CN 321 Computer Network Sucurity

เสนอ

ผศ.ดร.ปิยะ เตชะธีราวัฒน์

จัดทำโดย

นายกฤษณเทพ	บุญพรมมา	5810613199
นายนิติวัตร	สมภาวงษ์	5810613215
นายนคร	วัจนะสาธิต	5810613231
นายสรวิชญ์	จันทชาติ	5810680347
นายจิตรเทพ	จิตรานุวัฒน์กุล	5810680388

โครงงานนี้เป็นส่วนหนึ่งของรายวิชา วพ.321

ภาคเรียนที่ 2 ปีการศึกษา 2560

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธรรมศาสตร์

คำนำ

รายงานเล่มนี้จัดทำเพื่อเป็นส่วนหนึ่งของวิชา Computer Network Security (CN321) โดยมีเนื้อหาเกี่ยวข้องกับความปลอดภัยบนเครือข่ายของ PromptOan แอพพลิเคชัน ที่ใช้โอนเงินผ่านคิวอาร์โค้ด อันได้แก่ Firewall, DDos Mitigation, Spoofing and Sniffing Protection, Port Scanning, IPS และ VPN ที่อยู่ตั้งอยู่บนเซิร์ฟเวอร์ของ Heroku

ผู้จัดทำหวังว่า รายงานเล่มนี้จะเป็นประโยชน์แก่ผู้อ่าน หรือผู้ที่จะศึกษาเรื่องของการออกแบบการรักษาปลอดภัยบนเครือข่ายคอมพิวเตอร์ได้อย่างมาก หากมีข้อผิดพลาดประการใด ผู้จัดทำขอน้อมรับไว้และขออภัยมา ณ ที่นี้ด้วย

