Projektstudium Pentesting

Moritz Rupp, Marius Hald, Lukas Heinzelmann, Dean Basic

Inhalt

- Projektvorstellung
- Zielgerät
- Vorgehen
- Scan
- Berichte

Projektvorstellung

- Durchführung eines Penetrationstestes unter realen Bedingungen
- Anwendung auf ein reales Produkt/System
- Erstellung eines Reports
- Vorstellung bei Auftraggeber

Zielgerät Vorstellung

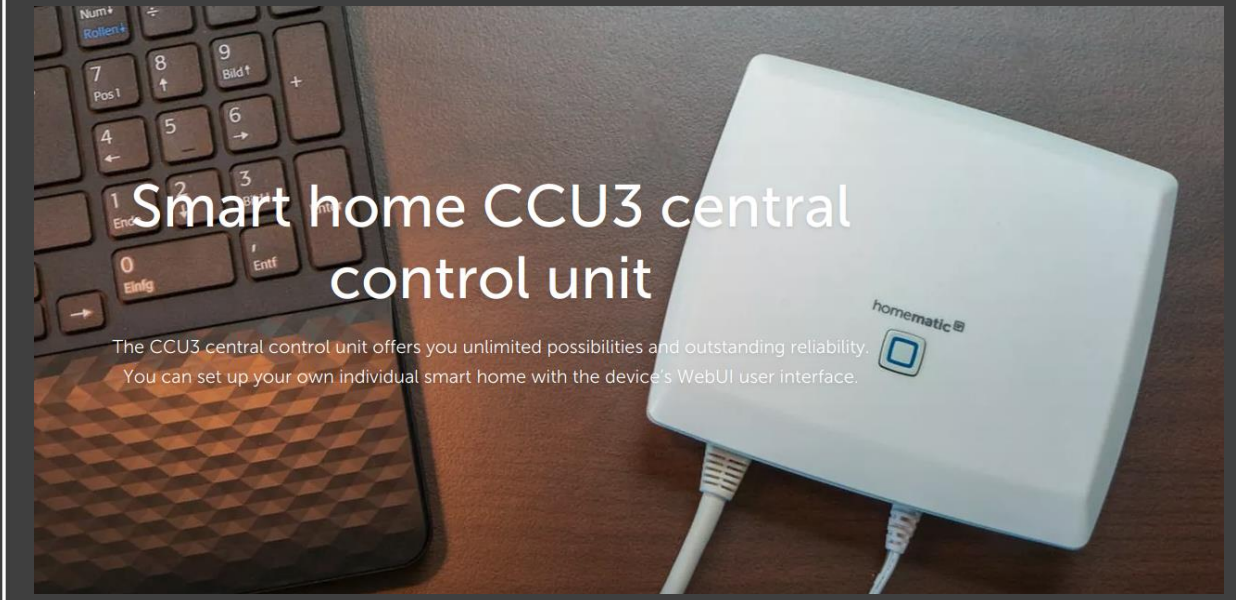
- Smart Home Zentrale

Heimautomatisierung

- Steuereinheit für Verbundene Geräte

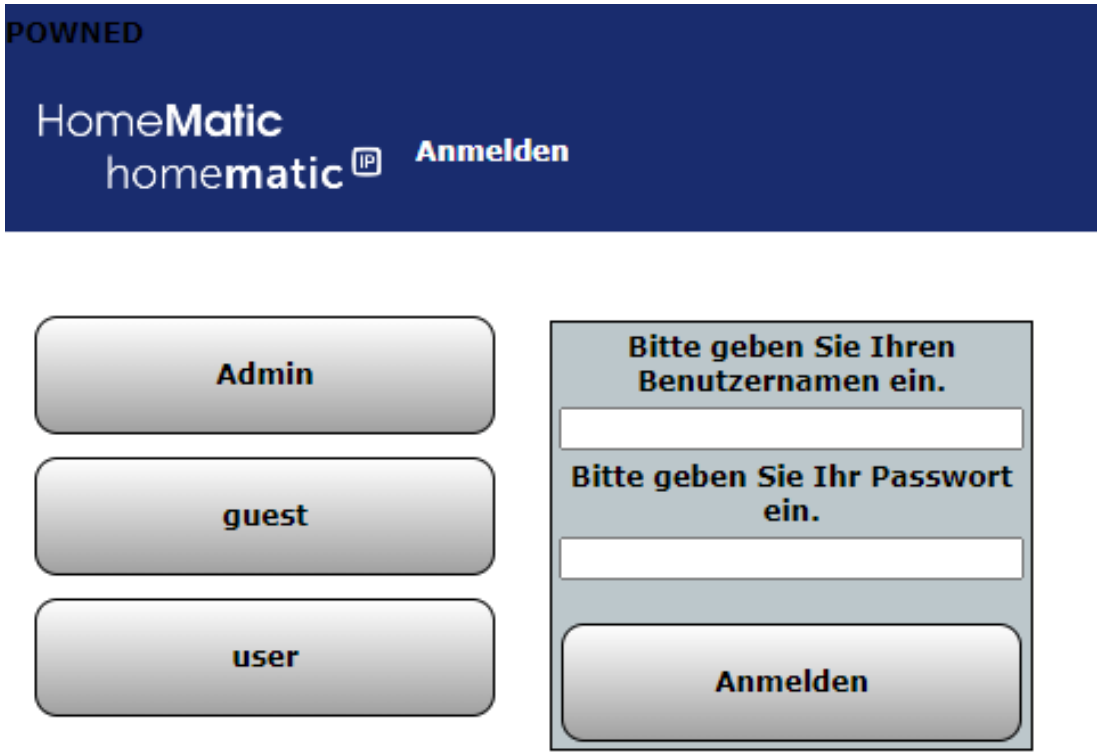
- Heizung, Rolläden, Türen, Fenster, Beleuchtung

