דו״ח בדיקת חדירות
CyCDR

תוכן עניינים :

Background story.. 2

EXECUTIVE SUMMARY.. 2

CONCLUSIONS.. 3

Details..4

Note.. 4

VULN-001.. 5

VULN-002.. 6

: Background story

the purpose of this test was to simulate an attack in a "smart cities" environment using : advanced tools and techniques. The main objectives of the test were as follows

Controlling the character and SDR (Software-Defined Radio) devices in the game using .arrow keys and virtual buttons

Identifying and configuring the correct frequency to bypass an IP camera, highlighting .potential security vulnerabilities in this technology

Using the correct frequency to gain access to a car, simulating a potential breach into smart systems

EXECUTIVE SUMMARY

In our security assessment, we discovered two key wireless vulnerabilities in the smart ,devices. First, we were able to jam a Wi-Fi camera by disrupting its signal at 2.42 GHz using Software Defined Radio (SDR) technology and proving how easily its feed could be compromised. The second vulnerability involved intercepting and replicating key fob signals for keyless car entry. We intercepted and mimicked the signal of a car key fob between 433-434 MHz frequencies, demonstrating a method to unlock and potentially start the car without physical access to the key. These findings underscore the urgent need for stronger security in wireless communications to protect against potential breaches in smart-city environments

CONCLUSIONS

Our analysis leads us to conclude that the current state of security for the examined wireless systems is inadequate, with an overall assessment of 'Low'. The vulnerabilities : found were

Unauthorized Wi-Fi Service Interruption via Signal Jamming Vulnerability •

Key Fob Relay Attack Vulnerability •

,Both vulnerabilities could be exploited with relatively basic technical knowledge highlighting the need for immediate security improvements to mitigate the risk of .disruption and unauthorized access to essential city services and private vehicles

Vulnerabilities

CONCLUSIONS

VULN-001 Unauthorized Wi-Fi Service Interruption via Signal Jamming (CRITICAL)

Description

This vulnerability is exploited by interrupting a Wi-Fi network's operations using a signaljamming technique at the 2.42 GHz frequency range. Performed with readily accessible
SDR tools, this attack can create a Denial-of-Service (DoS) condition, severely impacting smart-city services dependent on wireless communications. The criticality of
this vulnerability lies in its capacity to cause significant disruptions with relatively low
technical effort, posing a serious security threat to public and private sectors reliant on

Details

The investigation identified a critical flaw in the wireless network׳s ability to withstand unauthorized interference.

Using only a basic understanding of Software-Defined Radio (SDR) technology, an attacker could disrupt Wi-Fi operations by targeting the network׳s active frequency, 2.42 GHz.

This attack specifically disrupted the frequency used by Wi-Fi cameras, resulting in a Denial-of-Service (DoS) condition.

By overwhelming the camera׳s signals with interference, the attacker rendered it inoperable.

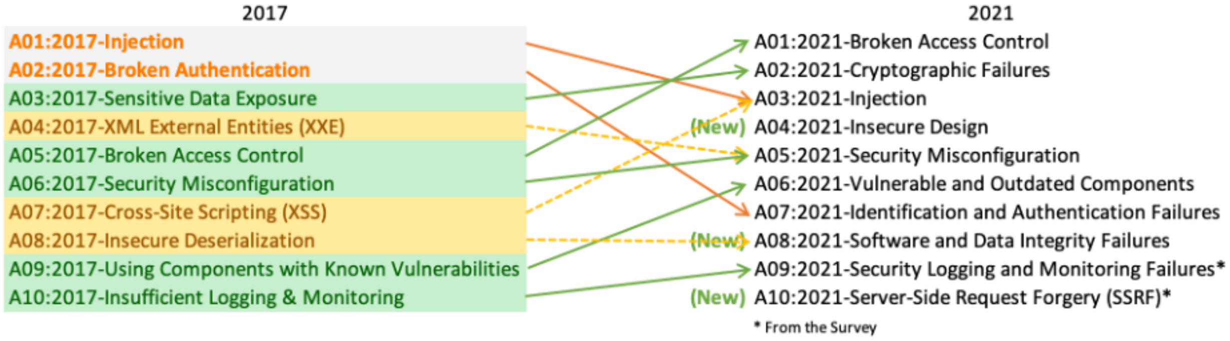
Notably, the method bypassed any need for network authentication, allowing the attacker to disable the camera without accessing the network itself.