ผู้จัดทำ

สารบัญ

Application Prompt Oan

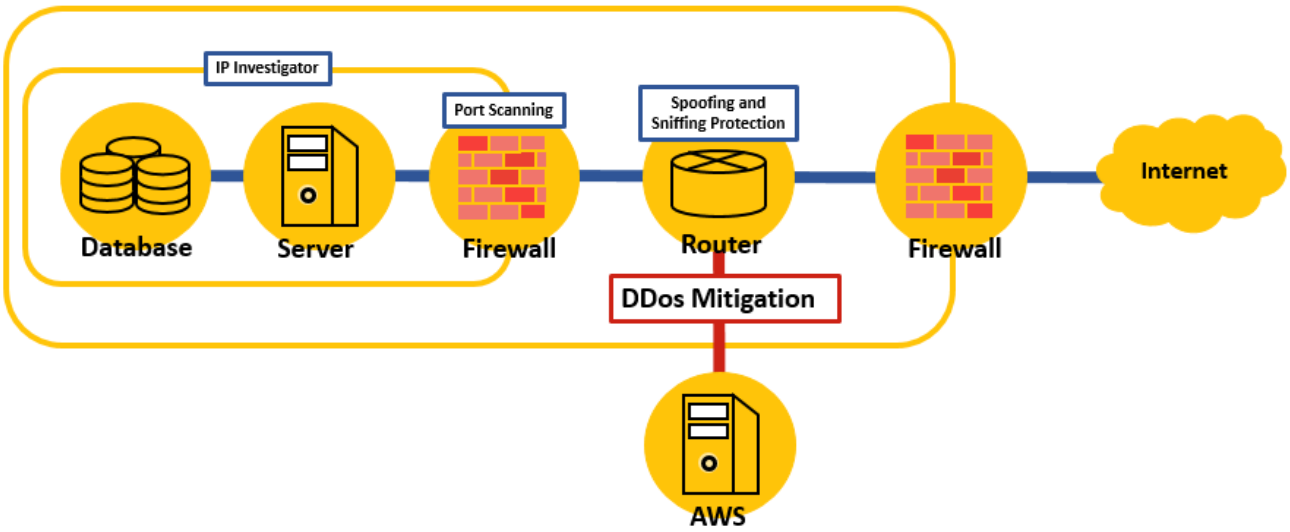
Introduction

การทำธุรกรรมทางการเงินในสมัยก่อนเป็นเรื่องที่ต้องใช้เวลา และมีข้อจำกัด กล่าวคือ ในการโอนเงินหรือชำระเงิน จำเป็นต้องไปทำที่ธนาคารหรือตู้เอทีเอ็ม โดยในบางพื้นที่ที่อยู่ห่างไกลจากธนาคารหรือตู้เอทีเอ็ม ผู้ใช้งานจะไม่ได้รับความสะดวก จึงทำให้ผู้ใช้งานในพื้นที่นั้นลำบากในการทำธุรกรรมทางการเงิน ในปัจจุบันการทำธุรกรรมทางการเงินเป็นสิ่งที่จำเป็นไม่ว่าจะในการทำธุรกิจหรือในชีวิตประจำวัน ถ้ายังสามารถทำธุรกรรมทางการเงินได้เฉพาะที่ธนาคารหรือตู้เอทีเอ็ม จะทำให้เสียโอกาสในการทำธุรกิจ และเสียเวลาในการเดินทางไปที่ธนาคารหรือตู้เอทีเอ็ม ซึ่งส่งผลเสียให้ทั้งผู้ใช้งาน และธนาคาร โดยทางธนาคารอาจเสียกลุ่มลูกค้าที่ไม่ได้รับความสะดวก ส่งผลให้ธนาคารจำนวนไม่น้อยจำเป็นต้องปรับตัวให้ผู้ใช้งานสามารถทำธุรกรรมทางการเงินได้อย่างสะดวก

เราจึงจำลองการพัฒนาระบบการทำธุรกรรมทางการเงินผ่านทางสมาร์ทโฟนซึ่งเป็นเทคโนโลยีได้รับความนิยมเป็นอย่างมากในปัจจุบัน รวมถึงได้นำเทคโนโลยีคิวอาร์โค้ดมาประยุกต์ใช้ร่วมกัน ทำให้ผู้ใช้งานได้รับความสะดวก ความรวดเร็ว และความปลอดภัยมากขึ้น โดย QR Code (Quick Response Code) คือ รหัสชนิดหนึ่งที่ถูกพัฒนามาจากบาร์โค้ดแต่ใช้งานง่ายกว่า และเก็บข้อมูลได้มากกว่า จึงถูกนำมาประยุกต์ในการใช้จ่ายสินค้า และบริการตามร้านค้า รวมถึงการโอนเงินในการทำธุรกรรมทางการเงินอีกด้วย ซึ่งในคิวอาร์โค้ดจะมีข้อมูลที่จำเป็นสำหรับการบริการต่างๆ โดยในที่นี้เราใช้เลขบัญชีของผู้รับเงิน

ทางคณะผู้จัดทำจึงสนใจที่จะจำลองการใช้ Network Security ขึ้นบนแอพพลิเคชัน โดยได้ทำการสร้าง Prompt Oan แอพพลิเคชันซึ่งเป็นเว็บแอพพลิเคชันบนสมาร์ทโฟนที่ให้ผู้ใช้งานที่เป็นสมาชิกของแอพพลิเคชันสามารถโอนเงินหากันได้ผ่านคิวอาร์โค้ด โดยคิวอาร์โค้ดจะถูกสร้างขึ้นใหม่ทุกครั้งในการโอน ซึ่งระบบของแอพพลิเคชันจะใช้บริการของ Heroku Cloud Platform as a Service ที่ให้บริการในเรื่องทรัพยากรและการตั้งค่าเซิร์ฟเวอร์ ซึ่งผู้ใช้บริการไม่จำเป็นต้องเสียเวลาในการตั้งค่าเซิร์ฟเวอร์ นอกจากนี้ยังมีบริการ Network Security อันได้แก่ Firewall, DDoS Mitigation, Spoofing and Sniffing Protections และ Port Scanning อีกทั้งเราได้ทำการเลือกใช้ IP Investigator ที่เป็นบริการเสริมของ heroku ซึ่งจะช่วยให้ผู้ใช้งานสามารถใช้งานได้อย่างปลอดภัยมากขึ้น

