1.2.2023

Enrique Munoz

Hirslanden AG

BadUSB

Enrique Munoz

Inhalt

[Erste Schritte 2](#_Toc126569073)

[Los geht’s 3](#_Toc126569074)

[Was nun? 4](#_Toc126569075)

[Das zweite Script 4](#_Toc126569076)

Einleitung

Sportferien sind angekommen und innerhalb von 8 Tagen starte ich ein Projekt. In diesem Projekt geht es darum, einen BadUSB selbst von Grund auf zu erstellen. Zur Verfügung habe ich ein Gerät namens Flipper Zero. Dieses Gerät soll mir helfen beim Konfigurieren des USBs und bei der Ausführung.

# Erste Schritte

Als erstes muss ich den Flipper reseten, damit dieser wie neu ist und keine Konfigurationen von früher hat. Unter Settings-> Storage-> Factory-Reset habe ich das Gerät zurückgesetzt. Jetzt muss ich nurnoch die neue Firmware updaten. Mit der Applikation qFlipper kann ich per GUI das Firmware Update durchführen.

# Los geht’s

Als erstes wollte ich ein Script schreiben, welches schnell geht und einfach zu testen ist. Ich habe mich für ein Script entschieden, welches direkt ein Youtube Video abspielt. Zuerst musste ich sehr viel Google benutzen, da ich keinen Plan hatte wie das funktioniert. Sehr schnell bin ich auf die Übersicht der Sprache gekommen. Ich habe direkt angefangen zu testen und mithilfe eines Scripts online habe ich meinen ersten Test durchgeführt. Der Test ist gescheitert und ich musste herausfinden warum. Das Problem war, dass Gerät welches ich benutze «Flipper Zero» unterstützt nur das US Tastaturlayout was heisst, alle Y werden zu Z etc. Ich habe danach ein Python Script benutzt welches die Zeichen umwandelt und somit hat der Youtube Link etwa so ausgesehen.

«https>&&www.zoutube.com&watch\_v)dQw4w9WgXcQ ab?channel)RickAstlez»

Nochmals getestet und es funktionierte. Beim zweiten Mal überraschenderweise nicht. Manchmal ging es und manchmal nicht. Ich war sehr verwirrt und ich wusste es war etwas mit dem Link. Nach vielen Tests habe ich gesehen, dass das Script nicht genau weiss, wo der Link startet. Rapide habe ich das US Zeichen für Doublequotes gesucht und es war ein «@». Somit hat der Link nun wie folgt ausgesehen.

«@https>&&www.zoutube.com&watch\_v)dQw4w9WgXcQ ab?channel)RickAstlez@»

Hiermit funktionierte es perfekt. Schliesslich war ich so stolz auf mich, weil ich das Script selber umgeschrieben habe und ich mich langsam sehr gut mit der Sprache ausgekannt habe. Ich war sehr motiviert und wollte direkt weiter machen.

## Was nun?

Nachdem mein erstes Script funktioniert hat, wusste ich nicht mehr weiter. Ich hatte Ideen aber keinen Plan mit welcher ich starten wollte. Mir war bewusst ich kenne mich langsam gut aus, also habe ich mich für ein Script entschieden, welches alle WLAN-Passwörter des Gerätes holt.

# Das zweite Script

Mit ein wenig Recherche habe ich die richtigen Schritte gefunden und das Script hat alle Passwörter in Files aufgeschrieben. Ich war aber nicht zufrieden. Die Files wurden auf demselben Gerät gespeichert und dies hat mich sehr gestört, weil die Passwörter auf dem anderen Gerät mir nichts bringen. Selbst bin ich auf die Idee gekommen und habe meine externe Disk mit dem Laufwerkbuchstaben W benennt. Das ist wichtig, weil der Pfad fest sein muss und da der Laufwerkbuchstabe W nie benutzt wird, habe ich diesen gewählt. Daraufhin habe ich den Befehl abgeändert und gesagt, die Files sollen auf meine externe Disk gespeichert werden. Getestet und es hat perfekt funktioniert. Je mehr ich gemacht habe desto mehr Motivation habe ich bekommen. Ich konnte schon Passwörter stehlen.