PT Report

CySDR

Executive Summary:

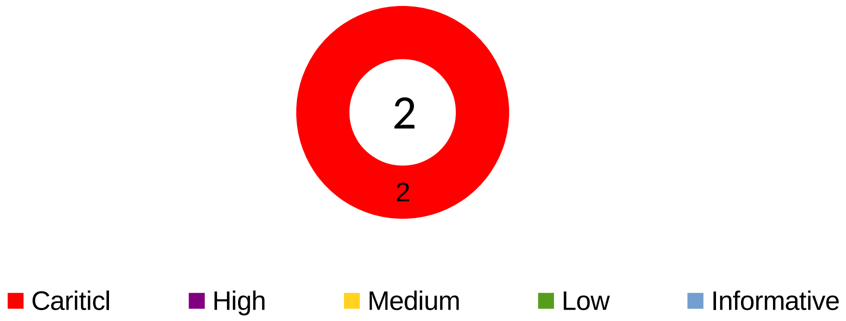
During this test, I identified and exploited critical vulnerabilities in the IoT security system, allowing unauthorized access to the vehicle and disabling security surveillance. These vulnerabilities were due to inadequate wireless security controls for both the security camera and the car entry system. Specifically, I was able to bypass the camera's monitoring capabilities through RF jamming and gain unauthorized access to the vehicle by capturing and replaying the unlock signal. These vulnerabilities present significant security risks, enabling potential attackers to compromise physical security without direct interaction with the protected assets. Due to the severity of these vulnerabilities, immediate remediation is strongly recommended to prevent potential breaches.

Conclusions:

From a professional security assessment perspective, the system is rated as **Critical**. The environment's wireless security mechanisms were deficient in protecting against common IoT vulnerabilities, specifically in signal management and access control, which allowed for successful exploitation of the following:

- **RF Jamming with the Security Camera**: This vulnerability allows attackers to disable the security camera by overwhelming its frequency, preventing it from recording or transmitting footage.
- **Signal Spoofing and Replay Attack on the Car**: This vulnerability enables attackers to capture the car's unlock signal and replay it to gain unauthorized entry.

The exploitation of these vulnerabilities requires a moderate level of technical knowledge in radio frequency (RF) manipulation and signal replay techniques. These weaknesses in the IoT security configuration could lead to significant asset exposure if left unaddressed.



Finding Details:

VULN-001 RF Jamming on the Security Camera (Critical)

Description:

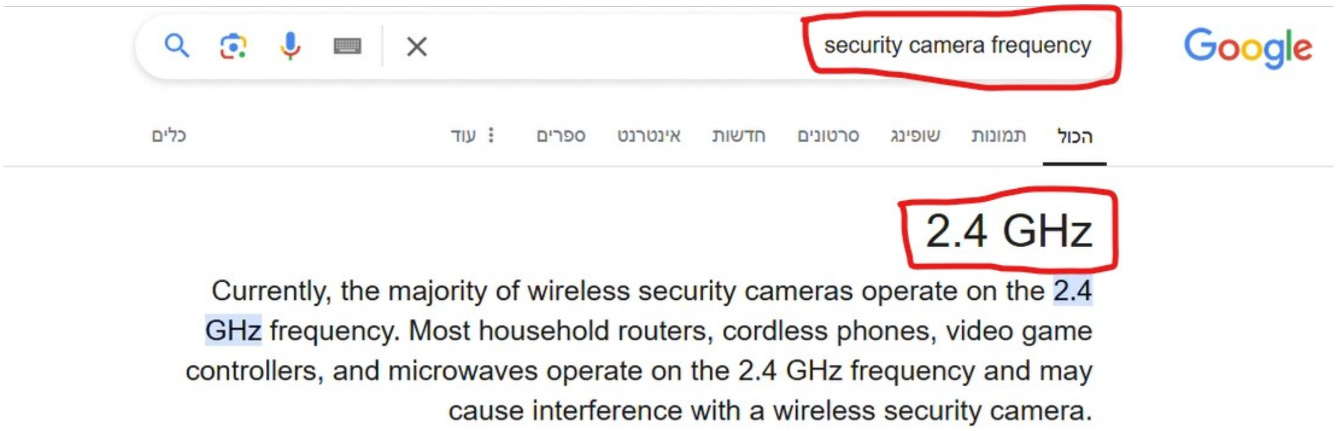
RF Jamming is a type of Denial of Service (DoS) attack that disrupts wireless communication by flooding the targeted frequency with interference signals. In this case, the security camera operates on a specific wireless frequency to transmit video feed and data. By jamming this frequency, an attacker can effectively disable the camera, preventing it from recording or transmitting any footage. This creates a blind spot in the security system, allowing unauthorized access without surveillance. In IoT environments, RF jamming poses a critical threat to security devices that rely on wireless communications, as it can be performed with relatively low-cost equipment and moderate technical knowledge. This vulnerability in the tested system compromises the effectiveness of security monitoring, especially in scenarios where continuous visual surveillance is necessary.

