CLICKJACKING

ศ.ดร.จักรชัย โสอินทร์

SC362006 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

หลักการและเหตุผล

เนื่องจากClickjackingเป็นหนึ่งในเทคนิคการโจมตีทางไซเบอร์ที่แฮกเกอร์ใช้หลอกให้ผู้ใช้คลิกบนองค์ประกอบที่ซ่อนอยู่ในเว็บไซต์โดยที่เหยื่อไม่รู้ตัวทำให้สามารถขโมยข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือสั่งให้เกิดพฤติกรรมที่เป็นอันตรายต่อบัญชีของผู้ใช้ได้

ขอบเขต

การจัดทำโครงงานนี้เน้นการทำความเข้าใจเกี่ยวกับกลไกของ Clickjacking รวมถึงวิธีการป้องกันผ่านเว็บไซต์

วิธีการใช้งาน

1. แฮกเกอร์ฝังเว็บไซต์เป้าหมายไว้ใน iframe บนเว็บไซต์
2. ใช้ CSS ทำให้ iframe โปร่งใส หรือซ้อนทับปุ่มบนหน้าเว็บของแฮกเกอร์
3. เมื่อเหยื่อคลิกปุ่มหรือองค์ประกอบที่ถูกซ่อนแท้จริงแล้วเป็นการกดปุ่มที่แฮกเกอร์ต้องการ

ความสามารถ

เป็นการฝัง iframe สำหรับ redirect ไปยังหาเว็บไซต์เป้าหมายที่ได้ทำการฝัง Trojan Horse ไว้และเมื่อผู้ใช้ทำการกรอกแบบฟอร์มก็จะทำการเก็บข้อมูลไปยัง database

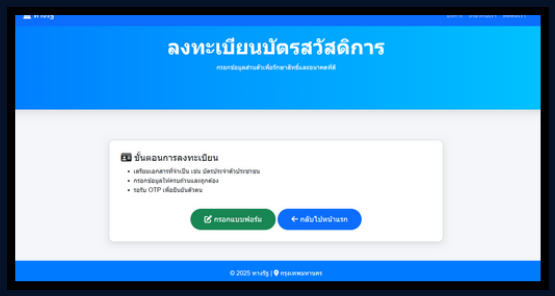
วัตถุประสงค์

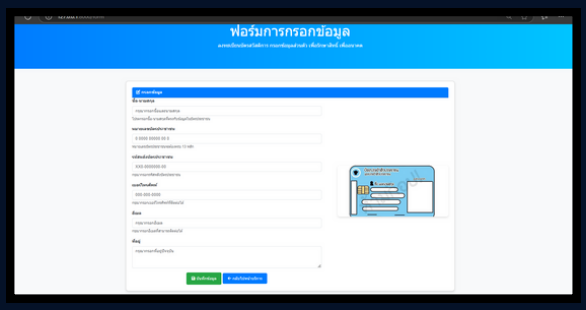
1. ศึกษารูปแบบและกลไกของ Clickjacking
2. ทดสอบการโจมตี Clickjacking ผ่านการสร้างตัวอย่างเว็บไซต์
3. แนะนำแนวทางป้องกัน เช่น ตรวจจับการฝัง iframe ผ่าน JavaScript

สมาชิก GROUP4 SEC.2

1. นายชุติพนธ์ หล้าอามาตย์ 663380485-3
2.นายพงศกร สระแก้ว 663380004-5
3.นายธนดล สาเสน 663380487-9
4นางสาวกุลศยา จันภูงา 663380145-7
5.นายกิตติธัช ปลั่งกลาง 663380144-9
6.ธรณ์ธันย์ นามแสง 663380163-5

ฝัง IFRAM ที่เว็บทางรัฐ





ข้อสรุป

คณะผู้จัดทำได้ทำการสร้างเว็บไซต์จำลองที่ชื่อว่าทางรัฐ และได้นำ iframe ไปฝังไว้ที่ปุ่มกรอกแบบ โดยให้ route ไปแสดงหน้ากรอกแบบฟอร์มทับหน้าแบบฟอร์มของเว็บไซต์จริง และเมื่อผู้ใช้ทำการกรอกแบบฟอร์มจนครบ จะดาวน์โหลดไฟล์ที่ชื่อว่า ทางรัฐ.exe ทันทีและข้อมูลที่กรอกไปจะเข้าไปสู่ฐานข้อมูลที่จัดตั้งไว้เพื่อดักเอาข้อมูล ดังนั้นเหยื่อจะถูก phishing ข้อมูลและโดนโจมตีโดย trojran horse

อ้างอิง

https://owasp.org/www-project-web-security-testing-guide