

Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

Search

Sign in

Sign up

NetSPI / PowerUpSQLPublic

Notifications

Fork463

Star2.5k

<> Code

Issues19

Pull requests3

Actions

Projects

Wiki


Security

Insights

master

Go to file

<> Code ▾



Update Get-Credentials-Hijack.tsqld5250eb · 3 months ago1,000 Commits

images

Add files via upload

5 years ago

presentations

Add files via upload

3 years ago

scripts

Create LinkConvertExample.ps1

6 months ago

templates

Update Get-Credentials-Hijack.tsqld5250eb · 3 months ago

tests

Update pesterdb.sql

6 months ago

LICENSE

Update LICENSE

2 years ago

PowerUpSQL.ps1

Update PowerUpSQL.ps1

6 months ago

PowerUpSQL.psd1

Update PowerUpSQL.psd1

6 months ago

PowerUpSQL.psm1

Clean PowerShell Scripts

8 years ago

README.md

Update README.md

3 years ago

READMELicense

licenseNew BSD

PowerUpSQLWiki

Stars2.5k

Forks463

issues19 open

PowerUpSQL

DISCOVER

AUDIT

EXPLOIT

A PowerShell Toolkit for Attacking SQL Server

PowerUpSQL includes functions that support SQL Server discovery, weak configuration auditing, privilege escalation on scale, and post exploitation actions such as OS command execution. It is intended to be used during internal penetration tests and red team engagements. However, PowerUpSQL also includes many functions that can be used by administrators to quickly inventory the SQL Servers in their ADS domain and perform common threat hunting tasks related to SQL Server.

PowerUpSQL Wiki

For setup instructions, [cheat Sheets](#), blogs, function overviews, and usage information check out the wiki: <https://github.com/NetSPI/PowerUpSQL/wiki>

Author and Contributors

Author: Scott Sutherland (@\_nullbind)

Major Contributors: Antti Rantasaari, Eric Gruber (@egru), Thomas Elling (@thomaselling)

About

PowerUpSQL: A PowerShell Toolkit for Attacking SQL Server

Readme

View license

Activity

Custom properties

2.5k stars

107 watching

463 forks

Report repository








Releases








No releases published

Packages

No packages published

Contributors16





+ 2 contributors

Languages

PowerShell98.9%

Other1.1%

Page 1 of 2

- Contributors: Alexander Leary (@0xbadjuju), @leoloobeek, Andrew Luke(@Sw4mpf0x), Mike Manzotti (@mmanzo\_), @TVqQAAMA, @cobbr\_io, @mariuszbit (mgeeky), @0xe7 (@exploitph), phackt(@phackt\_ul), @vsamiamv, and @ktaranov

Issue Reports

I perform QA on functions before we publish them, but it's hard to consider every scenario. So I just wanted to say thanks to those of you that have taken the time to give me a heads up on issues with PowerUpSQL so that we can make it better.

- Bug Reporters: @ClementNotin, @runvirus, @CaledoniaProject, @christruncer, rvrsh3ll(@424f424f),@mubix (Rob Fuller)

License

- BSD 3-Clause