Network Security

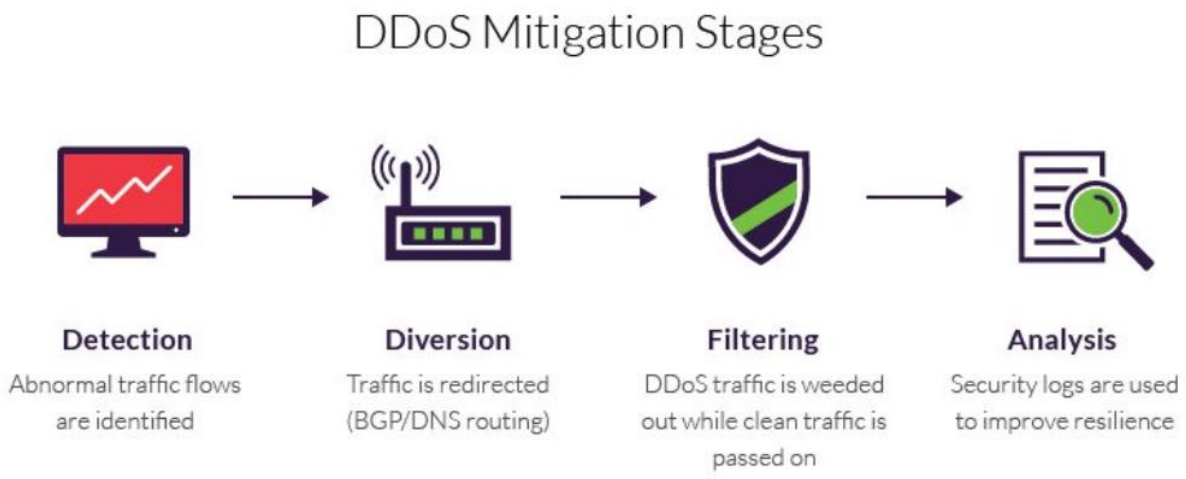


ภาพที่ 1 Network Diagram

Firewall

Firewall คือ ซอฟท์แวร์หรือฮาร์ดแวร์ในระบบเครือข่าย หน้าที่ของไฟร์วอลล์คือเป็นตัวกรองข้อมูลสื่อสารจะคอยตรวจสอบข้อมูลต่างๆ ระหว่างเครือข่าย หรือระหว่างเครื่องคอมพิวเตอร์ต่างๆ ซึ่งเพื่อคอยป้องกันการโจมตี สแปม และผู้บุกรุก ต่างๆ ที่ไม่หวังดีต่อระบบ เปรียบเสมือนยามเฝ้าประตูที่คอยตรวจสอบผู้เข้าออกต่างๆ ในสถานที่นั้นๆ ซึ่งทางคณะผู้จัดทำได้ใช้บริการ Firewall จาก Heroku ที่เป็นประเภท Host-based Firewall เป็นซอฟท์แวร์ที่สามาถติดตั้งได้ทั้งบนเครื่องคอมพิวเตอร์ส่วนตัว และเครื่องเซิร์ฟเวอร์ โดยของเราติดตั้งไว้ที่เครื่องเซิร์ฟเวอร์ ทำให้สามารถจำกัดการเชื่อมต่อขาเข้า และขาออกได้ตามความจำเป็น นอกจากนี้ข้อดีของ Firewall ประเภทนี้คือสามารถบล็อคการเชื่อมต่อของโปรแกรมและพอร์ตต่างๆ ได้ด้วยการกำหนดของผู้ใช้เอง รวมทั้งป้องกันการโจมตีที่เกิดขึ้นจากภายในเครือข่ายเดียวกันได้

DDoS Mitigation



ภาพที่ 2 DDoS Mitigation Stages

DDoS เป็นการโจมตีโดยมีจุดประสงค์เพื่อให้ระบบไม่สามารถทำงานต่อได้ ด้วยการส่ง request ไปให้ server จำนวนมาก เช่น ping of death ซึ่ง DDoS Mitigation เป็นโครงสร้างให้บริการการป้องกันการโจมตี DDoS โดยมีเทคนิคการใช้ TCP Syn cookies ที่ป้องกันการทำ SYN flood attacks (เป็นการโจมตีโดยการส่ง SYN packets ไปจำนวนมาก แล้วไม่ส่ง ACK packets กลับไป เพื่อยืนยัน connection ทำให้ client คนอื่นๆไม่สามารถติดต่อกับเซิร์ฟเวอร์ได้) และ การจำกัดอัตราการเชื่อมต่อของระบบ เพื่อไม่ให้เกินขนาดของ bandwidth ของผู้ใช้บริการที่จะสามารถรองรับได้โดย heroku จะตอบสนองอย่างรวดเร็วกับการโจมตีที่เกิดขึ้น

DDos Mitigation มีขั้นตอนเริ่มด้วยการตรวจสอบ และระบุ Traffic ที่ไม่ปกติ จากนั้นจะทำการส่งการติดต่อไปทางอื่นแล้วทำการกรองเพื่อลดการใช้ Bandwidth บนTraffic นั้นลง สุดท้ายจะนำข้อมูลมาวิเคราะห์ ซึ่งใน Heroku และยังสามารถเปิดการใช้บริการแบบขั้นสูงได้อีกด้วย เรามีการป้องกันและคอยตรวจสอบอยู่ตรงที่ router ซึ่งจะมี DDoS Scrubbing Center คอยรองรับ Traffic ต่างๆ และลด Traffic ที่มาจากการ spam หรือ bot ต่างๆ

