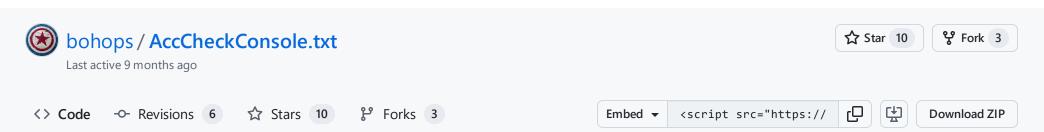


Instantly share code, notes, and snippets.



AccChecker LOLBIN [AccCheckConsole.exe]

```
Raw
     *Purpose
      - UI Accessibility Checker
      - Verifies UI accessibility requirements
     *LOLBIN Functionality/Steps
 5
      1) Go to "Custom Verification Routines" link in reference section and copy the sample verification C# code into Visual Studio.
 6
      2) Add proper assembly references (e.g. AccCheck.dll)
 7
      3) Insert your C# code under a target method such as Execute()
 8
      4) Compile to a .NET managed library (DLL)
 9
      5) Invoke the code
10
        a) There are several ways to do this. Easiest is to specify a program window name (e.g. you are going to get a handle to this).
11
           For POC, I'd recommend just opening notepad.exe and using the default Window name - "Untitled - Notepad"
12
        b) Run the following command:
13
14
        AccCheckConsole.exe -window "Untitled - Notepad" C:\path\to\your\lolbas.dll
15
16
     *LOLBAS Categories
17
      - Other MS Binary
18
19
      - Execute
      - AWL Bypass (AppLocker)
20
21
     *Location(s)
22
23
      - From Windows SDK
      - C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x86\AccChecker
24
      - C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x64\AccChecker
25
      - c:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm\AccChecker
26
      - c:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm64\AccChecker
27
      - (Other locations likely depending on SDK version and architecture)
28
29
30
     *Testing
      - Windows 10 Pro
31
32
      - Windows 10 Enterprise
      - Windows 11 Enterprise
33
34
35
     *Detection/Prevention
      - Quick KQL Search: process.name: "AccCheckConsole.exe" and process.command_line: *window* and process.args_count > 3
36
      - WDAC blocks execution of unsigned DLL
38
39
     *References:
40
       - General: https://docs.microsoft.com/en-us/windows/win32/winauto/ui-accessibility-checker
       - AccCheckConsole: https://docs.microsoft.com/en-us/windows/win32/winauto/the-accchecker-console
41
       - Custom Verification Routines: https://docs.microsoft.com/en-us/windows/win32/winauto/custom-verification-routines
42
```

Sign up for free

to join this conversation on GitHub. Already have an account? Sign in to comment

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information