This vulnerability could lead to unmonitored activity within the camera’s range, compromising the security and integrity of the monitored environment.

Note

Throughout the security assessment, we strictly followed the established guidelines and ensured that no Wi-Fi cameras were permanently disabled. This vulnerability has been categorized as Critical due to its ability to disrupt wireless services indiscriminately, .potentially leading to widespread security compromises within the smart-city network

The ramifications of this vulnerability are extensive, as it threatens any system reliant on Wi-Fi, including public surveillance and essential urban services. A successful exploitation could cause significant service outages and erode public confidence in the .safety and reliability of smart-city infrastructures



2017

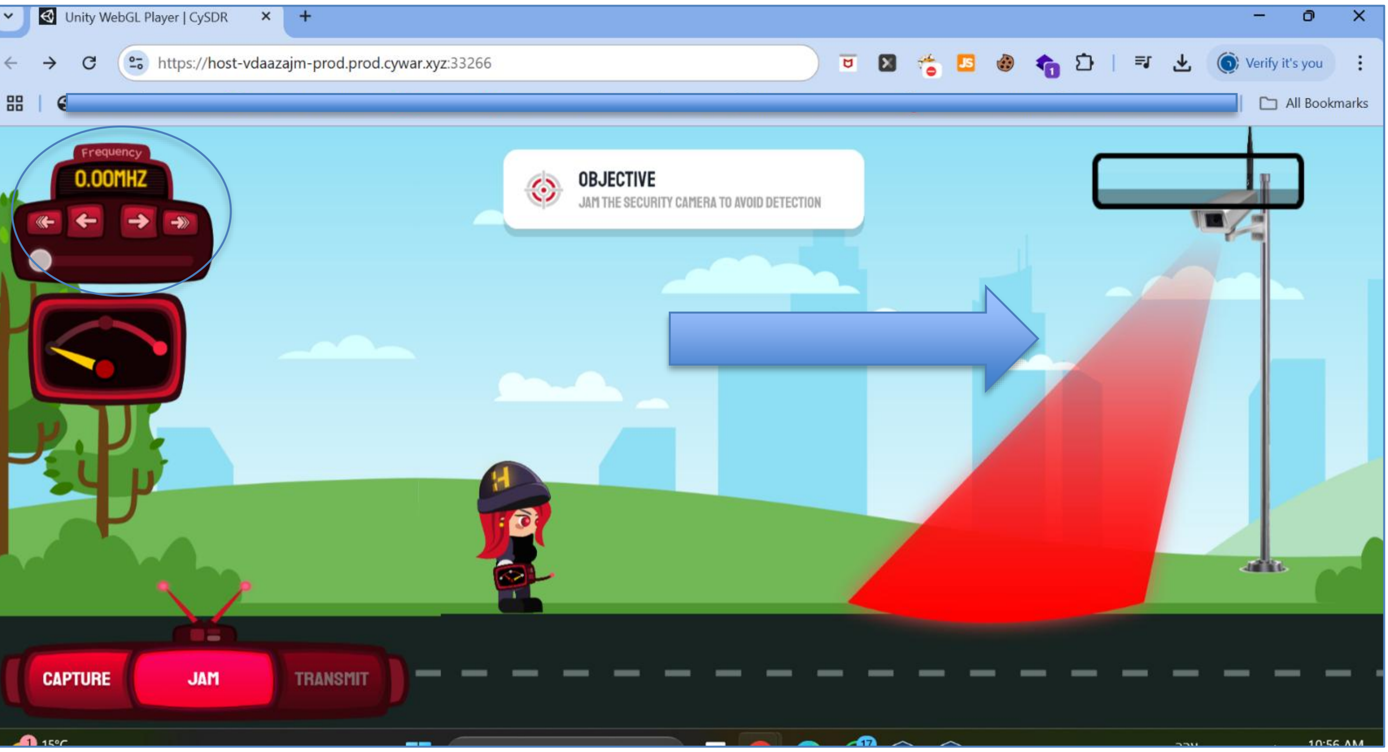
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

To discover this vulnerability, we need to stand as closest as we can without being detected by The Security Camera


Unity WebGL Player | CySDR
https://host-vdaazajm-prod.prod.cywar.xyz:33266
Verify it's you
All Bookmarks
Frequency
0.00MHZ
CAPTURE
JAM
TRANSMIT

