# บทที่ 5
# สรุป และอภิปรายผล

จากการทดลอง test การโจมตี ทั้ง 3 วิธีคือ BetterCap script เดิม BetterCap เปลี่ยน Script และ SSL Strip เมื่อวันที่ 7 มิถุนายน 2564 พบว่าการป้องกันเว็บไซต์ที่ไม่สมบูรณ์ไม่อาจการป้องกันการโจมตีอย่างง่ายได้ การโจมตีเว็บไซต์ Hacker มักจะหาวิธีโจมตีในรูปแบบใหม่อยู่เสมอเพื่อให้การโจมตีสำเร็จดังตารางที่ 5.1 ผลการทดสอบด้วย BetterCap ดังตารางที่ 5.1 ตารางที่ 5.2 และตารางที่ 5.3

การป้องกันเว็บไซต์ทั้งหมด 5 รูปแบบ คือ

1) ไม่มี HSTS Header
2) Header Preload และ Preload on Database
3) Header Preload แต่ไม่ได้ Preload on Database
4) Header ไม่ได้ Preload แต่ Preload on Database
5) Header ไม่ได้ Preload และไม่ได้ Preload on Database

**ตารางที่ 5.1** ผลการทดสอบด้วย BetterCap

| เว็บที่ใช้ทดสอบ | จำนวนเว็บไซต์ที่ทดสอบ | Strip | | Sniff | |
|---|---|---|---|---|---|
| | | ได้ | ไม่ได้ | ได้ | ไม่ได้ |
| เว็บไซต์มหาลัย | 7 | 6 | 1 | 5 | 2 |
| เว็บไซต์ธนาคาร | 5 | 2 | 3 | - | 5 |
| เว็บไซต์หน่วยงานรัฐ | 4 | 2 | 2 | 2 | 2 |
| เว็บไซต์ทั่วไป | 2 | - | 2 | - | 2 |

ผลการทดลสอบการใช้ BetterCap script เดิมที่ให้มากับการใช้ Tools BetterCap มีโอกาสในการโจมตีสำเร็จได้น้อย แม้บางเว็บไซต์ที่ไม่ได้ป้องกันเว็บมากเท่าไหร่นักก็ไม่อาจโจมตีได้สำเร็จ เว็บไซต์ที่ไม่ได้ set Preload บน Header และ load บน database มีโอกาสโจมตีสำเร็จได้อย่างง่ายดาย

**ตารางที่ 5.2** ผลการทดสอบด้วย BetterCap เปลี่ยน Script

| เว็บที่ใช้ทดสอบ | จำนวนเว็บไซต์ที่ทดสอบ | Strip | | Sniff | |
|---|---|---|---|---|---|
| | | ได้ | ไม่ได้ | ได้ | ไม่ได้ |
| เว็บไซต์มหาลัย | 7 | 5 | 2 | 5 | 2 |
| เว็บไซต์ธนาคาร | 5 | 4 | 1 | - | 5 |
| เว็บไซต์หน่วยงานรัฐ | 4 | 2 | 2 | 2 | 2 |
| เว็บไซต์ทั่วไป | 2 | 1 | 1 | - | 2 |

ผลการทดลองใช้ BetterCap เปลี่ยน Script ในการปลด HSTS มีโอกาสสำเร็จมากกว่าใช้ BetterCap แบบเดิม เมื่อเว็บไซต์มีการป้องกันโดยการ set Preload ไว้ใน Header การโจมตีด้วย BetterCap ไม่อาจสำเร็จได้โดยง่าย

**ตารางที่ 5.3** ผลการทดสอบด้วย SSL Stripping Attack

| เว็บที่ใช้ทดสอบ | จำนวนเว็บไซต์ที่ทดสอบ | Strip | | Sniff | |
|---|---|---|---|---|---|
| | | ได้ | ไม่ได้ | ได้ | ไม่ได้ |
| เว็บไซต์มหาลัย | 7 | 7 | - | 7 | - |
| เว็บไซต์ธนาคาร | 5 | 3 | 2 | 3 | 2 |
| เว็บไซต์หน่วยงานรัฐ | 4 | 3 | 1 | 3 | 1 |
| เว็บไซต์ทั่วไป | 2 | - | 2 | - | 2 |

