



# SQLGAME

## หลักการและเหตุผล

ปัจจุบัน SQL Injection ยังคงเป็นภัยคุกคามอันดับต้นๆ ที่สร้างความเสียหายรุนแรงต่อฐานข้อมูลและชื่อเสียงขององค์กรทั่วโลก อย่างไรก็ตาม การเรียนรู้เพียงทฤษฎีนั้นไม่เพียงพอต่อการเข้าใจกลไกการโจมตี ส่วนการฝึกฝนในระบบจริงก็มีข้อจำกัดด้านจริยธรรมและความเสี่ยง

คณะผู้จัดทำจึงพัฒนา สื่อการเรียนรู้ในรูปแบบเกม ที่จำลองสถานการณ์การโจมตี SQL Injection ในสภาพแวดล้อมที่ปลอดภัย เพื่อให้ผู้เรียนได้ลงมือปฏิบัติจริงผ่านบทบาทผู้โจมตี ซึ่งจะช่วยกระตุ้นความสนใจและสร้างความจดจำด้านการหาช่องโหว่รวมถึงแนวทางการป้องกันได้อย่างมีประสิทธิภาพ

## ขอบเขตการศึกษา

- ศึกษาแนวคิดพื้นฐานด้านความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์ (Network Security Fundamentals)
- มุ่งเน้นการจำลองสถานการณ์การโจมตีประเภท SQL Injection
- สร้างความตระหนักรู้ในเรื่องการตรวจสอบข้อมูลนำเข้า (Input Validation) และการใช้ Parameterized Queries เพื่อการป้องกัน
- แสดงเนื้อหาความรู้เบื้องต้นพร้อมโค้ดตัวอย่างประกอบการเรียนรู้

## ฟังก์ชัน

- ฟังก์ชันผู้ใช้ทั่วไป
  - ระบบปลดล็อกด่าน ต้องผ่านด่านก่อนหน้าเพื่อเล่นด่านถัดไป
  - บทเรียนและโค้ดตัวอย่างก่อนเริ่มเล่นจริง
  - ตารางคะแนน แสดงรายชื่อผู้เล่นที่มีคะแนนสูงสุด 10 อันดับแรก
  - ระดับความสามารถและผลการเรียนรู้จากความเร็วที่ใช้
  - สรุปบทเรียนและเทคนิคการเขียนโค้ดที่ปลอดภัยหลังจบด่าน
  - ระบบตัวช่วยผ่านด่านที่จะเปิดให้ใช้งานเมื่อรอจนครบเวลาที่กำหนด
- ฟังก์ชันผู้ใช้ทั่วไป
  - การเพิ่ม ลบ แก้ไขด่านภายในเกม
  - การเพิ่ม ลบ แก้ไขข้อมูล ให้ยศแอดมิน รีเซตคะแนนและแบนผู้เล่น
  - การดูข้อมูลใน Database ผ่านหน้าเว็บไซต์
  - การเข้าถึงฟังก์ชันต่างๆของผู้ใช้งานทั่วไป

## เครื่องมือ:



## สรุปผลดำเนินการ:

สามารถสร้างเว็บเกมที่สามารถฝึกให้ผู้เรียนได้เรียนรู้เกี่ยวกับ SQL Injection ได้

## อ้างอิง:

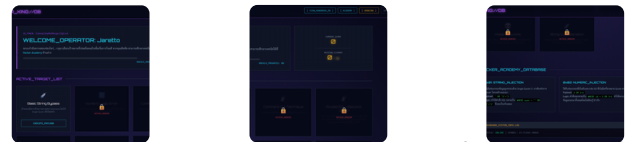
<https://phishingquiz.withgoogle.com>  
Mozamel M Saeed, Designing Scenarios for In-Organization Training Using the CyberCIEGE Game (2022)

## วัตถุประสงค์

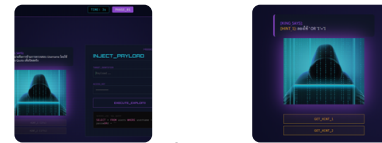
1. เพื่อพัฒนาเกมด้าน Cybersecurity ในรูปแบบมิมีเกมที่เล่นคนเดียวและสามารถเล่นซ้ำได้
2. เพื่อสร้างแพลตฟอร์มการเรียนรู้ที่ปลอดภัยสำหรับการฝึกฝนทักษะการทำ SQL Injection
3. เพื่อสร้างความตระหนักรู้เกี่ยวกับความสำคัญของการตรวจสอบข้อมูลนำเข้า (Input Validation) และการใช้ Parameterized Queries
4. เพื่อประยุกต์ใช้ความรู้จากบทเรียนวิชา Security มาสร้างเครื่องมือที่ช่วยส่งเสริมการเรียนรู้ให้แก่ผู้อื่น
5. เพื่อใช้เป็นต้นแบบ (Prototype) สำหรับการพัฒนาเครื่องมือฝึกอบรมหรือสื่อการเรียนรู้ด้าน Cybersecurity ในอนาคต

## วิธีใช้งาน

- หน้าหลักแสดงด่านที่สามารถเล่นได้ ความคืบหน้า คะแนนรวม และเนื้อหาการเรียนรู้



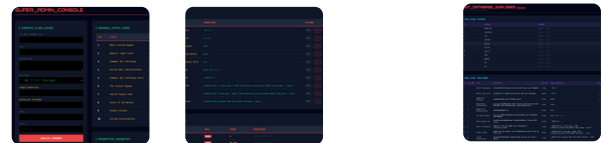
- เมื่อกดเล่นเกม จะมีโจทก์ และมีช่องให้กรอกเพื่อตอบคำถาม ซึ่งมีจับเวลา หากเวลาถึงกำหนดจะสามารถเปิดคำใบ้ได้



- หน้า Handbook จะรวมคำศัพท์ที่เกี่ยวข้องกับ SQL Injection
- หน้า Leaderboard จะแสดงคะแนนผู้เล่น 10 อันดับแรก



- หน้าเพิ่ม ลบ แก้ไขโจทก์
- หน้าดูข้อมูลใน Database



## สมาชิก

- 673380019-3 ภูมิภัทร ริพิมพ์
- 673380022-4 นางสาวสิริธดา หงษ์แสงไทย
- 673380208-0 นายจิรภัทร พวงงษา
- 673380217-9 นายณัฐวิชัย วารินทร์รณากานต์
- 673380499-3 นายจิรายุ ร่มลำดวน
- 673380506-2 นายสรวิศ สลิดชัย
- 643021374-2 นายเจษฎา กำpha