OBJECTIVE
JAM THE SECURITY CAMERA TO AVOID DETECTION

FIGURE 1: CAMERA IS ACTIVE AT THIS MOMENT

FIGURE 2: STEP 1 SETTING THE SDR TO THE CORRECT FREQUENCY OF 2.42GHZ

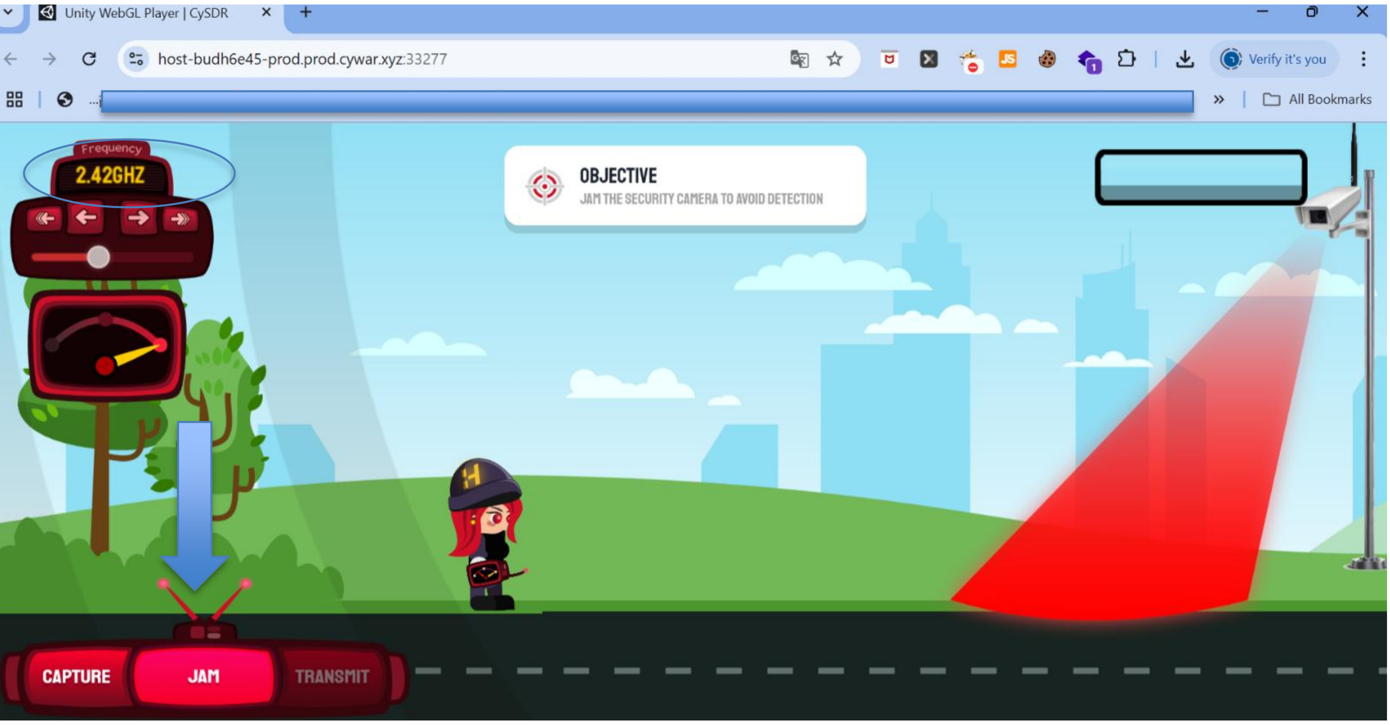
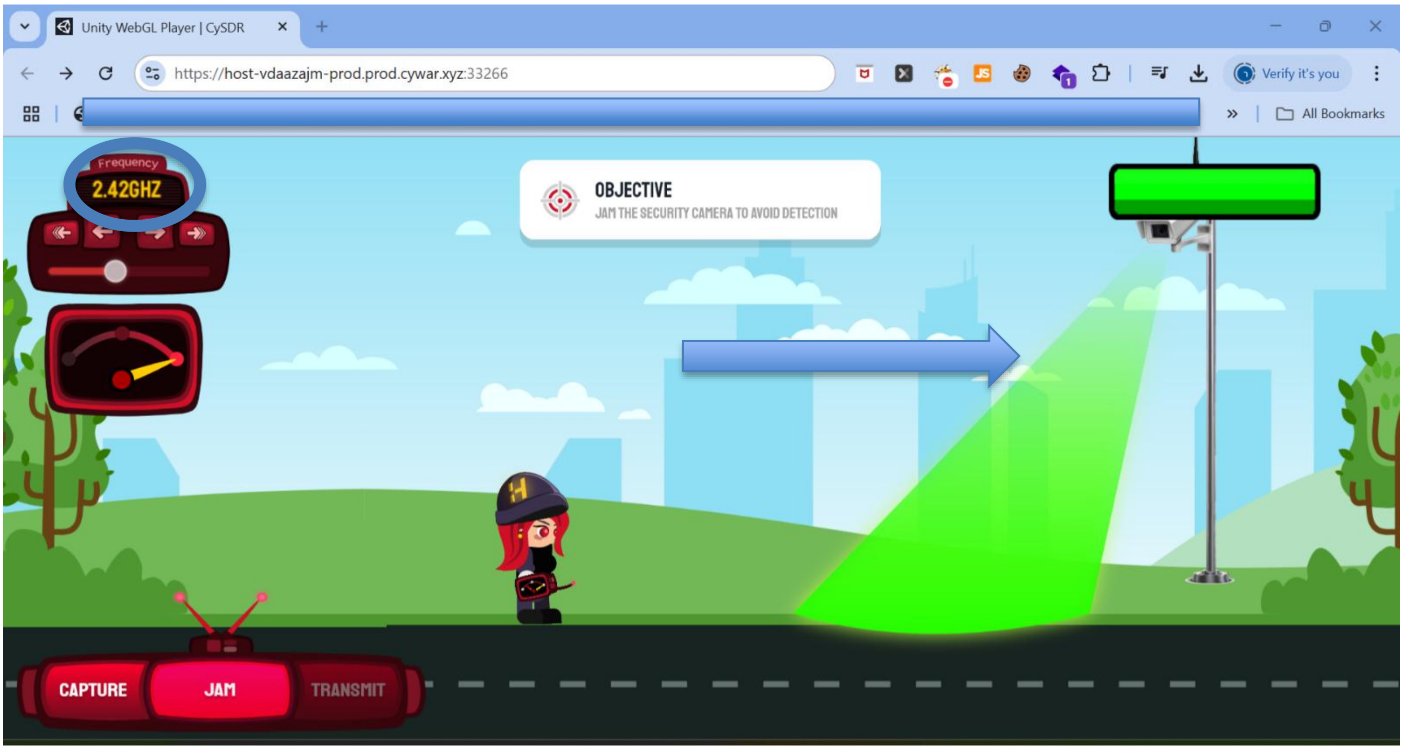
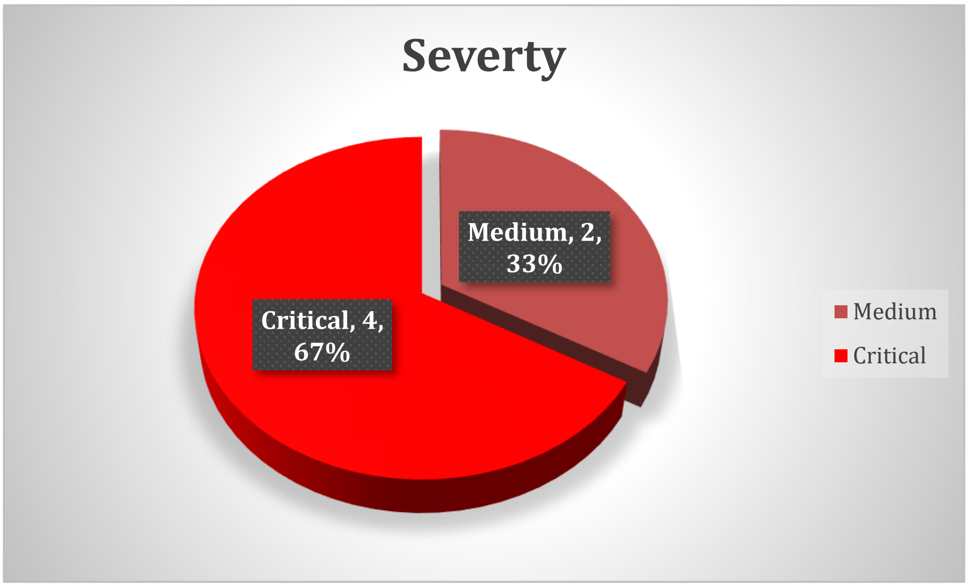