Details:

During the audit, it was identified that the security camera system relied solely on an unsecured wireless communication channel within the 2.4 GHz frequency band for transmitting real-time video feed. This channel was susceptible to RF interference, allowing an attacker to disrupt the signal without any form of authentication or specialized access. To demonstrate the vulnerability, I generated a high-power interference signal on the camera’s operating frequency using a software-defined radio (SDR) device. This effectively jammed the camera’s communication, preventing it from recording or transmitting any footage. As a result, the camera became unresponsive, creating a complete blackout of video monitoring in the secured area. An attacker could exploit this vulnerability to create blind spots within the camera’s coverage, enabling unauthorized physical access to restricted areas without being detected. This weakness in the camera’s wireless security could have serious implications for overall physical security, as it would allow an attacker to evade surveillance entirely.

Evidence:

This vulnerability was identified when I came to the security camera with my SDR device and I checked with google what is the camera’s frequency

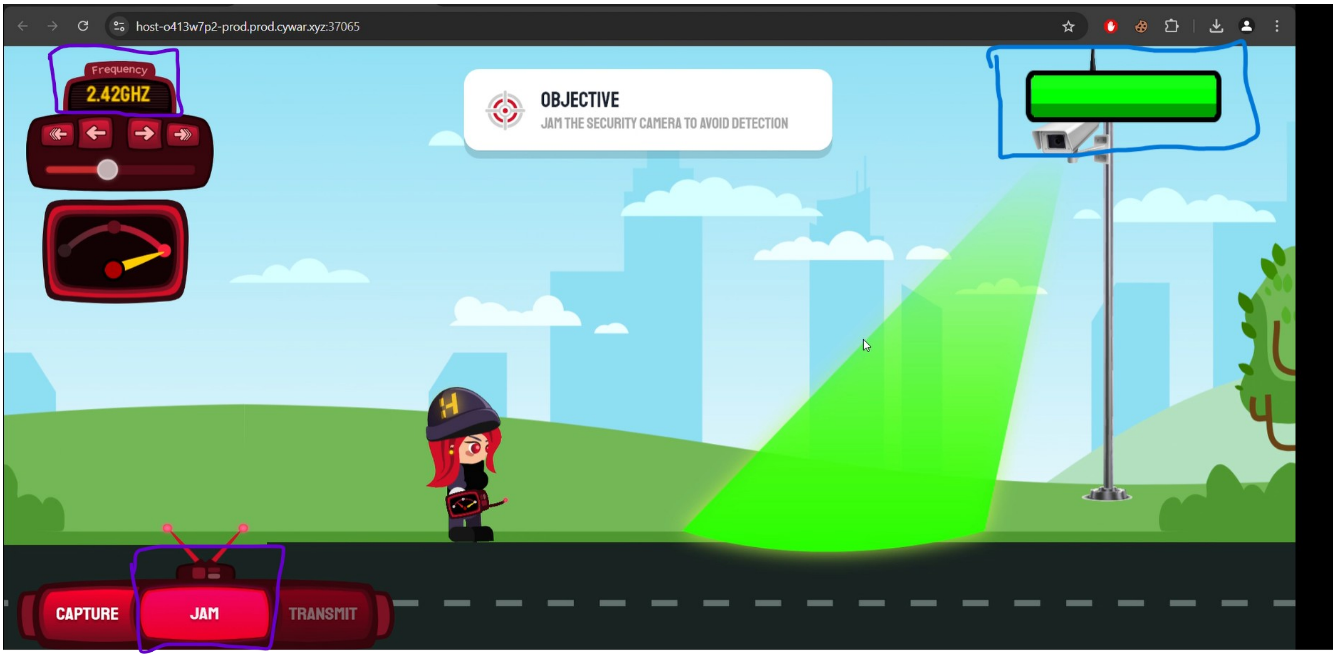


security camera frequency

2.4 GHz

Currently, the majority of wireless security cameras operate on the 2.4 GHz frequency. Most household routers, cordless phones, video game controllers, and microwaves operate on the 2.4 GHz frequency and may cause interference with a wireless security camera.

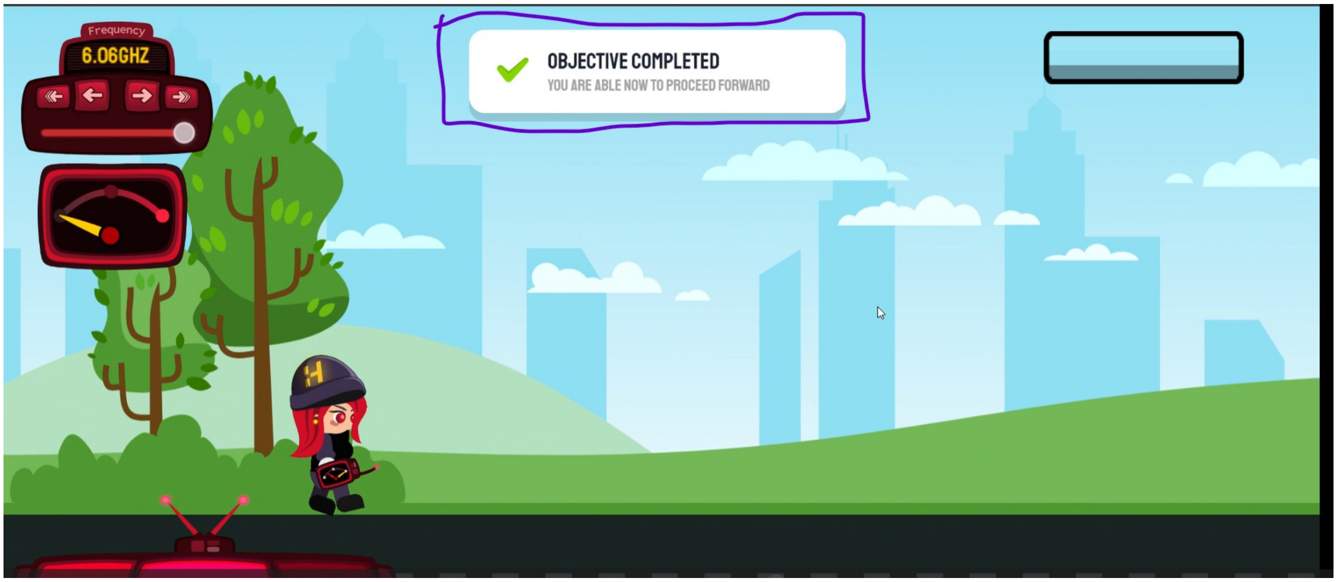
After I discovered the frequency, I began to scan the SDR by the 2.4 GHz frequency range and jam the security camera to avoid detection



host-o413w7p2-prod.prod.cywar.xyz:37065

OBJECTIVE
JAM THE SECURITY CAMERA TO AVOID DETECTION

and it’s worked and I succeed to bypass the security camera



Remediation Options:

- **Switch to Wired Cameras or Add Wired Backups for Critical Areas**: Use wired systems to eliminate RF jamming risks, or add wired backups for key cameras to ensure uninterrupted monitoring.
- **Implement Frequency-Hopping Spread Spectrum (FHSS)**: Using frequency-hopping and encrypted wireless cameras makes it harder for attackers to jam the signal.
- **Install Jamming Detection and Alert Systems**: Deploy monitoring systems to detect interference and alert security personnel in real time.
- **Increase Surveillance Redundancy**: Overlap camera views or add motion sensors for additional coverage in critical areas.
- **Conduct Regular Security Audits**: Regularly assess RF vulnerabilities and monitor the frequency spectrum for unusual activity.
- **Train Security Staff**: Educate personnel on RF jamming risks and indicators for a faster, more effective response.

VULN-002 Signal Spoofing and Replay Attack on the Car (critical)

Description:

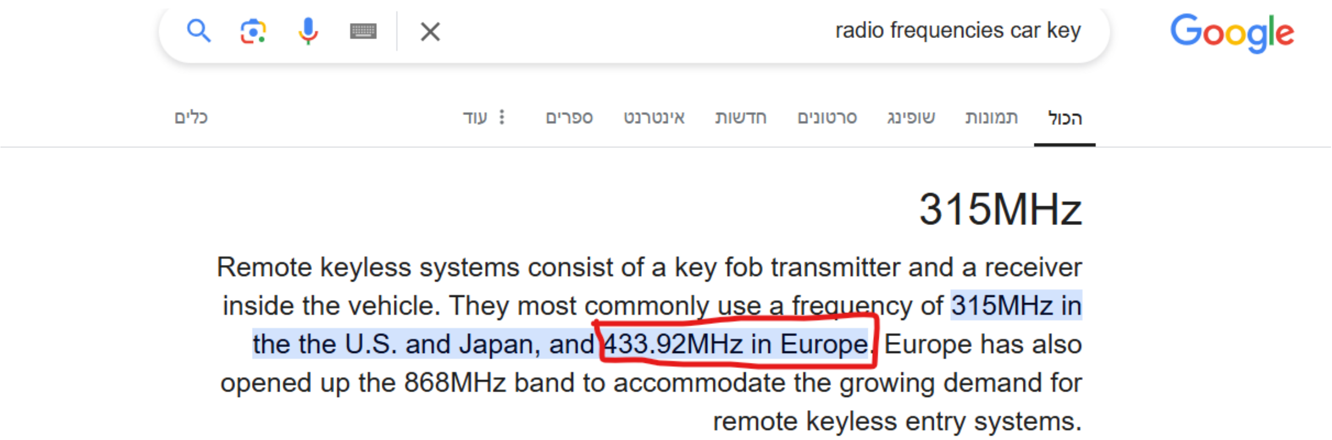
The **Signal Spoofing and Replay Attack** vulnerability affects the car’s remote keyless entry system. This type of vulnerability occurs when an attacker can capture an unlock signal from the key fob and replay it to gain unauthorized access to the vehicle. The car’s system lacks mechanisms like encryption or rolling codes, which are essential for securing wireless signals. As a result, this vulnerability allows attackers to reuse a captured signal without needing the original key, bypassing standard security controls. In automotive security, the absence of secure signal protocols in the remote access system poses a critical risk. It enables attackers to access the vehicle without physically breaking in, leaving minimal traces of the unauthorized entry.