Spoofing and Sniffing Protections

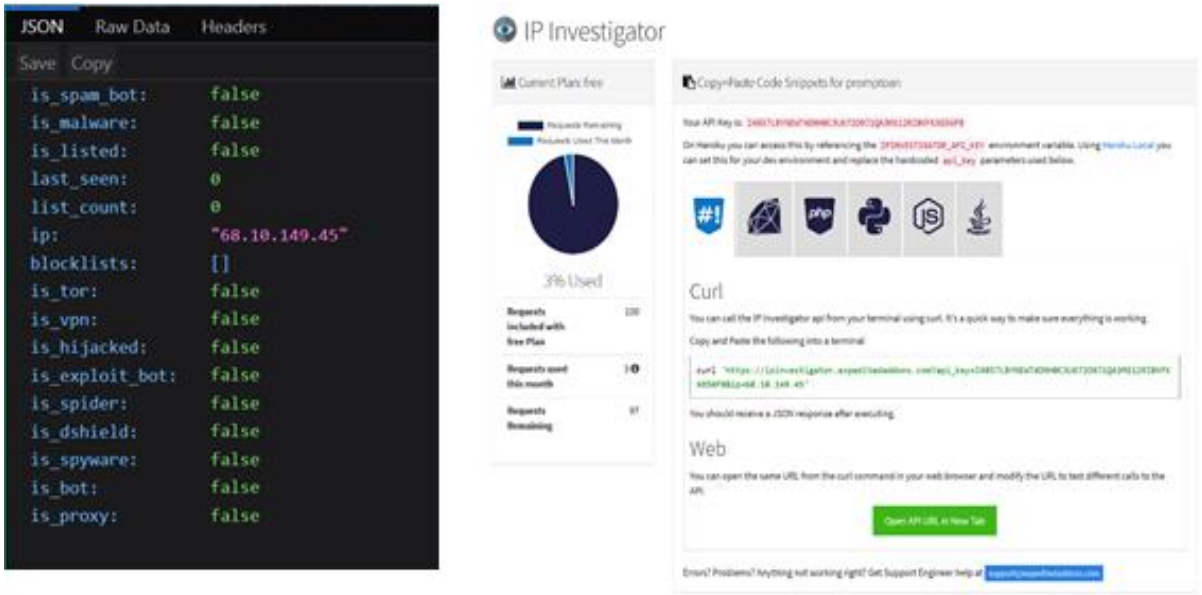
Spoofing Protection คือ การป้องกันการโจมตีโดยการปลอมแปลงข้อมูลของ packet ต้นทาง ให้เป็นข้อมูลต้นทางที่มาจากทางอื่น โดยมีเป้าหมายในการป้องกันขโมยข้อมูล การลงมัลแวร์ และการ bypass access control รวมถึงป้องกันการโจมตีอื่นๆที่ Spoofing Attack อำนวยให้การโจมตีนั้นๆ ง่ายขึ้น เช่น DOS session hijacking และ man-in-the-middle attacks เป็นต้น โดยทาง heroku ให้บริการ Spoofing Protection สามแบบ อย่างที่หนึ่งคือ IP Spoofing เป็นวิธีการปลอมแปลง ip address ของ packet ต้นทาง เพื่อให้ระบบของเป้าหมายเกิด Denial-of-Service อย่างที่สอง MAC Spoofing เป็นวิธีการปลอมแปลง MAC Address ของ network interface บนอุปกรณ์ต่างๆ โดยปกติแล้ว MAC Address ไม่สามารถเปลี่ยนแปลงได้ แต่ยังมีอุปกรณ์ที่อนุญาตให้สามารถแก้ไข MAC Address อีกทั้งยังมีเครื่องมือที่ทำให้ระบบเชื่อว่า Network Interface Controller มี MAC Address นั้นอยู่จริง การโจมตีนี้มีจุดประสงค์เพื่อการ Bypass Access Control Lists บนเซิร์ฟเวอร์หรือ Routers และอย่างสุดท้าย ARP Spoofing เป็นฎิธีการปลอมแปลง MAC Address ของ packet ต้นทาง เป็น MAC Address ของผู้โจมตี ทำให้เซิร์ฟเวอร์ส่งข้อมูลตอบกลับไปที่ผู้โจมตีแทนที่จะส่งให้ผู้รับจริงๆ

ในส่วนของ Sniffing Protection คือ การป้องกันการดักจับ packet ที่วิ่งอยู่บนระบบ เพื่อไม่ให้ผู้โจมตีได้รับข้อมูลที่อาจเป็นประโยชน์ในการโจมตีมากขึ้น โดย heroku จะมีโครงสร้างที่ประกอบด้วย hypervisor ซึ่งจะไม่ส่งข้อมูลไปให้ interface ที่ไม่ได้กำหนด ซึ่ง heroku มีได้จัดการ Spoofing and Sniffing Protections ผ่านทางการตั้งค่า firewall และไว้ที่ router เพื่อตรวจสอบ packet ที่วิ่งเข้ามา

