CAPTIVE PORTAL Group06

CP422021 Introduction to Wireless and Mobile Networks with Internet of Things

อาจารย์ที่ปรึกษา: ศ.ดร.จักรชัย โสอินทร์
อ.ดร.เพชร อิ่มทองคำ

หลักการและเหตุผล

การโจมตีแบบ Phishing เป็นหนึ่งในวิธีที่แฮกเกอร์ใช้เพื่อหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลสำคัญ เช่น Username และ Password โดยมักมาในรูปแบบของเว็บไซต์ปลอมที่เลียนแบบเว็บจริง เพื่อให้ผู้ใช้กรอกข้อมูลโดยไม่รู้ตัว

วัตถุประสงค์

เรียนรู้วิธีการสร้าง Web Server บน ESP32 และการจัดเก็บข้อมูล
เรียนรู้แนวทางการทำ หน้าเว็บ Phishing จาก ESP32 เพื่อให้สามารถสร้างแนวทางในการป้องกันได้
เพื่อสร้างความตระหนักรู้ต่อผู้ใช้งานในโลกอินเตอร์เน็ตเกี่ยวกับความเสี่ยงด้านความปลอดภัยในชีวิตประจำวัน เช่น การเข้าใช้ Wi-Fi สาธารณะ

ขอบเขตการศึกษา

- สามารถทำ Phishing Website จาก ESP32 ได้
- สามารถเก็บข้อมูลที่ผู้ใช้กรอกเข้ามาเมื่อทำการเข้าสู่ระบบได้ เช่น ชื่อผู้ใช้ รหัสผ่าน

เครื่องมือที่ใช้

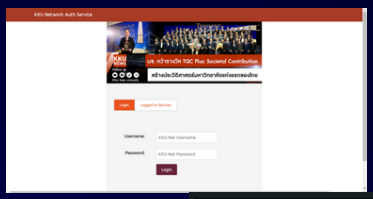
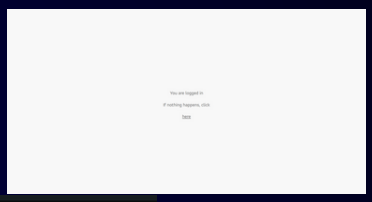
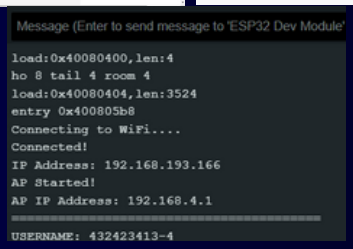


ARDUINO
ChatGPT

หลักการทำงานCAPTIVE PORTAL

เชื่อมต่อ esp32และardudino หลังจากนั้นกดรันโค้ดที่สร้างขึ้นแล้ว การทำงานนั้นก็จะเด้งขึ้นหน้าเว็บ index.html เมื่อผู้ใช้login ข้อมูลusername password จะแสดงในarduino

ผลลัพธ์ที่ได้

สรุปผล

จากการทำงานของ ESP32 และ Arduino พบว่าสามารถถูกนำไปใช้เป็นช่องโหว่ด้านความปลอดภัยได้ เนื่องจากสามารถ ดักจับและเก็บข้อมูลชื่อผู้ใช้ และรหัสผ่าน ของผู้ที่ทำการล็อกอิน ได้สำเร็จ ซึ่งอาจเกิดจากการจำลอง หน้าเว็บปลอม phishingทำให้ผู้ใช้ไม่รู้ตัวว่าข้อมูลของตนถูกขโมยไป

อ้างอิง

1.https://randomnerdtutorials.com/esp32-vs-code-platformio-spiffs/?fbclid=IwY2xjawIxCyZleHRuA2FlbQIxMAABHdu8FTBJQKZa4fOVSi6IX1WyMrYtRVgTuicITwWgEcK370B4F__hgoSSoA_aem_J2A4ClwcPglWsLZXJ8Vhag
2.https://csperson.kku.ac.th/chakchai/images/362006_2023/11.pdf?fbclid=IwY2xjawIxC7BleHRuA2FlbQIxMAABHas2r_jIXGc1lVJCM4ooYZkuuN8ElG9etiOqjiBKFGn5ZI20IwkG1GHKqw_aem_6FqY94eYX1QPlsJr4SY7gg
3.HTTPS://LOGIN.KKU.AC.TH/

สมาชิก

66338092-2 กนกนิภา ปัญเศษ
663380093-0 กนกรส ศรีบัวบุญ
663380122-9 ภูริพัฒน์ เกิดกลาง
663380477-2 ศิริญาภรณ์ ก้อนทอง