Details:

During the test, I identified that the car’s remote access system operated without any encryption or rolling code technology, making it susceptible to signal interception and replay attacks. To confirm this vulnerability, I used a software-defined radio (SDR) device to monitor the frequency on which the key fob transmitted its unlock signal. When the key fob was used to unlock the car, I captured the signal broadcasted on this frequency and recorded its structure. Since the system lacked encryption, the signal data was stored in its original form, allowing for straightforward reuse without requiring any complex decryption. With the captured signal in hand, I proceeded to test the possibility of a replay attack. Using the SDR device, I retransmitted the recorded unlock signal to the car. As expected, the car responded to this replayed signal by unlocking, treating it as though it had been sent directly from the original key fob. This confirmed that the system did not use rolling codes or other mechanisms to validate the uniqueness of each signal, allowing the same signal to be used repeatedly without detection. Through this test, I demonstrated that an attacker could easily exploit this vulnerability to gain unauthorized access to the car. This flaw in the system’s security design could enable attackers to access the vehicle with minimal effort and no visible signs of forced entry, presenting a serious risk to vehicle security.

Evidence:

This vulnerability was identified while I came to the car with the SDR device and I checked with google what is the car key’s frequency



radio frequencies car key

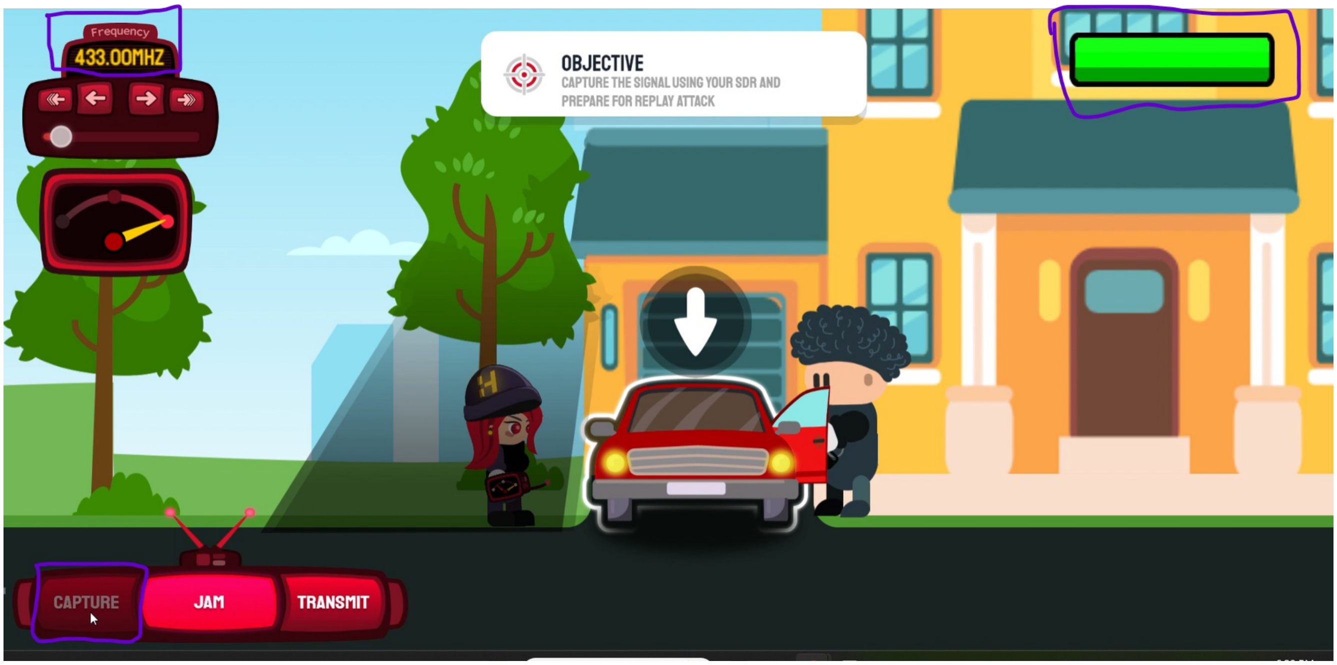
Google

הכול תמונות שופינג סרטונים חדשות אינטרנט ספרים ⋮ עוד כלים

315MHz

Remote keyless systems consist of a key fob transmitter and a receiver inside the vehicle. They most commonly use a frequency of 315MHz in the the U.S. and Japan, and 433.92MHz in Europe. Europe has also opened up the 868MHz band to accommodate the growing demand for remote keyless entry systems.