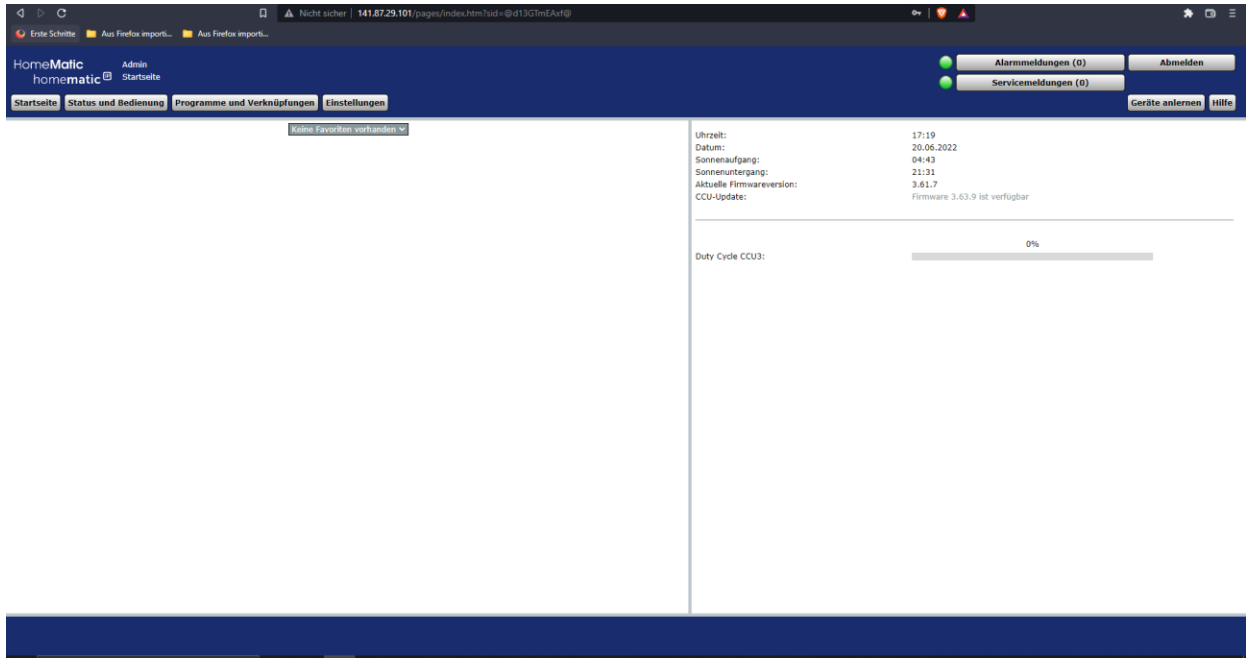
- Bietet Weboberfläche



- Homematic nutzt ein verbauten Raspberry Pi 3b2015
- Custom board mit Antenne zugebaut
- Leicht zugänglich

Weboberfläche





Vorgehen

- Planung

- Scope

- Ziele

- Scan

- Manuelle/Automatische Vulnerability scanner

Nmap, Dirbuster, OWASP ZAP, Curl, Shodan

- Minimierung der Befunde
- Austestung der Schwachstellen
- Analyse und Report

Planung

Scope: Testen der Geräte Hardware und Software auf Schutzziele der Informationssicherheit

