

A person in a dark suit is shown from the chest down, typing on a laptop. The image is overlaid with various futuristic digital elements: a large shield icon with a keyhole and binary code, a Bitcoin symbol, a smartphone displaying 'A1', and various glowing lines and data points. The word 'Bienvenidos' is prominently displayed in the center.

Bienvenidos

"Ad Augusta, Per Angusta"
Marco Tulio Cicerón

INSTITUTO UNIVERSITARIO DE TECNOLOGIA DE
ADMINISTRACION INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACION ALTOS MIRANDINOS



PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR

Tutores:

Ing. Vicky Linares

MSc. Henry Martinez

Autor:

Diego Aristiguieta

C.I N° V-26.624.931

Los Teques, diciembre 2022

Índice de contenido

Planteamiento del problema

Marco teórico de la investigación

Marco metodológico de la investigación

Análisis e interpretación de los resultados

Prueba de concepto

Conclusiones y Recomendaciones

Planteamiento del problema

01 ?

¿Cuál es la situación actual con respecto a la seguridad del escaneo de los códigos QR?

02 ?

¿Cuáles serían los requerimientos necesarios para conocer las vulnerabilidades de un código QR?

03 ?

¿Cómo evaluar la efectividad de la seguridad del código QR mediante la prueba de concepto como fortalecimiento tecnológico?

Justificación

Objetivos de la Investigación




Objetivo General


Demostrar una prueba de concepto como aplicación tecnológica para el fortalecimiento de la seguridad del código QR.



Objetivos Específicos

 **Identificar** la situación actual con respecto a la seguridad del escaneo de los códigos QR

 **Determinar** los requerimientos necesarios para conocer las vulnerabilidades de un código QR

 **Evaluar** la efectividad de la seguridad del código QR mediante la prueba de concepto como fortalecimiento tecnológico.

Marco Teórico

Bases Conceptuales

Prueba de concepto



Hardening o Fortalecimiento



Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo

Seguridad



Código QR



Metodología Ágil



Metodología MITRE ATT&CK

MITRE Adversarial Tactics, Techniques, and Common Knowledge. Es una base de conocimientos y un modelo seleccionados para el comportamiento del adversario cibernético



OWASP MASVS

Es el estándar de la industria de la ciberseguridad proporcionado por OWASP para la seguridad de aplicaciones móviles



Antecedentes



Rojas Guerra, Rodrigo
Andrés(2018)

CVE-2017-18192 exploit ejecutado por Metasploit sobre Kali Linux contra un SO Android para acceder al Shell



Abdelbasset Elnouby,
Mohamed (2020)

QRLJacking - A New
Social Engineering
Attack Vector



José María “Chema”
Alonso(2014 y 2019)

Robar WhatsApp de Android con Meterpreter de Metasploit y Cómo se espían móviles Android con Metasploit V5

Bases Legales

Constitución de la
República Bolivariana de
Venezuela
Artículos 60, 110

Ley Especial contra los Delitos Informáticos
Artículos 1, 4, 6, 11 y 20





Marco Metodológico

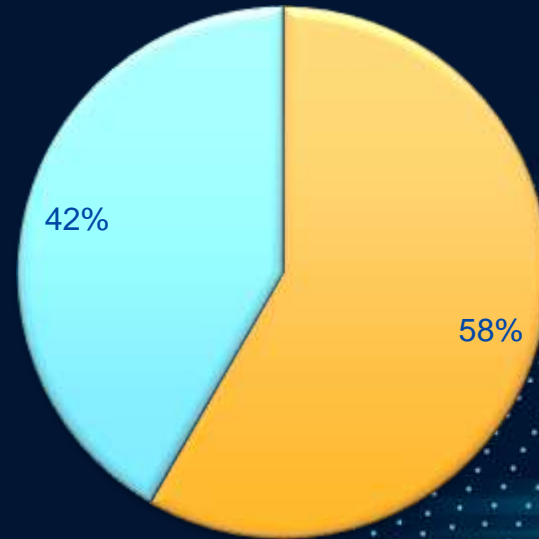


Análisis e interpretación de resultados

¿Conoce cómo funciona el escaneo de un código QR?