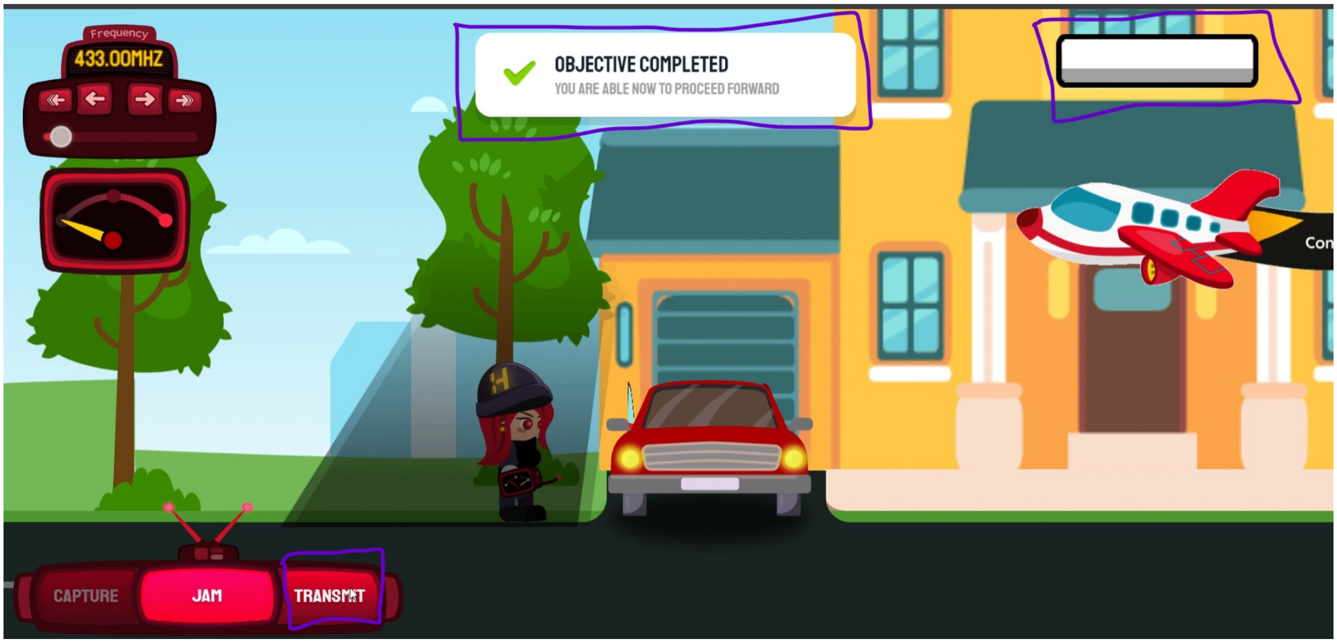
After I discovered the frequency, I began to scan the SDR by 433 MHz frequency range and captured the signal



