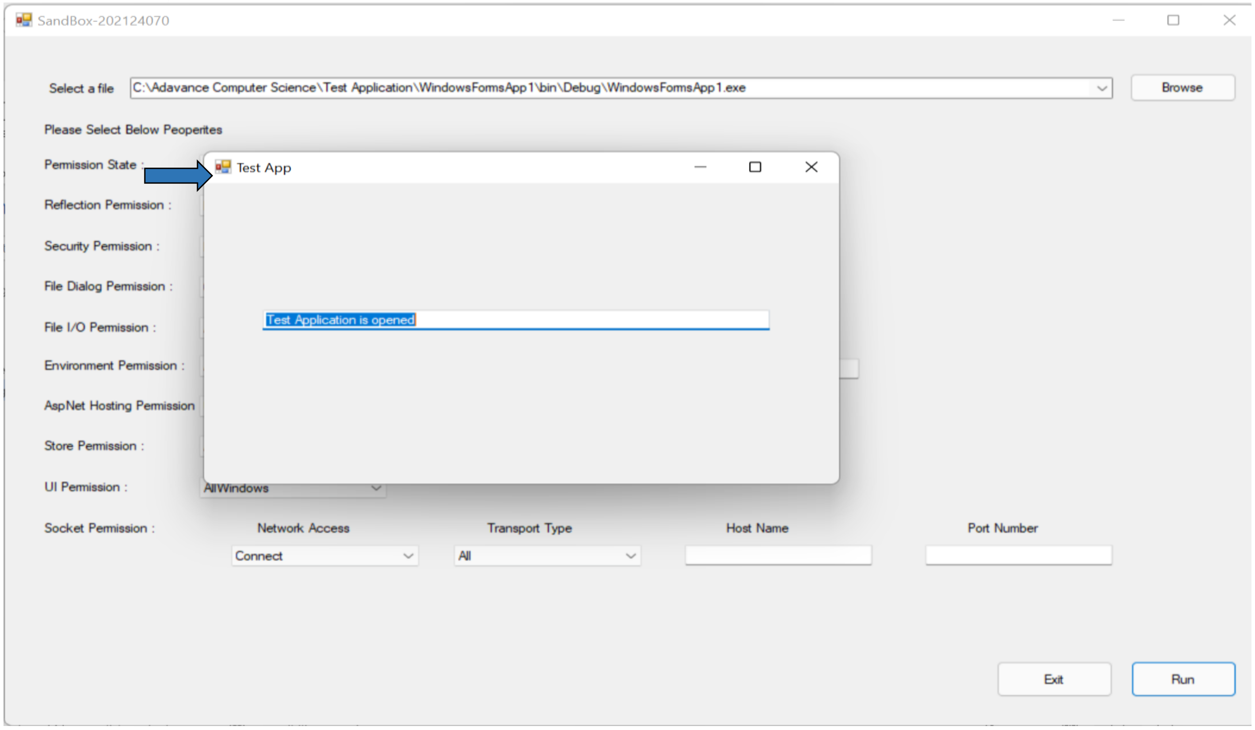
AspNet Hosting Permission Unrestricted

Store Permission : AllFlags

UI Permission : AllWindows

Socket Permission : Network Access Connect Transport Type All Host Name Port Number

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



SandBox-202124070

Select a file: C:\Adavance Computer Science\Test Application\WindowsFormsApp1\bin\Debug\WindowsFormsApp1.exe

Please Select Below Peopertes

Permission State :

Reflection Permission :

Security Permission :

File Dialog Permission :

File I/O Permission :

Environment Permission :

AspNet Hosting Permission

Store Permission :