Sí  No 

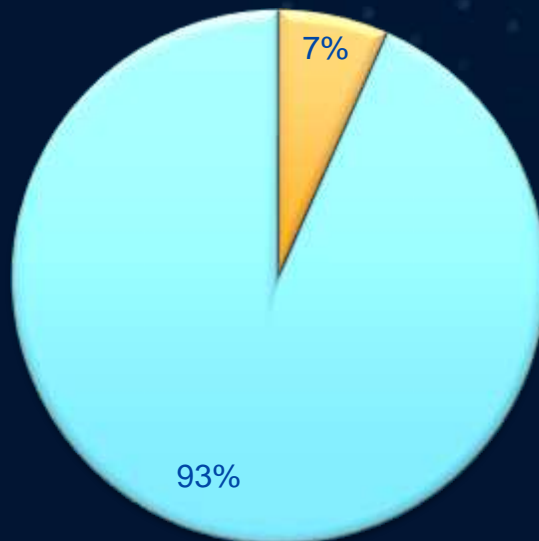
 Si
 No



¿Sabe de alguna vulnerabilidad asociada a los
códigos QR?

Sí  No 

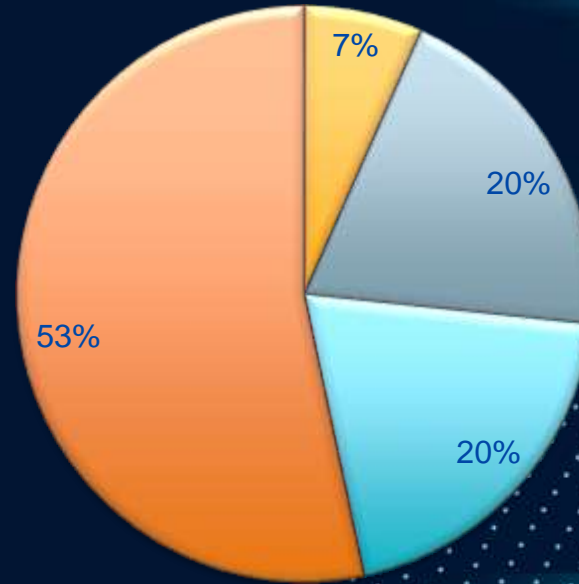
 Si
 No



¿Considera que las medidas de seguridad actuales en los códigos QR son efectivas ante ataques maliciosos?



SI ■ CS ■ AV ■ NU ■

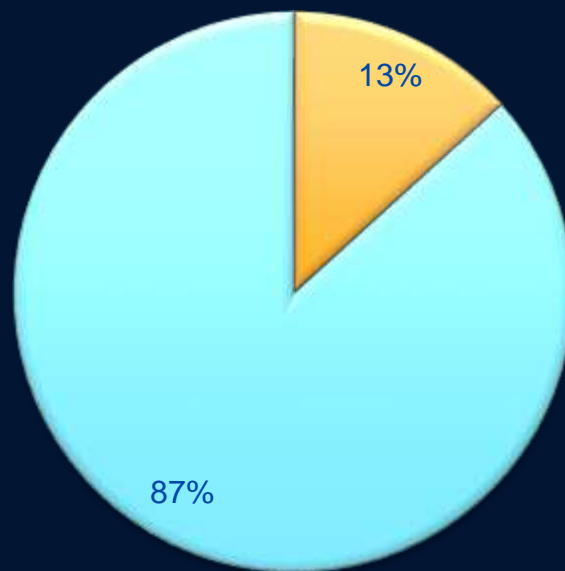
■ SI
■ CS
■ AV
■ NU



¿Sabe que mediante una prueba de concepto se pueden demostrar los posibles riesgos asociados a un código QR?