ผลการทดลองเว็บไซต์ที่ไม่ได้ set Preload ไว้บน Database สามารถใช้เทคนิค SSL Strip Attack โจมตีได้สำเร็จเป็นส่วนมาก เว็บไซต์ที่ set Preload on database ไม่สามารถโจมตีได้เลย

5.1.1 จากผลการวิเคราะห์ปัญหา SSL Stripping Attack

HTTP Strict Transport Security เป็นการเพิ่มประสิทธิภาพในการรักษาความปลอดภัย เป็นการทำงานเหมือนกับ HTTP แต่ทำงานอยู่บน SSL เพื่อให้เกิดความปลอดภัยในการส่งข้อมูลมากขึ้นมีรูปแบบดังนี้

1) การใช้งาน URL จะขึ้นต้นด้วย HTTPS://

2) ทำงานที่ port 443

3) ส่งข้อมูลแบบ Cipher text มีการเข้ารหัสข้อมูลระหว่างการส่ง ถึงจะสามารถถูกดักจับได้ แต่จะอ่านข้อมูlไม่รู้เรื่อง

4) มีการทำ Authentication เพื่อตรวจสอบยืนยันข้อมูล

การโจมตีด้วยเทคนิค SSL Striping Attack จะเป็นการโจมตีไปที่ HTTPS โปรโตคอลการสื่อสารอินเทอร์เน็ต โดยการถอด HTTPS เป็น HTTP ทำให้มีการส่งข้อมูลแบบ Clear text ไม่ได้ทำการเข้ารหัส ทำให้สามารถถูกดักจับได้ง่ายการสื่อสารขง HTTP มีรูปแบบดังนี้

1) เป็นโปรโตคอลหลักที่ใช้ในการแลกเปลี่ยนข้อมูล (HTML) ระหว่าง web server และ web Client (Browser)

2) ใช้ URL ในการเข้าถึงเว็บไซต์ ด้วย http://

3) ทำงานที่ port 80

4) ส่งข้อมูลแบบ Clear text คือไม่มีมการเข้ารหัสข้อมูลระหว่างการส่ง จึงสามารถถูกดักจับและอ่านข้อมูลได้

5.1.2 การวิเคราะห์ปัญหา Downgraded Attack

ปัญหา Downgraded Attack คือ TLS Protocol Version ของปัจจุบันถูก Downgraded ให้ใช้ TLS/SSL Protocol Version เก่านั่นเอง Downgraded Attack แบ่งออกเป็น 3 การโจมตีหลัก ๆ ได้แก่ down Attack, beast Attack และ poodle Attack

การทำงานของ Downgraded Attack เมื่อ Client request ไปยัง server ด้วย TLS Protocol ใด ๆ ที่มากกว่า TLS Version 1.0 จะถูก Hacker โจมตีด้วยการ Downgraded TLS Protocol ลงมาใช้เวอร์ชันที่เก่ากว่า หาก server มการ config อนุญาตให้สามารถทำงานด้วย TLS Protocol Version 1.0 หรือต่ำกว่า Downgraded Attack จึงถือว่าทำงานอย่างสมบูรณ์

ในการป้องกันการโจมตีสามารถป้องกันได้อย่างไร สำหรับแนวทางการป้องกันการโจมตีด้วยเทคนิค Downgraded Attack ทำได้โดยการตรวจสอบ Version ของ SSL/TLS Protocol ด้วยคำสั่ง openssl Version และเปิดใช้งาน TLS 1.2 และ TLS 1.3 สำหรับ Apache

**5.1 ปัญหา และอุปสรรคในการดำเนินงาน**

1) การทดลองไม่ได้ผลสำเร็จทุกเมื่อ หากเว็บไซต์มีการ update ระหว่างการจัดทำโครงการ

2) ในช่วงแรกของการทำรูปเล่มค่อนข้างมีความลำบากในการหาข้อมูล เนื่องจากคนไทยที่เขียนเอกสารที่เกี่ยวข้องมีจำนวนน้อยมาก หรือแทบไม่มีเลย

**5.2 ข้อเสนอแนะ**

ควรติดตามการอัพเกรด Browser และมาตรฐานความมั่นคงอยู่ตลอด