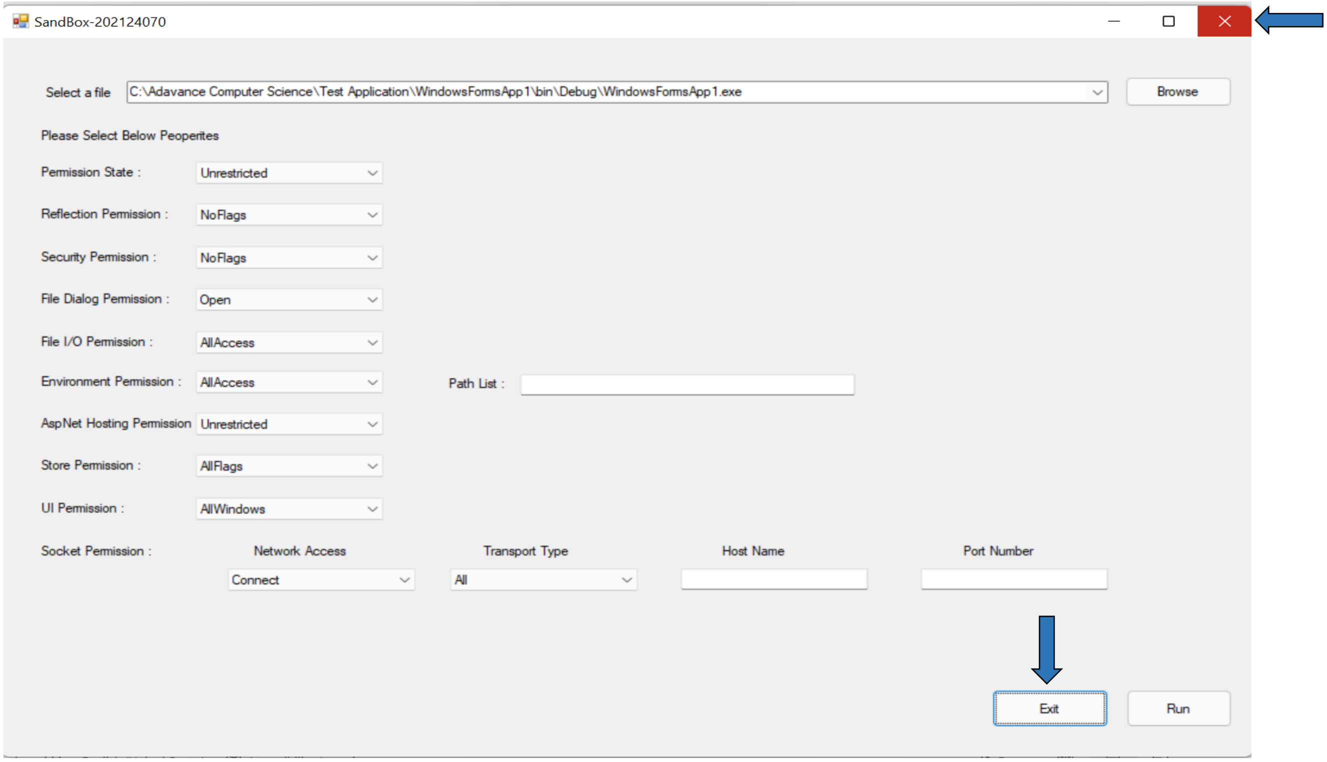
UI Permission : AllWindows

Socket Permission : Network Access: Connect; Transport Type: All; Host Name: ; Port Number:

Test App

Test Application is opened

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



SandBox-202124070

Select a file: C:\Adavance Computer Science\Test Application\WindowsFormsApp1\bin\Debug\WindowsFormsApp1.exe

Please Select Below Peopertes

Permission State : Unrestricted

Reflection Permission : NoFlags

Security Permission : NoFlags

File Dialog Permission : Open

File I/O Permission : AllAccess

Environment Permission : AllAccess   Path List :

