

สารบัญ

หน้า

บทคัดย่อ	ก
กิตติกรรมประกาศ.....	ข
สารบัญ.....	ค
สารบัญตาราง.....	จ
สารบัญภาพประกอบ.....	ฉ
บทที่ 1 บทนำ	1
1.1 หลักการและเหตุผล.....	1
1.2 วัตถุประสงค์ของโครงการ.....	2
1.3 ขอบเขตของโครงการ	2
1.4 ตัวอย่างโปรแกรม	4
1.5 ภาพรวมของโครงการปริญญาานิพนธ์	6
1.6 ประโยชน์ที่คาดว่าจะได้รับ	9
1.7 อุปกรณ์และเครื่องมือที่ใช้ในการดำเนินงาน.....	9
1.8 แผนการดำเนินงาน.....	10
บทที่ 2 ทฤษฎี และงานที่เกี่ยวข้อง.....	11
2.1 งานวิจัยและทฤษฎีที่เกี่ยวข้อง	11
2.2 Software ที่เกี่ยวข้อง.....	18
บทที่ 3 ขั้นตอนการดำเนินงาน	21
3.1 กรอบการดำเนินงาน	21
3.2 การทดสอบการโจมตีด้วยเทคนิค SSL Stripping Attack	22
3.3 ตัวอย่างการโจมตีด้วยเทคนิค SSL Stripping Attack.....	26
3.4 การวิเคราะห์ผลการทดสอบการโจมตีด้วยเทคนิค SSL Stripping Attack	31

สารบัญ (ต่อ)

หน้า

3.5 การสร้างเว็บไซต์ล็อกอินต้นแบบในการป้องกันการโจมตีด้วยเทคนิค SSL Stripping Attack..	33
3.6 วิธีการป้องกันเทคนิคการโจมตี SSL Stripping Attack.....	35
3.7 การทดสอบการป้องกันการโจมตีด้วยเทคนิค SSL Stripping Attack.....	37
3.8 การสรุปผลกลไกการป้องกัน.....	37
3.9 การสร้างโปรแกรมที่ใช้ในการตรวจสอบหาช่องโหว่.....	38
3.10 แนะนำการใช้ HTTP Strict Transport Security (HSTS)	40
บทที่ 4 ผลการดำเนินงาน	43
4.1 ผลการทดสอบการจำลองการโจมตีด้วยเทคนิค SSL Stripping Attack	43
4.2 เียบผลการทดสอบ.....	55
4.3 ผลการตรวจสอบการป้องกันกับเว็บไซต์อื่น ๆ.....	56
4.4 ทดสอบหน้าล็อกอิน Salted – Hash Password.....	57
บทที่ 5 สรุป และอภิปรายผล.....	65
5.1 ปัญหา และอุปสรรคในการดำเนินงาน.....	67
5.2 ข้อเสนอแนะ.....	67
เอกสารอ้างอิง	68
ภาคผนวก.....	69
ภาคผนวก ก คู่มือการติดตั้ง.....	70
ภาคผนวก ข คู่มือการใช้งาน.....	73
ภาคผนวก ค รายงาน.....	76
บทความวิจัย.....	87
โปสเตอร์โครงงาน.....	92
ประวัติย่อผู้จัดทำโครงงาน.....	94