Port Scanning

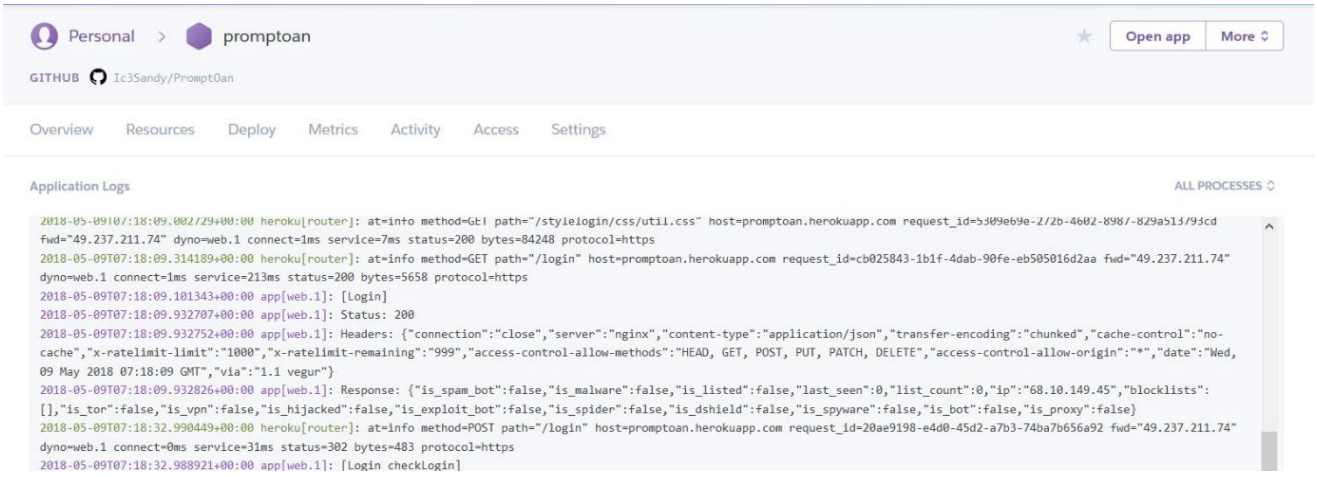
Port Scanning เป็นกระบวนการติดต่อไปที่พอร์ตของเครื่องเป้าหมายเพื่อตรวจสอบว่ามีบริการใดบ้างบนระบบที่รอรับการเชื่อมต่อ หรืออยู่ในสถานะที่ให้บริการได้ และยังสามารถค้นหาประเภทของระบบปฏิบัติการที่อยู่บนเครื่องเป้าหมาย โดยทำการส่งข้อความไปที่เป้าหมายเพื่อรอดูข้อความตอบกลับว่ามีลักษณะเป็นอย่างไร ซึ่งข้อความนั้นจะบอกข้อมูลบางอย่างให้แก่ผู้โจมตีซึ่งสามารถนำไปใช้ในการโจมตีระบบส่วนอื่นๆ ต่อไป Port Scanning จัดว่าเป็นแผนการขั้นต้นของผู้ร้ายในการที่จะโจมตีไปยังเป้าหมายซึ่ง Heroku จะไม่อนุญาติการทำ Port Scanning และจะมีการรายงานไปให้ผู้ให้บริการตรวจสอบ โดยการตรวจสอบว่ามีการใช้ Port Scanning หรือไม่ จะอยู่บน firewall ก่อนถึงเซิร์ฟเวอร์ และฐานข้อมูล เมื่อระบบพบว่ามีการทำ Port Scanning เกิดขึ้น การเข้าถึงนั้นจะถูกหยุดและถูกบล็อก

IP Investigator



ภาพที่ 3 ซ้าย : หน้าต่าง Request , ขวา : หน้า Controller

เราได้ทำการเปิดใช้บริการนี้ของ heroku โดยใช้ IP Investigator ซึ่งสามารถทำการตรวจสอบว่าเป็น spam-bots, malware, hijacked, spider, spyware และ spam ต่างๆ ก่อนที่จะทำการบล็อค รวมถึงการตรวจสอบการเข้าถึงโดยใช้ VPN และ proxy โดยการตรวจสอบจะอยู่บน firewall ก่อนถึงเซิร์ฟเวอร์ และฐานข้อมูล ซึ่งเรามี DShield IDS Data ไว้สำหรับรายงานผลจาก ip address บันทึกใน log file ที่จะแสดงผลอยู่ตลอดเวลา แต่ในการใช้บริการนี้ทางเราใช้เป็นแบบฟรีต่อเดือน ซึ่งจะจำกัดการตรวจสอบได้ 100 requests ต่อเดือนเท่านั้น