Unity WebGL Player | CySDR
host-budh6e45-prod.prod.cywar.xyz:33277
Verify it's you
All Bookmarks
Frequency
2.42GHZ
OBJECTIVE
JAM THE SECURITY CAMERA TO AVOID DETECTION
CAPTURE
JAM
TRANSMIT

FIGURE 3: STEP 2 JAMMING THE SECURITY CAMERA WITH THE RIGHT FREQUENCY


Unity WebGL Player | CySDR
https://host-vdaazajm-prod.prod.cywar.xyz:33266
Verify it's you
All Bookmarks
Frequency
2.42GHZ
OBJECTIVE
JAM THE SECURITY CAMERA TO AVOID DETECTION
CAPTURE
JAM
TRANSMIT



Remediation Options

Deploy a Wireless Intrusion Prevention System (WIPS) to continuously monitor the airspace for unauthorized signals and devices. This system should provide real-time alerts and execute automated countermeasures to address potential .jamming attempts

Utilize advanced techniques such as frequency hopping or spread spectrum modulation to reduce susceptibility to RF jamming. These methods complicate an attacker's efforts by requiring them to interfere with a wider range of .frequencies simultaneously

Schedule routine security assessments to detect signs of RF jamming and develop response protocols to quickly mitigate attacks, minimizing potential .downtime

Provide staff training to identify and respond to cyber threats, including RF interference. Regular simulations should be conducted to ensure readiness for actual attack scenarios

VULN-002 Key Fob Relay Attack Vulnerability (HIGH)

Description

The Key Fob Relay Attack vulnerability pertains to the exploitation of the keyless entry system of vehicles.

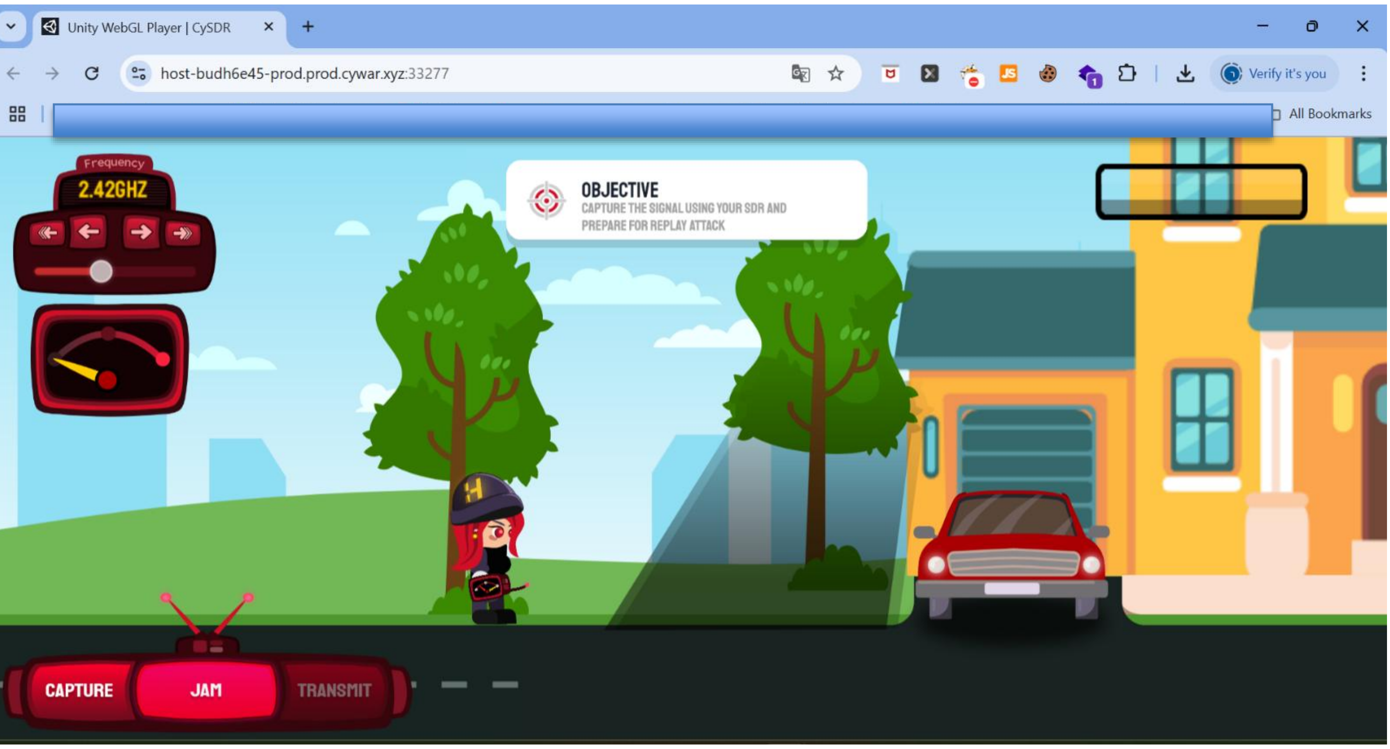
Attackers can amplify or relay the signal from a car's key fob to unlock and start the vehicle without physical possession of the key.