AspNet Hosting Permission Unrestricted

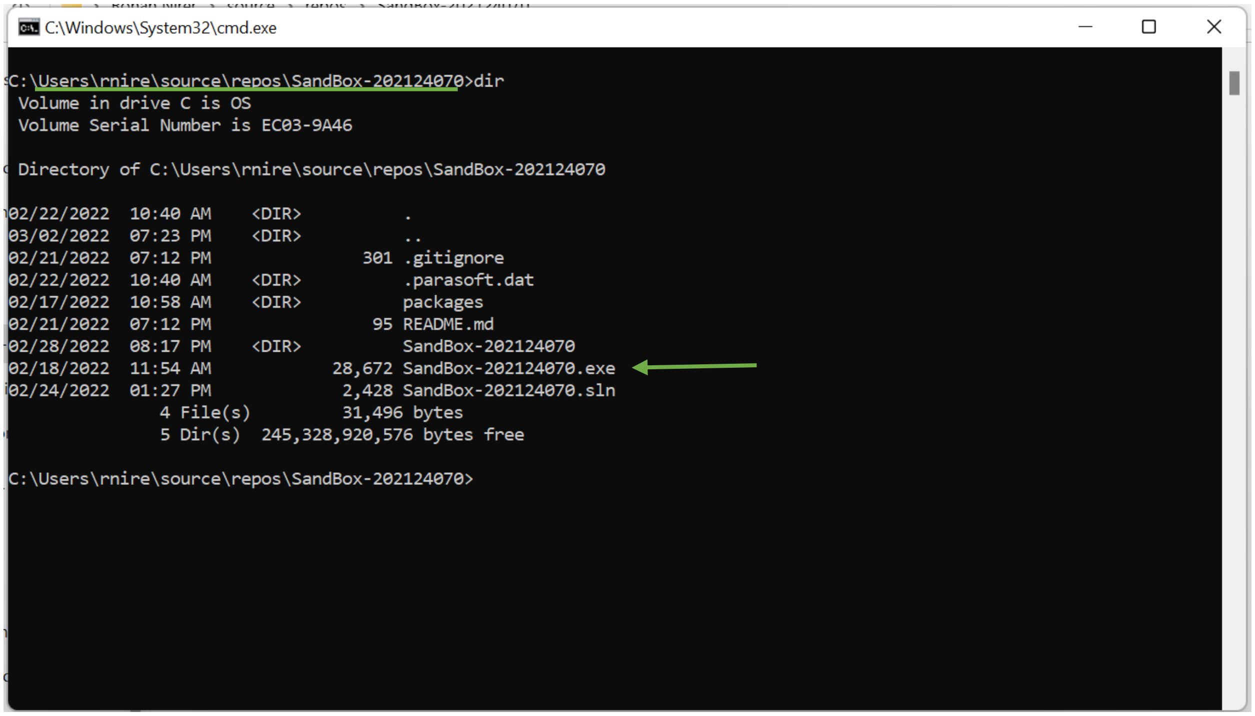
Store Permission : AllFlags

UI Permission : AllWindows

Socket Permission : Network Access: Connect; Transport Type: All; Host Name: ; Port Number:

Through Command Line

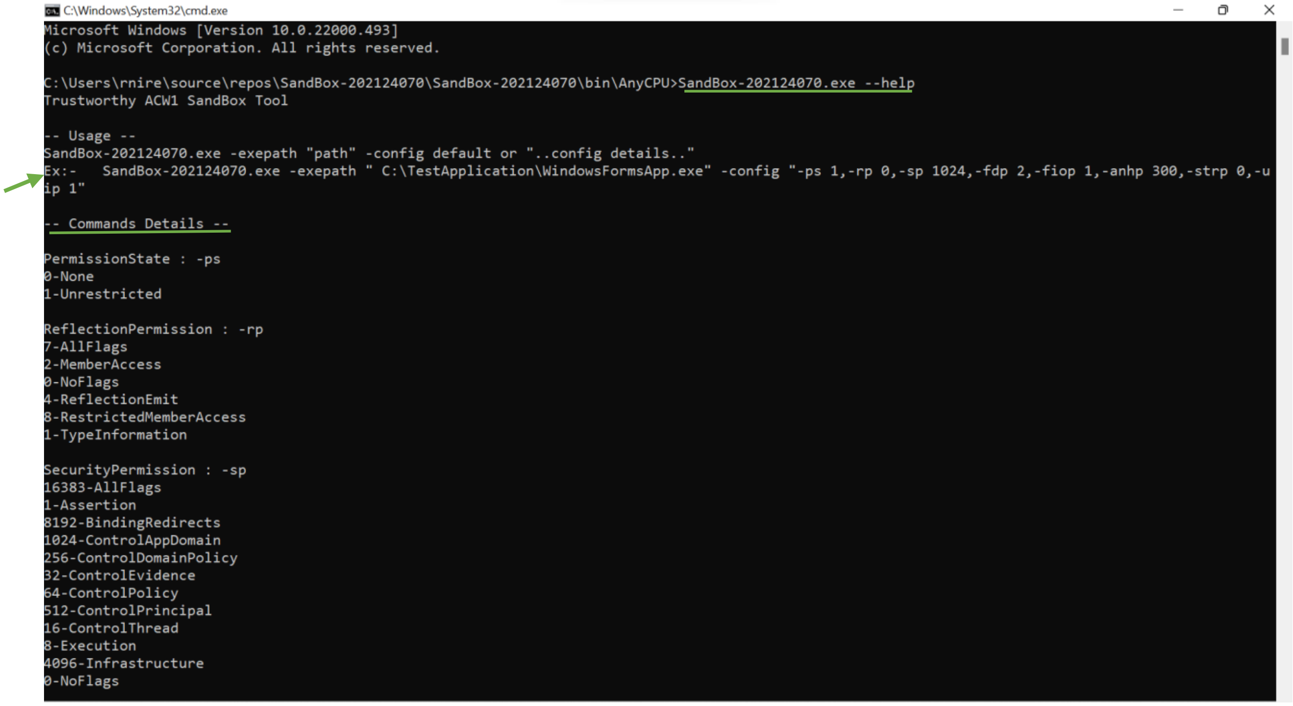
1. Open the command prompt in the directory of SandBox-202124070.exe file.