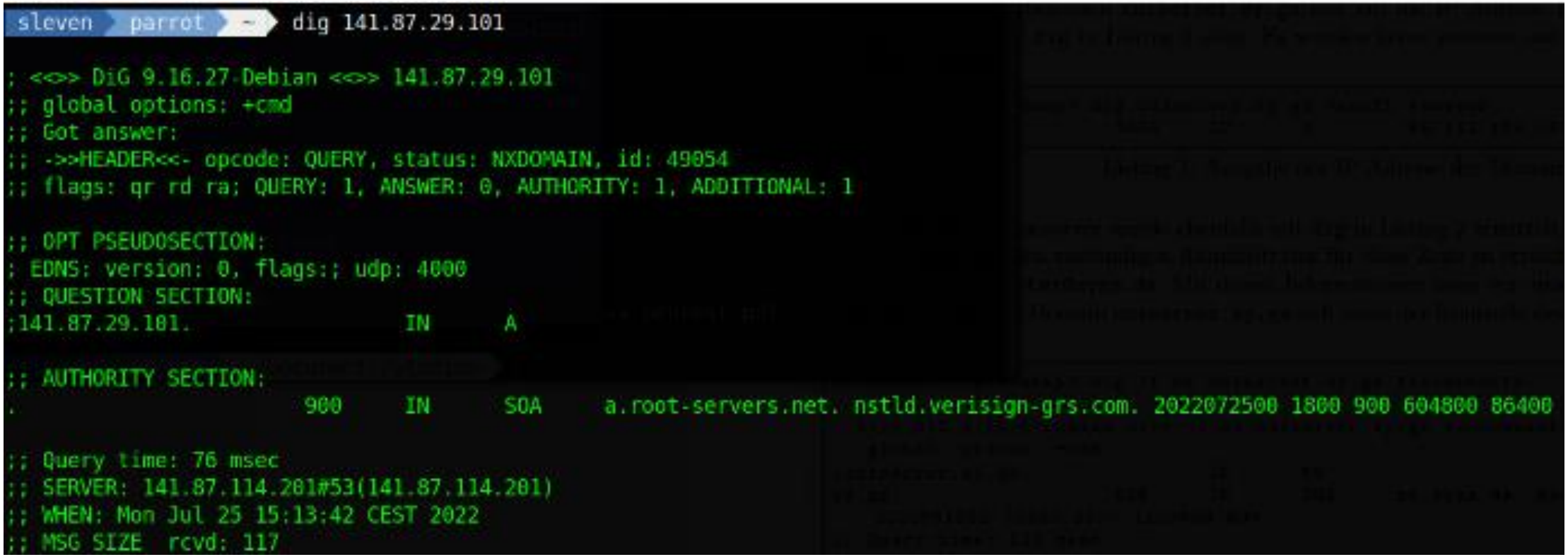
Greybox ansatz

Szenario abhängig

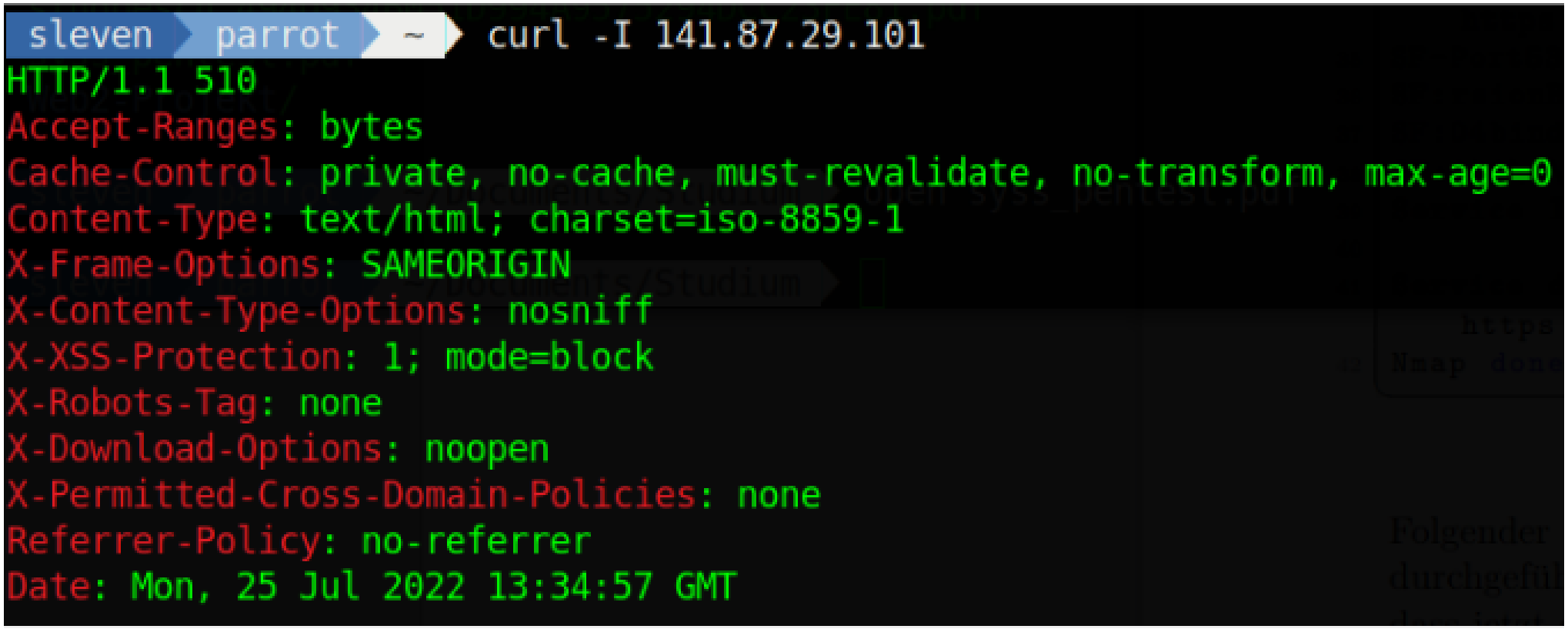
Ziele: Festellung und Verbesserung des Sicherheitszustandes