This breach is possible due to the lack of sufficient encryption and authentication between the key fob and the vehicle's electronic control unit.

The vulnerability is exacerbated by the key fobs continuously broadcasting signals that can be captured by unauthorized devices, making vehicles susceptible to theft and unauthorized use.

Details

In our testing, it was observed that the signal between the vehicle's key fob and its corresponding receiver lacks robust encryption, making it vulnerable to relay attacks. By utilizing a signal amplification device, an attacker can extend the range of the key fob's signal, allowing them to unlock and start the car from a distance, bypassing any need for direct contact with the key fob. This vulnerability is critical as it allows for unauthorized access to the vehicle without triggering traditional alarms or needing to overcome physical barriers.

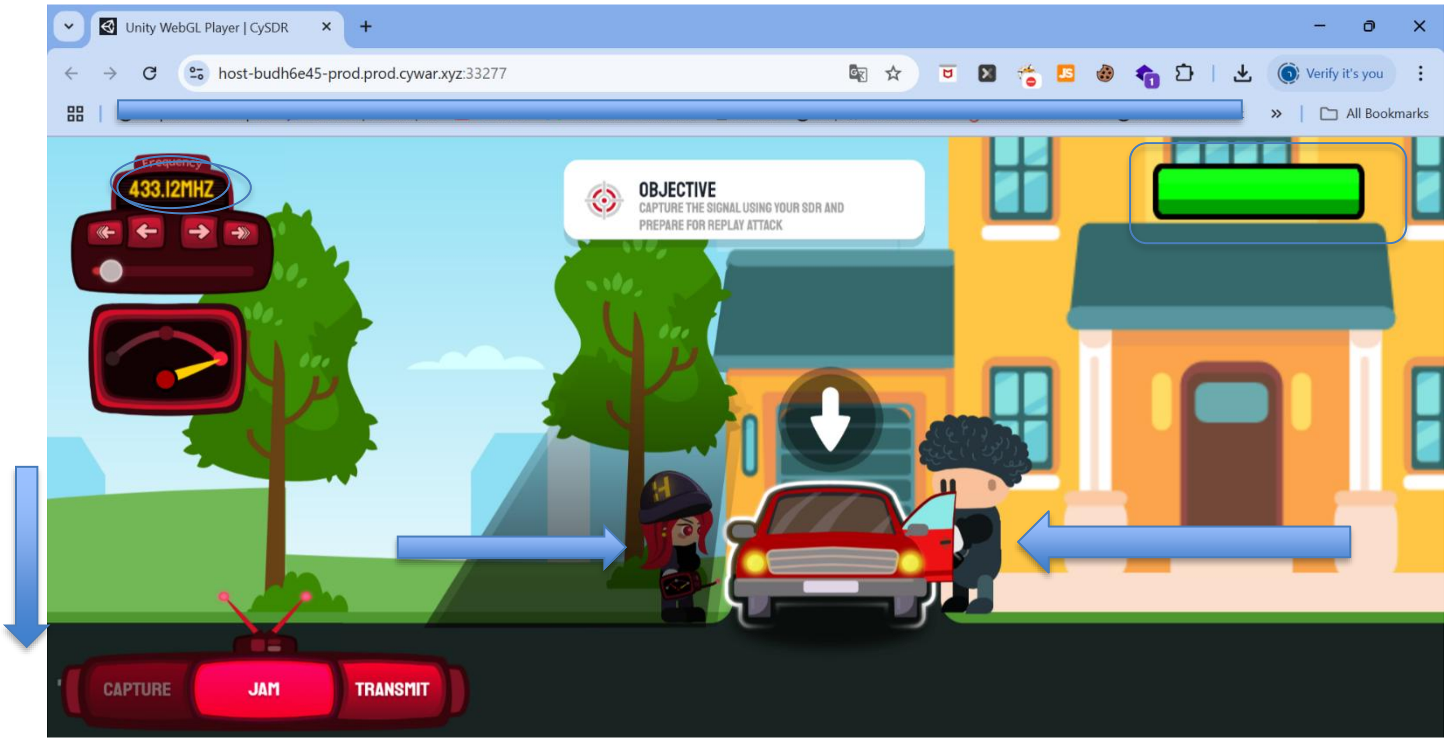


OBJECTIVE

CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

Unity WebGL Player | CySDR
host-budh6e45-prod.prod.cywar.xyz:33277
Verify it's you
All Bookmarks
Frequency
2.42GHZ
CAPTURE
JAM
TRANSMIT