C:\Windows\System32\cmd.exe

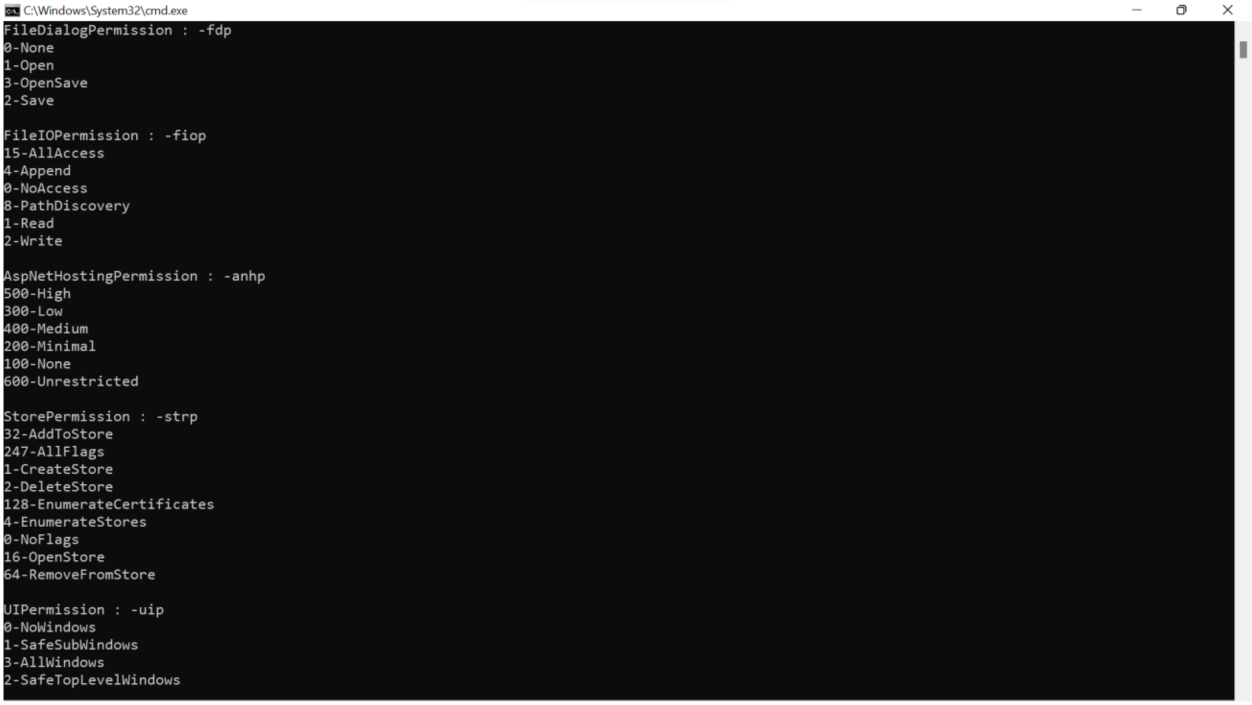
```
C:\Users\rnire\source\repos\SandBox-202124070>dir
 Volume in drive C is OS
 Volume Serial Number is EC03-9A46

 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    <DIR>          .parasoft.dat
02/17/2022  10:58 AM    <DIR>          packages
02/21/2022  07:12 PM                95 README.md
02/28/2022  08:17 PM    <DIR>          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 10).



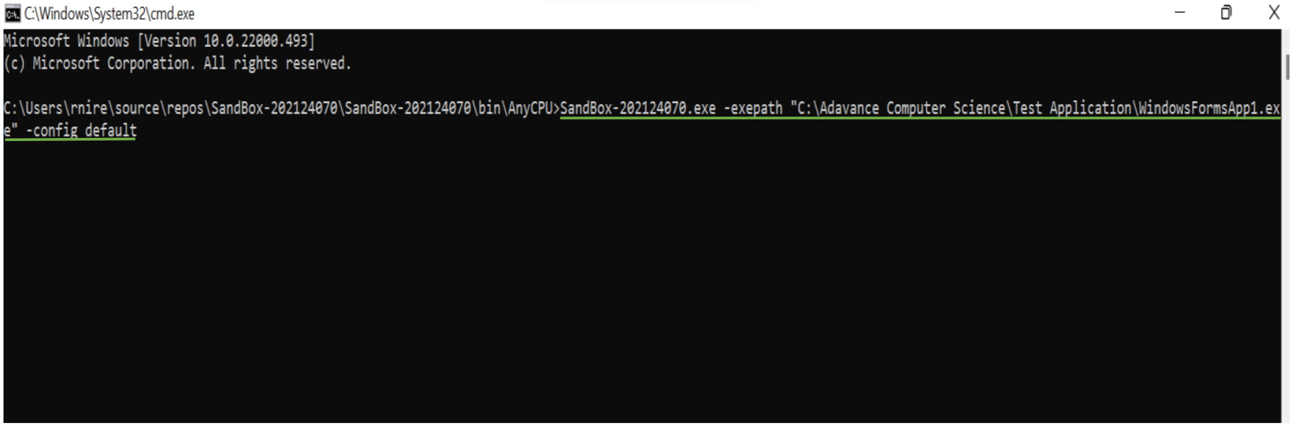
C:\Windows\System32\cmd.exe