Scan

- Reconnaissance mit tools wie dig, nmap, curl



Fingerprinting



Fehlender HTTP Security header

- **Content-Security-policy (csp):**

Über diese kann gesteuert werden, welche Inhalte aus welcher Quelle Zugelassen werden. Hierüber können Javascript Angriffe wie XSS etc. Verhindert werden.

Empfehlung:

- default-src 'self/none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';base-uri 'self';form-action 'self'

- **Strict transport Security:**

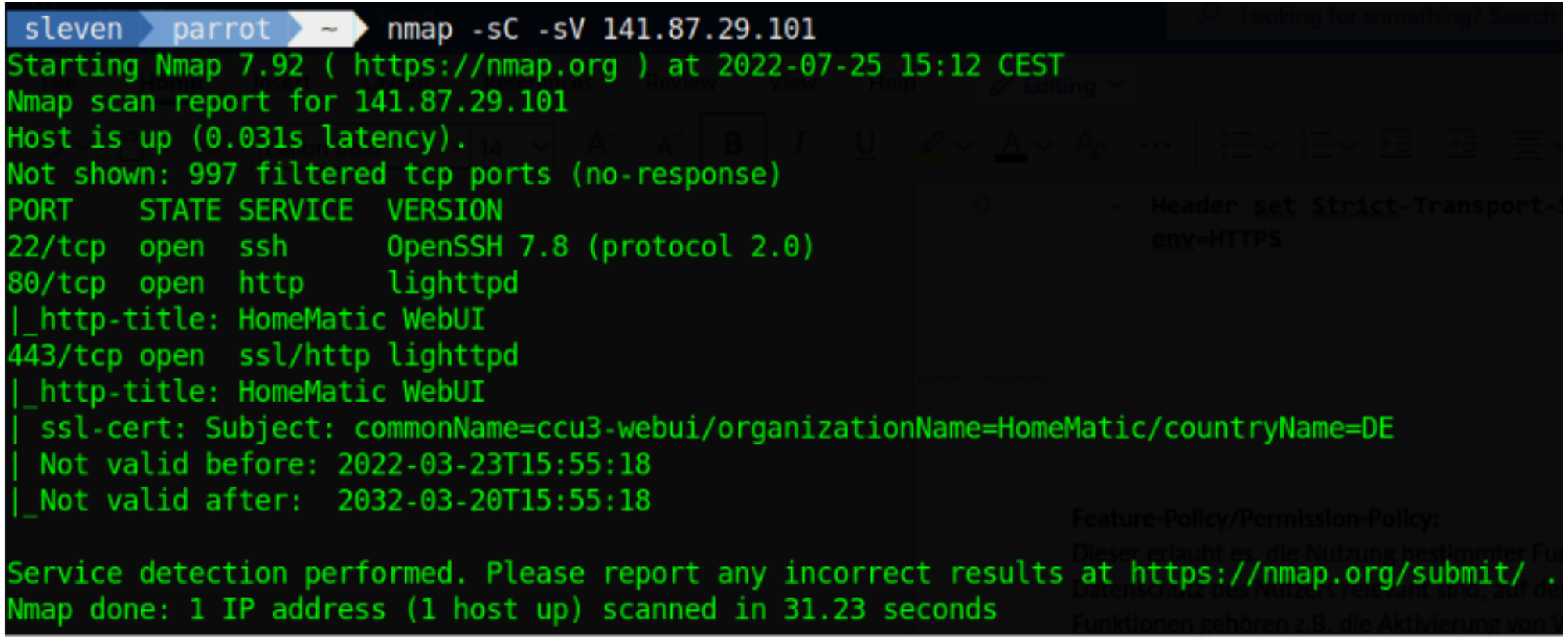
- Festlegung zu Webseiten Aufrufe auschließlich über HTTPS.