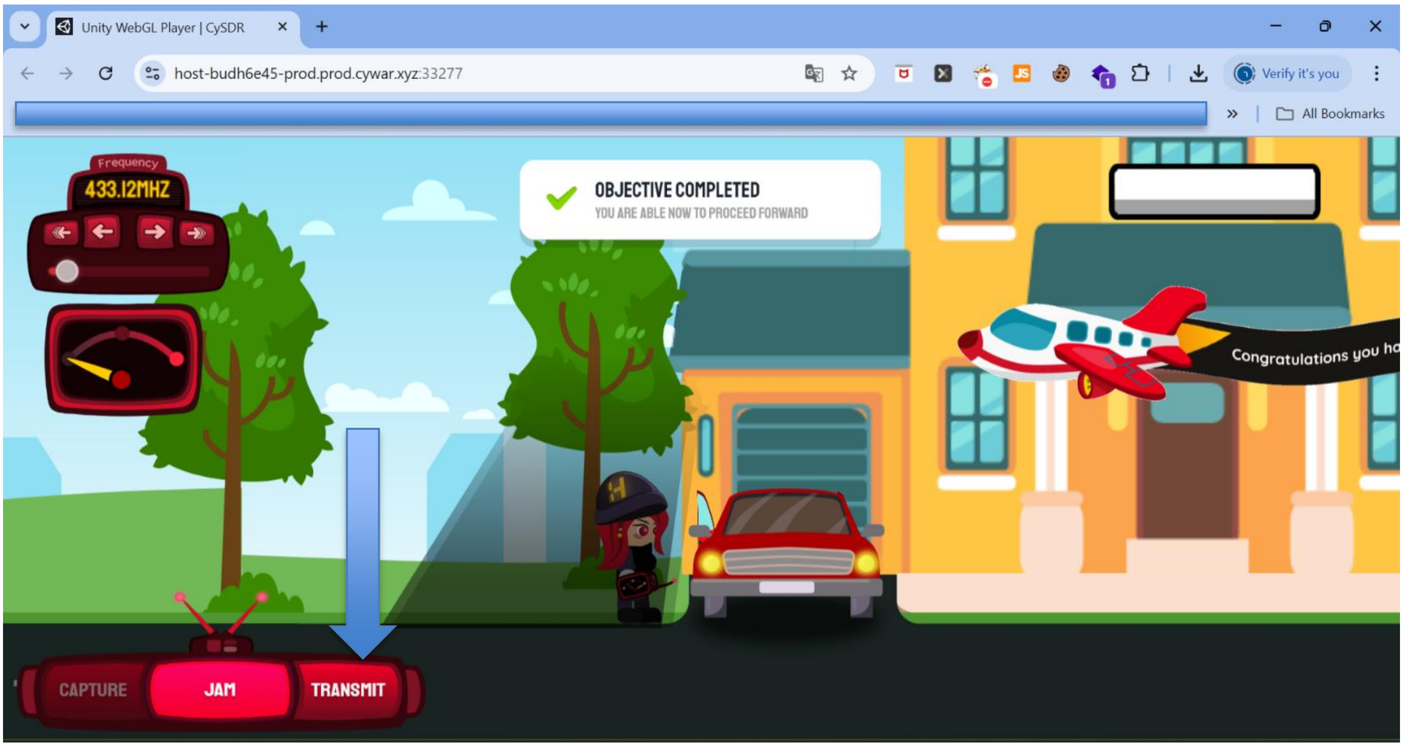
FIGURE 1: FOR OPTIMAL CAPTURE OF THE VEHICLE'S KEY SIGNAL ACTIVATION, IT IS RECOMMENDED TO SECURE A PROXIMATE AND CONCEALED POSITION.