```
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 --help
Trustworthy ACW1 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,-u
ip 1"

-- Commands Details --

PermissionState : -ps
0-None
1-Unrestricted

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
```



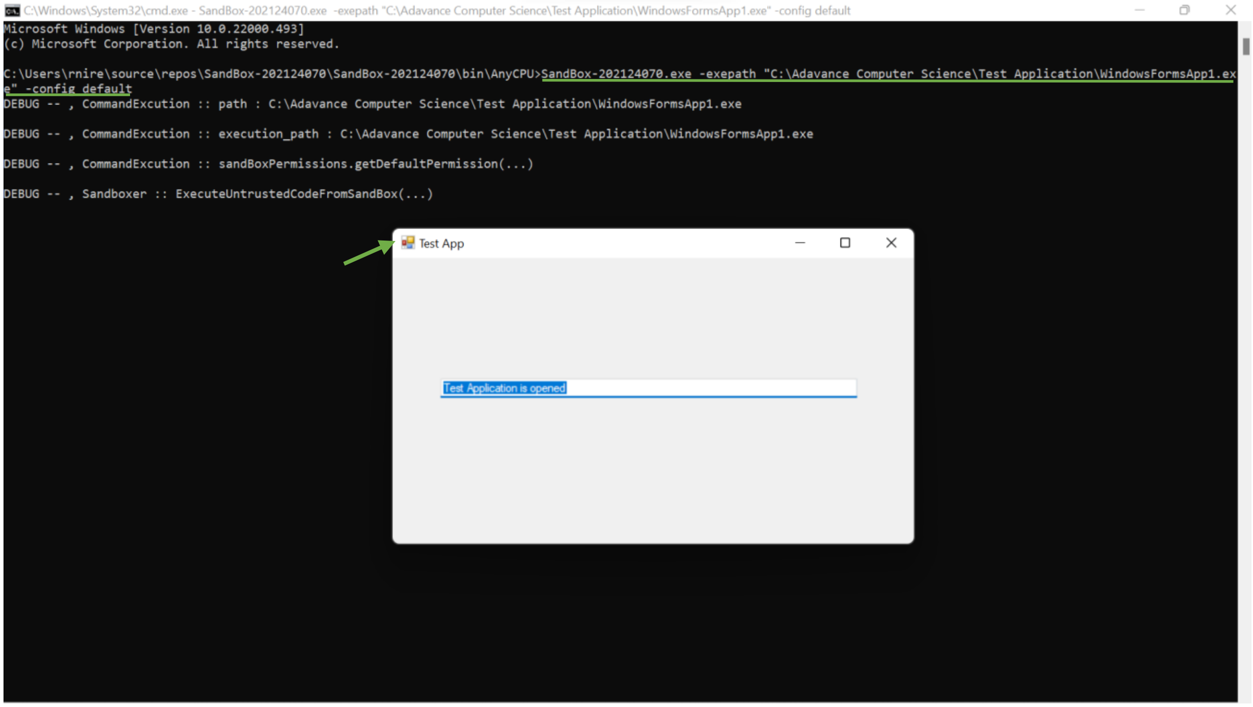
```
FileDialogPermission : -fdp
0-None
1-Open
3-OpenSave
2-Save

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.



```
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.ex
e" -config default
```

Once you press enter the untrusted application will run.



```
C:\Windows\System32\cmd.exe - SandBox-202124070.exe  -exepath "C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config default
```

```
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.ex
e" -config default
DEBUG -- , CommandExcution :: path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe

DEBUG -- , CommandExcution :: execution_path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe

DEBUG -- , CommandExcution :: sandBoxPermissions.getDefaultPermission(...)

DEBUG -- , Sandboxer :: ExecuteUntrustedCodeFromSandBox(...)
```

Test Application is opened

4. In order to set the permissions instead of using tool default permissions, you need to pass them like -config "-ps 1,-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:\AdavanceComputerScience\TestApplication\WindowsFormsApp1.exe" -config "-ps 1,-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.

```
-ps: Permission State
       0 – None
       1 – Unrestricted

-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
```

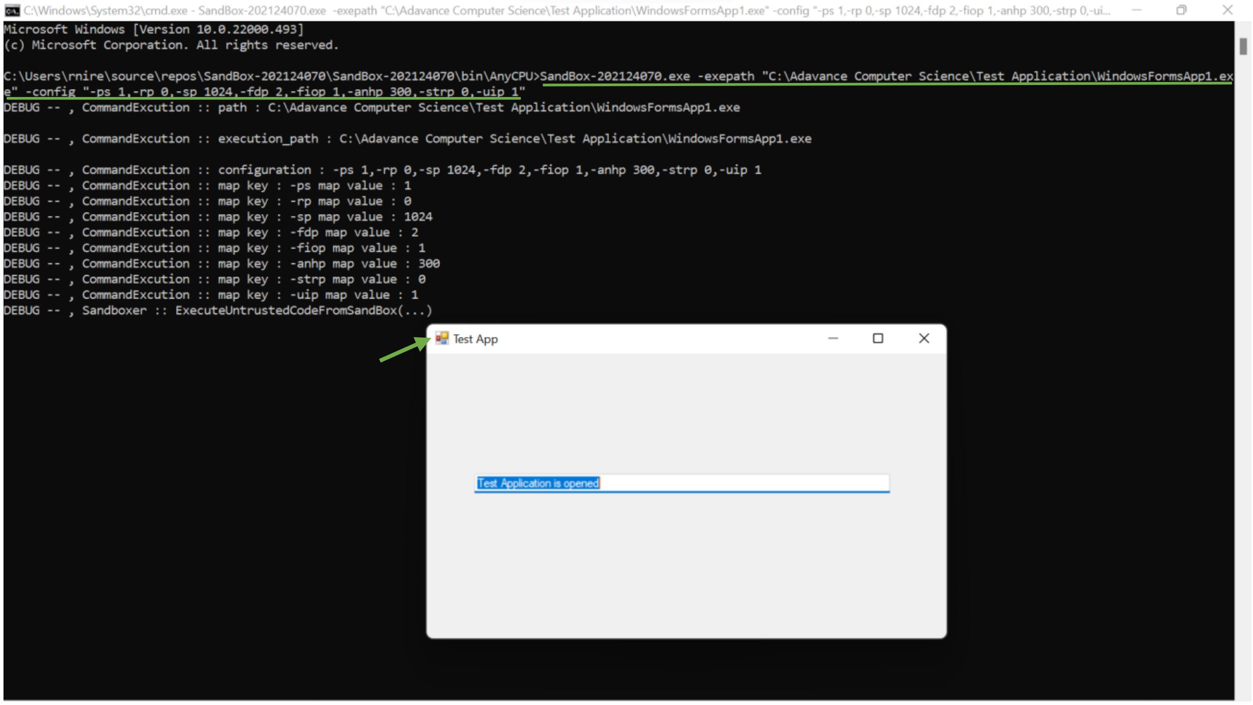
-strp: Store Permission

```
        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:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe" -config "-ps 1,-rp 0,-sp 1024,-fdp 2,-fiop 1,-anhp 300,-strp 0,-ui...
Test App