- Verhinderung von MiM Angriffen

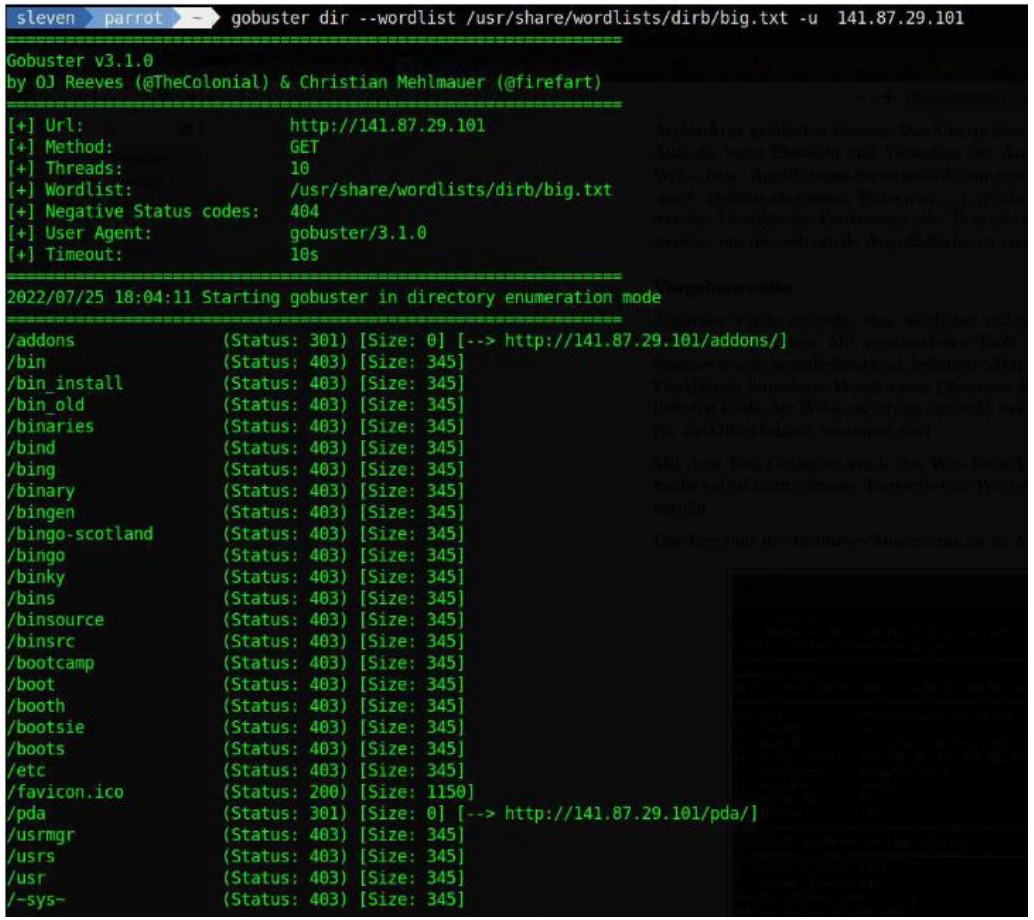
Empfehlung:

- Header set Strict-Transport-Security "max-age=31557600" env=HTTPS

Portscan


sleven parrot ~ nmap -sC -sV 141.87.29.101
Starting Nmap 7.92 (https://nmap.org) at 2022-07-25 15:12 CEST
Nmap scan report for 141.87.29.101
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.8 (protocol 2.0)
80/tcp open http lighttpd
|_http-title: HomeMatic WebUI
443/tcp open ssl/http lighttpd
|_http-title: HomeMatic WebUI
| ssl-cert: Subject: commonName=ccu3-webui/organizationName=HomeMatic/countryName=DE
| Not valid before: 2022-03-23T15:55:18
|_Not valid after: 2032-03-20T15:55:18
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.23 seconds

Enumeration



Outdated jquery Versionen

- http://141.87.29.101/webui/js/extern/jquery.js?_version_=2.0pre1
  - Führen zu CVE-2020-11023 und CVE-2020-11022
  - Empfehlung: Updaten auf neuste jquery Version

CVE-2020-11023 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.

Current Description

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Fehlende Anti CSRF Tokens

- http://141.87.29.101/login.htm
- Umgehung von Same origin policy
- Cross-site request forgery möglich

- Empfehlung

- Verwendung eines anti-CSRF Packetes

Session ID Rewrite

- Bei Anmeldung wird eine Session ID angelegt.

- Diese wird über URL rewrite erzeugt.