Unity WebGL Player | CySDR
host-budh6e45-prod.prod.cywar.xyz:33277
Verify it's you
All Bookmarks
Frequency
433.12MHZ
CAPTURE
JAM
TRANSMIT

OBJECTIVE
CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

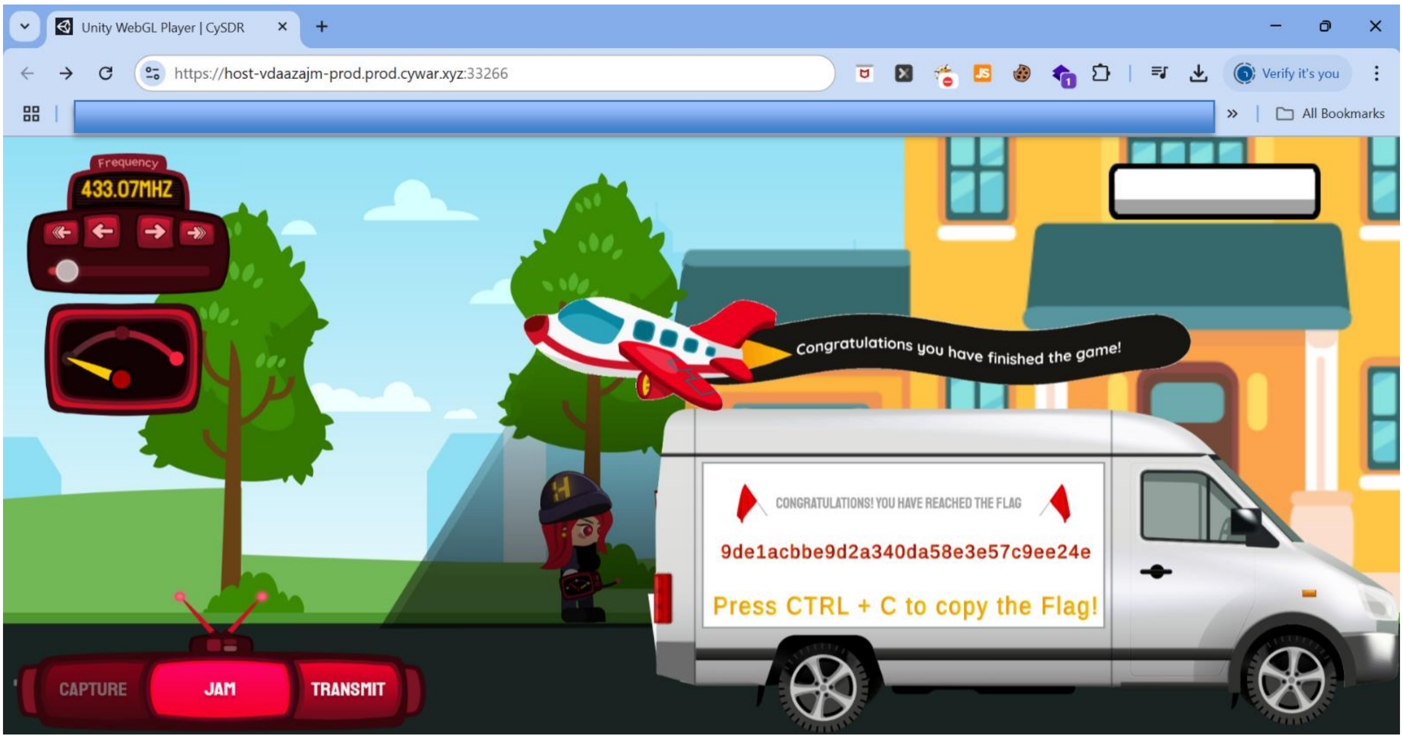
FIGURE 2: SUCCESSFULLY INTERCEPTED A SIGNAL AT 433MHZ.

FIGURE 4: SIGNAL SUCCESSFULLY INTERCEPTED!



OBJECTIVE COMPLETED
YOU ARE ABLE NOW TO PROCEED FORWARD

FIGURE 5: SUBSEQUENTLY, TRANSMISSION RESULTED IN THE VEHICLE'S DOOR UNLOCKING WITH EASE.



Unity WebGL Player | CySDR
https://host-vdaazajm-prod.prod.cywar.xyz:33266
Verify it's you
All Bookmarks
Frequency
433.07MHZ
CAPTURE
JAM
TRANSMIT

Congratulations you have finished the game!

CONGRATULATIONS! YOU HAVE REACHED THE FLAG

9de1acbbe9d2a340da58e3e57c9ee24e

Press CTRL + C to copy the Flag!