Sí  No 

 Si
 No



Prueba de concepto



Objetivo General

Demostrar que es posible tomar control de un dispositivo móvil mediante una prueba de concepto para el fortalecimiento de la seguridad del código QR.

Objetivos Específicos

Seleccionar

Realizar

Crear

Convencer

Obtener

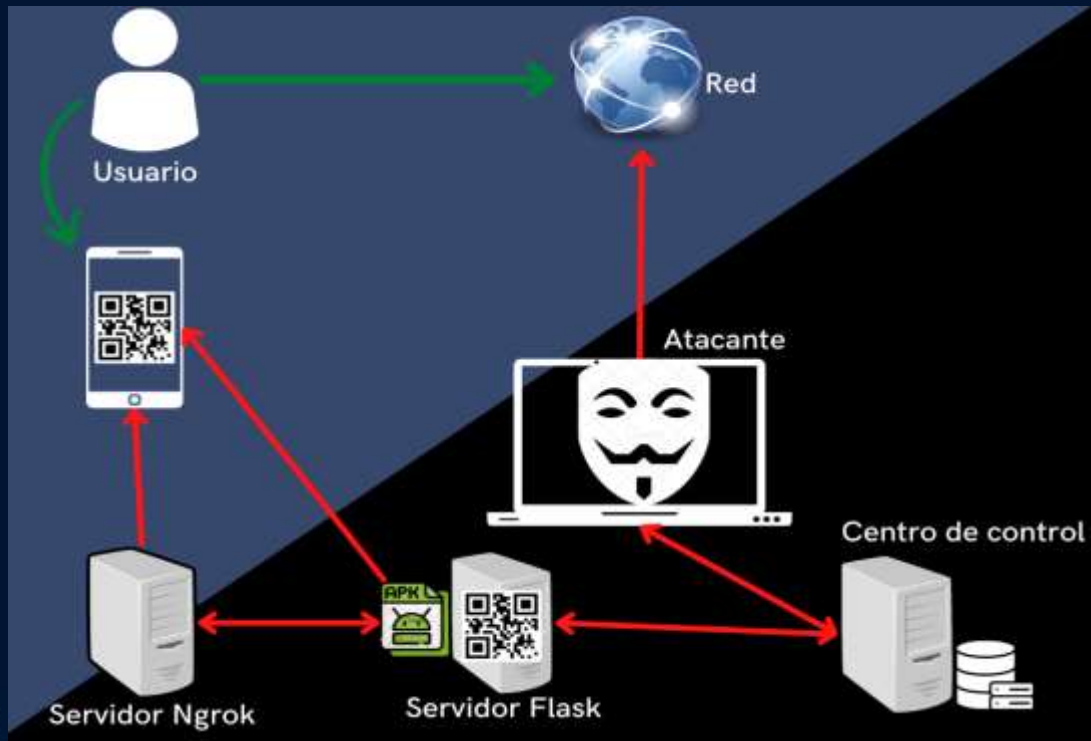
Sustraer

Mantener

Modelo entidad relación

VICTIM	
victimid	varchar(255)
ip	varchar(255)
latitud	varchar(255)
longitud	varchar(255)
city	varchar(255)
country	varchar(255)
idisp	varchar(255)

Ejecución de la POC



Demostración de la prueba de concepto

Conclusiones

El sistema de escaneo actual por defecto es ineficaz y no brinda medidas de seguridad al usuario.

Pueden ser usados bajo tres técnicas Qrphishing, descarga de malware y QRLjacking

El nivel de seguridad dependerá de diversos factores

Si es posible fortalecer la seguridad de los códigos QR.