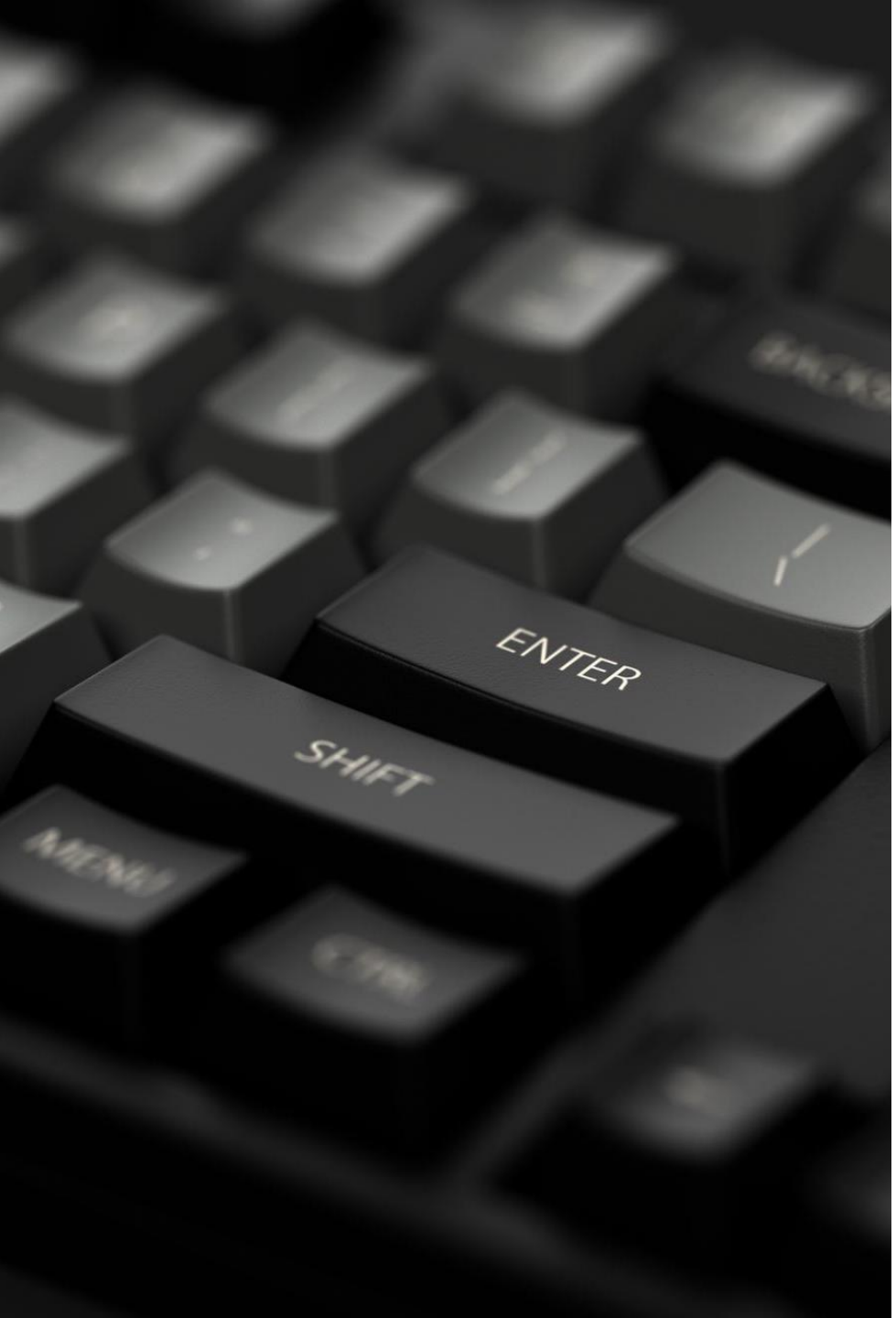
- Kann somit in Server logs, oder Browser cache/verlauf einsehbar werden.

- Nach Fenster Schließung ist Session ID 300 Sekunden lang gültig.

Empfehlung:

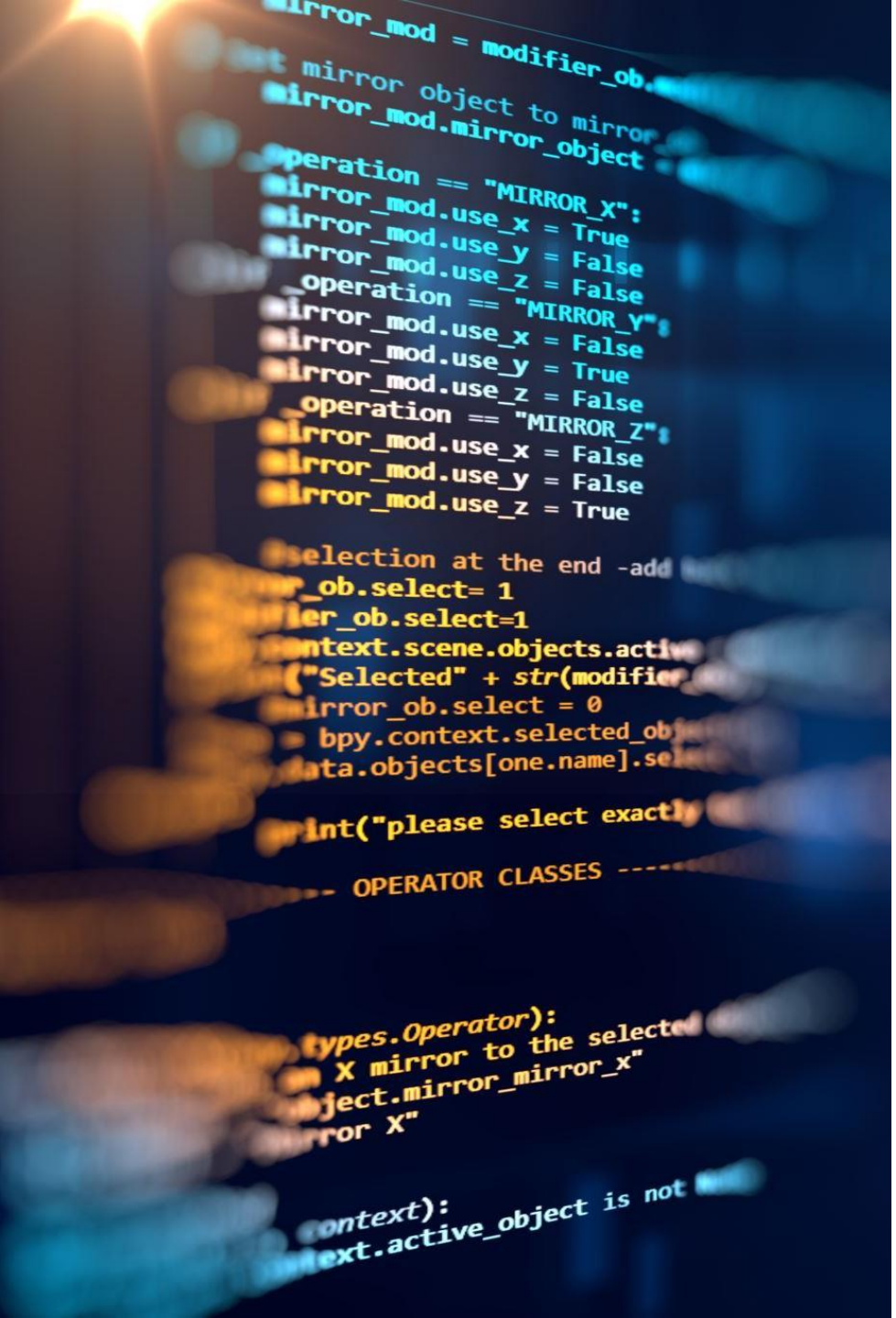
- Session ID in einem Cookie speichern

- Gültigkeit nach Fensterschließung auf 180 sekunden reduzieren



Brute Force

- Keinen Cooldown bei Passwort Eingabe
- Admin Passwort wird nie verändert
- Keine Benachrichtigung mehrmaliger falsch Eingabe
- Passwort mit Zufallsgenerator erstellen
- Cooldown einrichten
- Besitzer des Homematic Geräts benachrichtigen



Skripte hochladen

- Skripte können innerhalb der CCU3 hochgeladen werden
- Können Schadsoftware beinhalten
- Skripte müssen erste getestet werden
- Keine unbekannten Skripte herunterladen

Software Update

- Software Updates nicht automatisch
- Update Vorgang kann sehr lange dauern
- Manche Geräte funktionieren nach Update nicht mehr
- Updates können nur vom Techniker durchgeführt werden

Remote Code Execution

- Aktuell keine bekannten Schwachstellen
- Wichtig Version >3.56.6
- Letzte bekannte kritische Schwachstelle CVE-2019-9583
- Meist wird die SessionID wird ausgelesen

Replay Angriff

- Bei einem Replay Angriff werden die Signale zur Steuerung von diversen Geräten wie z.B. Autoschlüsseln, Garagentoröffnern oder Smart Home Geräten aufgezeichnet und zu einem späteren Zeitpunkt wieder Abgespielt um diesen Steuervorgang erneut auszulösen

- Voraussetzung ist, dass dieser nicht bereits durch Rolling Code, Nonces oder ähnliches vorgebeugt wird