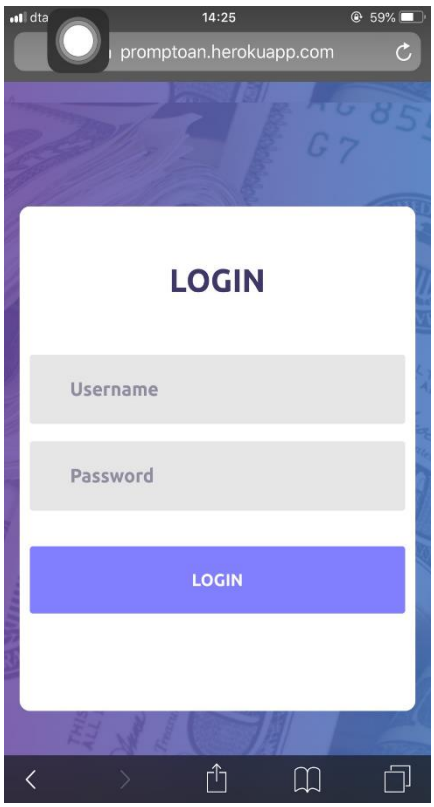
ภาพที่ 4 ตัวอย่าง log

VPN

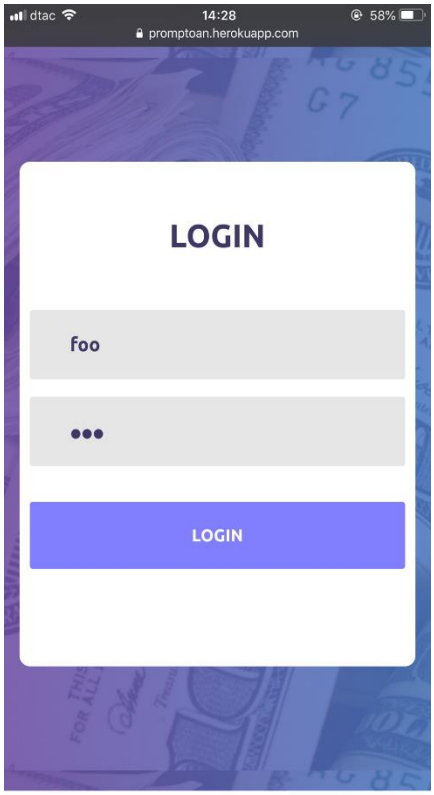
VPN (Virtual Private Network) คือ ฟังก์ชันที่อยู่ในระบบเครือข่าย ที่มีไว้เพื่อทำให้การรับส่งข้อมูลได้ปลอดภัยมากขึ้นโดยการเข้ารหัสข้อมูลก่อนส่งทุกครั้ง และเชื่อมต่อกับอุปกรณ์ใน VPN เดียวกันได้สะดวกขึ้น รวมถึงการเปลี่ยนภูมิภาคการใช้อินเตอร์เน็ตโดยการเชื่อมต่อกับ VPN Server ของภูมิภาคนั้นๆ จะช่วยให้ลดการแฝงตัวของผู้แอบสุ่มโจมตี และมีระบบ Trusted IP โดยจะจำกัดช่วงของ IP ที่สามารถเชื่อมต่อเซิร์ฟเวอร์ได้ตามความต้องการ โดย feature เหล่านี้จะอยู่ในระบบของ Heroku Private Spaces เป็นของ Enterprise ซึ่งถ้าจะเปิดการใช้งานต้องเสียค่าใช้จ่ายรายเดือน