OBJECTIVE

CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

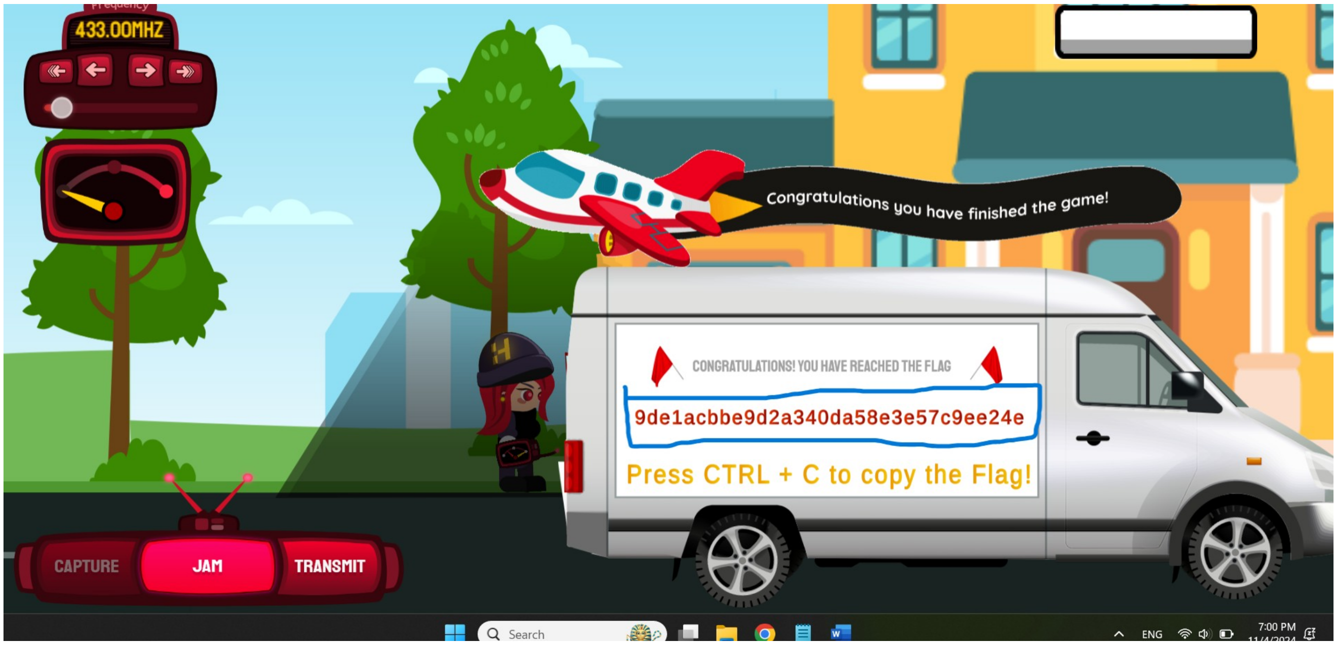
Then I transmitted the signal for replay attack



OBJECTIVE COMPLETED

YOU ARE ABLE NOW TO PROCEED FORWARD

And then I succeed to bypass and find the flag



CONGRATULATIONS! YOU HAVE REACHED THE FLAG

9de1acbbe9d2a340da58e3e57c9ee24e

Press CTRL + C to copy the Flag!

Remediation Options:

- **Implement Rolling Codes**: Upgrade the car’s remote access system to use rolling codes, which generate a unique code for each button press. This prevents replay attacks, as each code can only be used once, and the car will not respond to previously recorded signals.

- **Encrypt Wireless Signals**: Ensure the unlock signals are encrypted to prevent attackers from understanding or reusing captured transmissions. Using secure encryption protocols would make it nearly impossible for attackers to replay intercepted signals.

- **Regular Firmware Updates**: Enable regular firmware updates for the car’s remote system to patch security vulnerabilities and stay current with advanced encryption standards. Firmware updates should be easy for users to install, either through an authorized dealership or a secure, over-the-air update.

- **User Education**: Educate users on securing their key fobs to minimize the risk of interception. For example, users can store key fobs in signal-blocking pouches or cases when not in use to prevent attackers from capturing signals.

- **Introduce Physical Two-Factor Authentication**: For high-security applications, consider requiring a secondary authentication factor, such as biometric access or PIN verification, to enhance the security of remote vehicle entry systems.