```
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.ex
e" -config "-ps 1,-rp 0,-sp 1024,-fdp 2,-fiop 1,-anhp 300,-strp 0,-uip 1"
DEBUG -- , CommandExcution :: path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe

DEBUG -- , CommandExcution :: execution_path : C:\Adavance Computer Science\Test Application\WindowsFormsApp1.exe

DEBUG -- , CommandExcution :: configuration : -ps 1,-rp 0,-sp 1024,-fdp 2,-fiop 1,-anhp 300,-strp 0,-uip 1
DEBUG -- , CommandExcution :: map key : -ps map value : 1
DEBUG -- , CommandExcution :: map key : -rp map value : 0
DEBUG -- , CommandExcution :: map key : -sp map value : 1024
DEBUG -- , CommandExcution :: map key : -fdp map value : 2
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 : -uip map value : 1
DEBUG -- , Sandboxer :: ExecuteUntrustedCodeFromSandBox(...)
```

Test Application is opened

Permissions

In this section will be describing all the permission used in the tool and what are the default permissions are set in the tool.

Permissions used in the tool and their description

- *PermissionSet*: Represents a collection that can contain many different types of permissions. You can use Permission Set to perform operations on several different permissions as a group.

- *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.

- *SocketPermission*: Controls rights to make or accept connections on a transport address. This constructor creates a Socket Permission that controls access to the specified host name and port number using the specified transport. The hostname can be a DNS name, an IP address, or a specified IP subnet, such as 192.168.1.*. The port number can be any valid port number defined by the transport, or SocketPermission.AllPorts.

- *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. This class cannot be inherited and initializes a new instance of the Security Permission class with the specified initial set state of the flags.

- *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. This class cannot be inherited and initializes a new instance of the File IO Permission class with the specified access to the designated file or directory.

- *EnvironmentPermission*: Controls access to system and user environment variables. This class cannot be inherited and initializes a new instance of the Environment Permission class with the specified access to the specified environment variables.

- *AspNetHostingPermission*: Controls access permissions in ASP.NET hosted environments. This class cannot be inherited and initializes a new instance of the Asp .Net Hosting Permission class with the specified permission level.

- *StorePermission*: Controls access to stores containing X.509 certificates. This class cannot be inherited and initializes a new instance of the Store Permission class with the specified access.

- *UIPermission*: Controls the permissions related to user interfaces and the Clipboard. This class cannot be inherited and initializes a new instance of the UI Permission class with the permissions for windows, and no access to the Clipboard.

Limitations of the tool

- In this tool only few of the permissions are considered.
- In this tool we are setting the Permission State value to Dns Permission, Sql Client Permission, Web Permission and Type Descriptor Permission.
- Through the command line we cannot set Socket and 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