Example

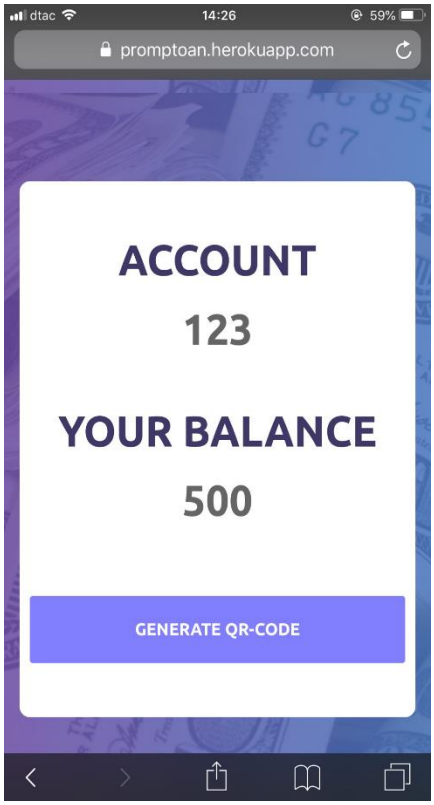
1.หน้า Main



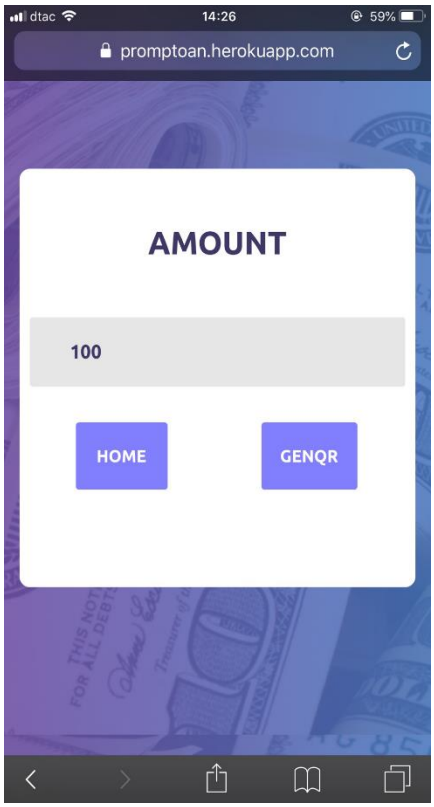
2. หน้าล็อคอิน



3. ล็อคอินเป็นผู้ใช้งานชื่อ foo
โดยในที่นี้จะเป็นผู้รับเงิน

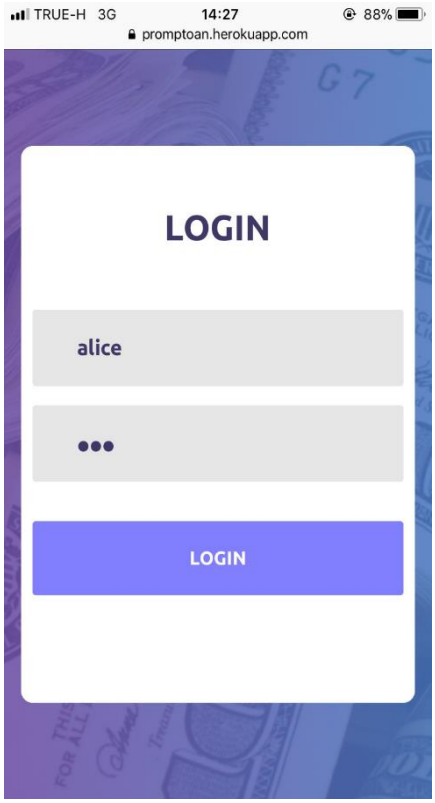


4. เมื่อล็อคอินแล้วจะแสดง
เลขที่บัญชี และยอดเงินคงเหลือ

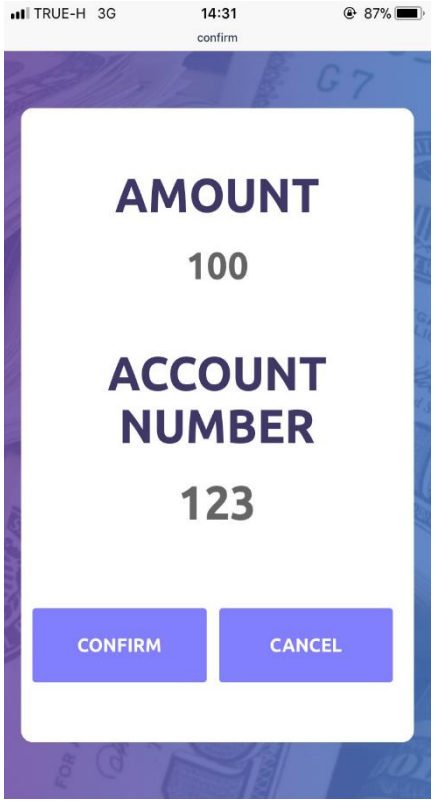


5. กด Generate QR-Code และ
กรอกจำนวนเงินที่ต้องการจะรับเงิน

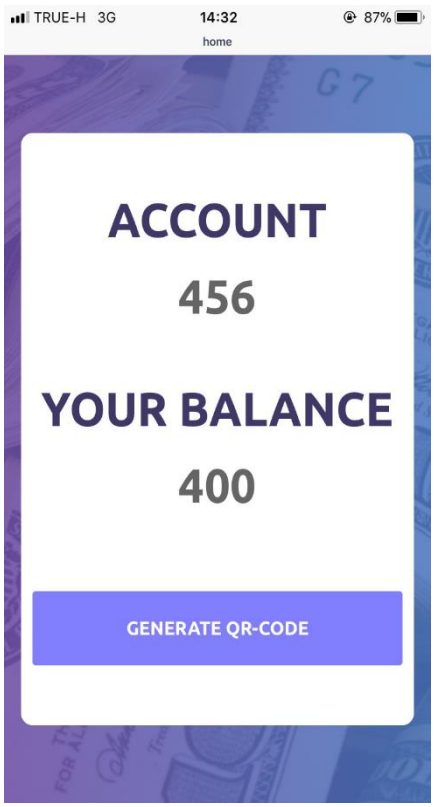
6. ได้รับคิวอาร์โค้ด
มาให้ผู้จ่ายเงินสแกน