Recomendaciones

Basta con tener un comportamiento seguro y mantenerse alerta, ya que algunos detalles no pueden ser alterados ni siquiera por el atacante más experimentado



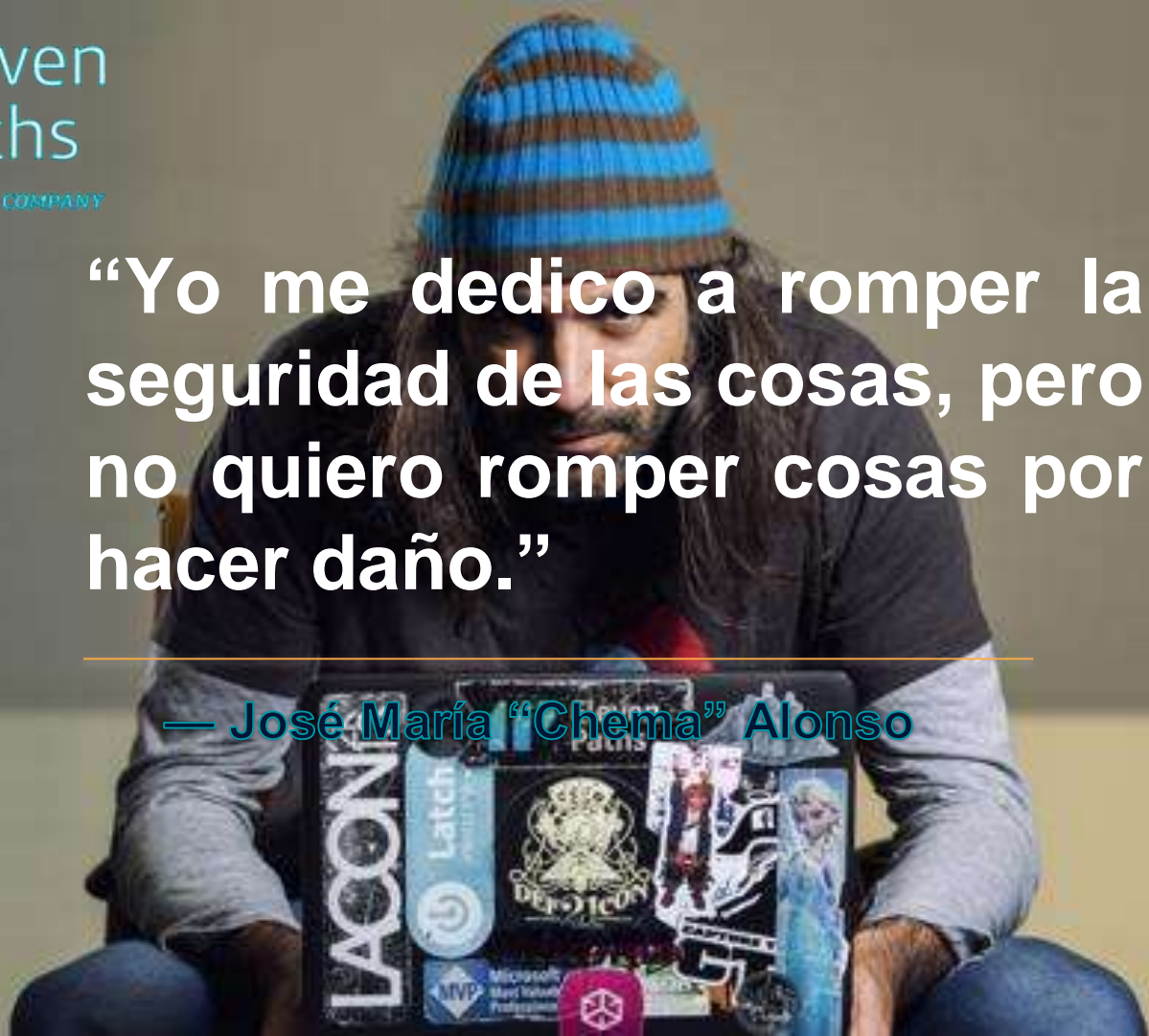


Eleven
Paths

Telefonía CYBER SECURITY COMPANY

“Yo me dedico a romper la seguridad de las cosas, pero no quiero romper cosas por hacer daño.”

— José María “Chema” Alonso





¡Gracias!