Replay Angriff

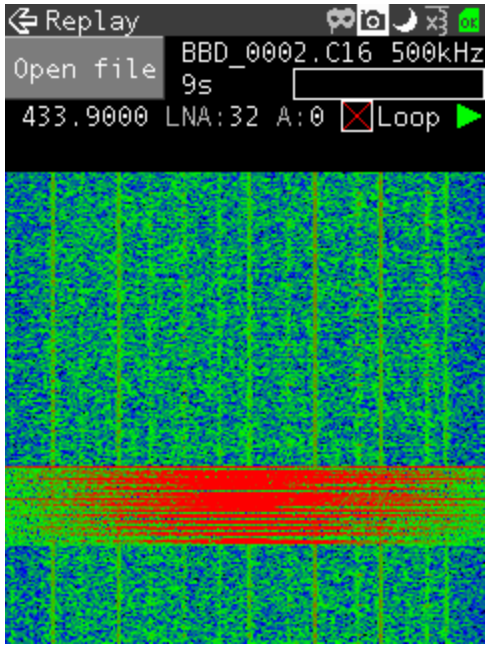
https://www.nooelec.com/store/sdr/sdr-receivers/nesdr-smart-xtr-sdr.html

Unser verwendetes SDR
(Rx only!)

https://greatscottgadgets.com/hackrf/one/I

SDR mit Rx/Tx Fähigkeit

https://www.rtl-sdr.com/tag/replay-attack/



HackRF mit Portapack

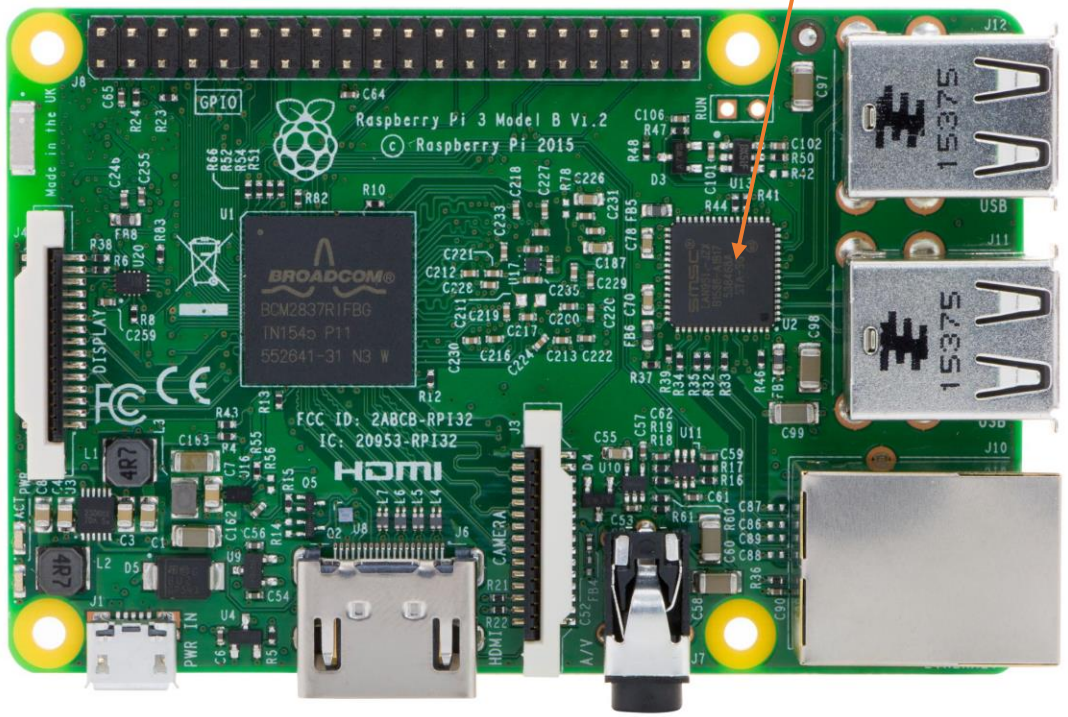
- Empfehlung: Nicht immer das Selbe Signal zur Steuerung verwenden

Usb Killer

https://scheible.it/usb-killer-rechner-zerstoeren/

Der innere Aufbau eines Usb Killers

https://de.farnell.com/raspberry-pi/raspberrypi3-modb-1gb/sbc-raspberry-pi-3-model-b-1gb/dp/2525225



Raspberry Pi 3B, wie im CCU-3 verbaut

Empfehlung:
Überspannungsschutz auf Datenleitungen oder Gerät unzugänglich machen

SD-Karte mit Software

https://www.otto.de/p/sandisk-ultra-microsdxc-64gb-speicherkarte-64-gb-120-mb-s-lesegeschwindigkeit-1461576777/#variationId=1461576778

SD-Karte auf der die Software gespeichert ist

Empfehlung: Software Verschlüsseln, Softwarehash Verifizierung und Passwörter nur mit gesalteten Hashes abspeichern