7. เมื่อสแกนคิวอาร์โค้ด จะต้องล็อคอินก่อน โดยในที่นี้เป็น alice ซึ่งเป็นผู้โอนเงิน

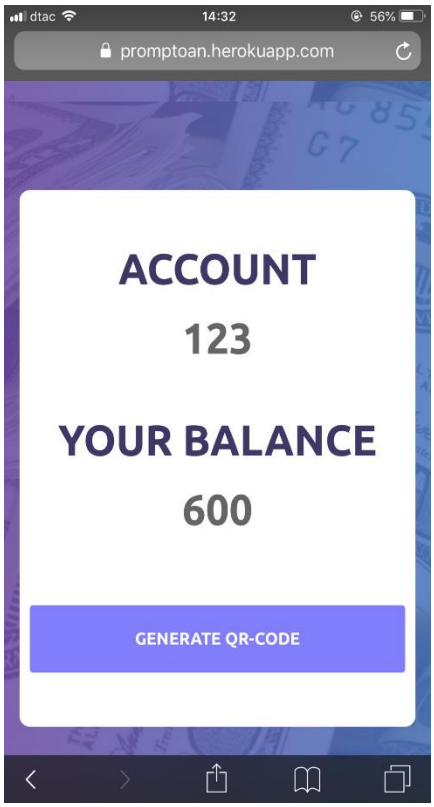


8. เมื่อล็อคอินแล้วจะแสดงหน้าคอนเฟิร์มเพื่อยืนยันการโอนเงิน



9. ระบบหักเงิน alice ไปให้ foo

alice เหลือเงิน 400



10. foo ได้รับเงิน 100 จาก alice

Conclusion

เราสร้างแอพพลิเคชันที่ผู้ใช้งานสามารถโอนเงินผ่านสมาร์ทโฟนโดยใช้การสแกนคิวอาร์โค้ดแทนการใช้เลขบัญชีจากผู้รับ ซึ่งได้ใช้บริการบน heroku ที่ให้บริการในเรื่องทรัพยากร และการตั้งค่าเซิร์ฟเวอร์ รวมถึงให้บริการด้านความปลอดภัยบนระบบเครือข่าย โดยมีในเรื่องของ Firewall ที่คอยป้องกันการเข้าถึงระบบจากเครือข่ายภายนอก และระหว่างระบบภายใน ในด้านป้องกันการเชื่อมต่อกับ เซิร์ฟเวอร์ รวมถึงการถูกโจมตีด้วย DDoS ที่จะส่ง request จำนวนมากเพื่อให้เซิร์ฟเวอร์ไม่สามารถใช้งานได้ สามารถป้องกันโดยใช้ DDos Mitigation ที่เมื่อเกิดการโจมตีจะทำการส่ง Traffic ไปที่อื่นแทน เช่น AWS เป็นต้น ส่วนของ Spoofing and Sniffing Protections ที่มีการป้องกันการปลอมแปลงของ packet ต้นทาง และการป้องกันการดักจับ packet ระหว่างทางเพื่อไม่ให้ผู้ร้ายได้รับข้อมูลที่อาจช่วยในการโจมตีอื่นๆ อีกได้ นอกจากนี้ยังมีการป้องกัน Port Scanning จะไม่ให้ผู้ร้ายได้รับข้อมูลเกี่ยวกับระบบเพื่อจะนำมาใช้โจมตีในส่วนอื่นต่อไป และมีการใช้บริการเสริมของทาง Heroku ที่เรียกว่า IP Investigator ซึ่งจะสามารถตรวจสอบ log ได้ว่ามีการแอบแฝงมาหรือไม่ สุดท้ายการใช้ VPN ของ heroku นั้นเป็นการให้บริการของ Heroku Private Spaces ที่เป็นของ Enterprise ที่จะสามารถเลือกที่จะรันแอพพลิเคชันได้บนเซิร์ฟเวอร์ต่างๆ ของ Heroku Private Spaces

ปัจจุบันแอพพลิเคชันของเรายังมีช่องโหว่อยู่ในหลายๆ ด้านจึงทำให้แอพพลิเคชันยังมีความปลอดภัยได้ไม่ดีเท่าที่ควร กล่าวคือ ไม่มีการใช้การยืนยันตัวตนด้วยอุปกรณ์ภายนอก เช่น ยืนยันผ่านรหัส OTP หรือการยืนยันผ่านอีเมล เป็นต้น ซึ่งในส่วนนี้สามารถทำเพิ่มเติมได้ในอนาคต