สารบัญตาราง

	หน้า
ตารางที่ 1.1 แผนการดำเนินงาน	10
ตารางที่ 3.1 การปลด HTTPS และดักจับข้อมูลกับ HSTS Header	24
ตารางที่ 3.2 การวิเคราะห์ผล HSTS กับการโจมตีด้วย SSLStripping Attack	33
ตารางที่ 3.3 สรุปผล HSTS Header	33
ตารางที่ 4.1 เว็บไซต์ของมหาวิทยาลัย.....	43
ตารางที่ 4.2 เว็บไซต์ของธนาคาร	44
ตารางที่ 4.3 เว็บไซต์ของหน่วยงานภาครัฐ	45
ตารางที่ 4.4 เว็บไซต์ทั่วไป.....	46
ตารางที่ 4.5 เว็บไซต์ของมหาวิทยาลัย.....	47
ตารางที่ 4.6 เว็บไซต์ของธนาคาร	48
ตารางที่ 4.7 เว็บไซต์ของหน่วยงานภาครัฐ	49
ตารางที่ 4.8 เว็บไซต์ทั่วไป.....	50
ตารางที่ 4.9 เว็บไซต์ของมหาวิทยาลัย.....	51
ตารางที่ 4.10 เว็บไซต์ธนาคาร	53
ตารางที่ 4.11 เว็บไซต์ของหน่วยงานภาครัฐ.....	54
ตารางที่ 4.12 เว็บไซต์ทั่วไป	55
ตารางที่ 5.1 ผลการทดสอบด้วย BetterCap	65
ตารางที่ 5.2 ผลการทดสอบด้วย BetterCap เปลี่ยน Script.....	66
ตารางที่ 5.3 ผลการทดสอบด้วย SSL Stripping Attack	66
ตารางที่ ค-1 เปรียบเทียบการโจมตีเว็บไซต์โดยใช้ BetterCap.....	78
ตารางที่ ค-2 เปรียบเทียบการโจมตีเว็บไซต์โดยใช้ BetterCap เปลี่ยน Script.....	79
ตารางที่ ค-3 เปรียบเทียบการโจมตีเว็บไซต์โดยใช้ Moxie's Script	80
ตารางที่ ค-4 กลไกการป้องกันของเว็บไซต์	84

สารบัญภาพประกอบ

	หน้า
ภาพประกอบที่ 1.1 ตัวอย่างโปรแกรมเมื่อต้นสแกนช่องโหว่ของเว็บไซต์ HTTPS	4
ภาพประกอบที่ 1.2 ตัวอย่างโปรแกรมสแกนช่องโหว่ของเว็บไซต์ HTTPS	4
ภาพประกอบที่ 1.3 ตัวอย่างหน้ารายงานการจากประมวลผล	5
ภาพประกอบที่ 1.4 ภาพรวมของโครงการปริญญาโท	6
ภาพประกอบที่ 1.5 การทดสอบการโจมตีด้วยเทคนิค SSL Stripping Attack.....	7
ภาพประกอบที่ 1.6 โครงสร้างภายในของ Software ที่จะพัฒนา	8
ภาพประกอบที่ 1.7 แนวทางการแก้ไขปัญหา	9
ภาพประกอบที่ 2.1 การรับ – ส่งข้อมูลบน HTTP Protocol	11
ภาพประกอบที่ 2.2 การรับ – ส่งข้อมูลบน HTTPS Protocol	12
ภาพประกอบที่ 2.3 กรณีตัวอย่าง Salted - Hash Password.....	13
ภาพประกอบที่ 2.4 ตัวอย่างการเข้ารหัสด้วยเทคนิค Hash ด้วย SHA256.....	13
ภาพประกอบที่ 2.5 การเข้ารหัสด้วยเทคนิค Hash ด้วย SHA256.....	14
ภาพประกอบที่ 2.6 ลักษณะการโจมตีด้วยเทคนิค DROWN Attack.....	15
ภาพประกอบที่ 2.7 ลักษณะการโจมตีด้วยเทคนิค POODLE Attack.....	16
ภาพประกอบที่ 2.8 ลักษณะการโจมตีด้วยเทคนิค MITM.....	18
ภาพประกอบที่ 2.9 Software license QT ทั้ง 3 แบบ.....	19
ภาพประกอบที่ 2.10 ตัวอย่างเว็บไซต์ที่ให้บริการตรวจสอบช่องโหว่ของ SSL/TLS	20
ภาพประกอบที่ 2.11 ตัวอย่างเว็บไซต์ที่ให้บริการตรวจสอบช่องโหว่ของ SSL/TLS	20
ภาพประกอบที่ 3.1 ภาพรวมของโครงการปริญญาโท.....	21
ภาพประกอบที่ 3.2 การสื่อสาร HTTPS แบบทั่วไป.....	22
ภาพประกอบที่ 3.3 การแทรกกลางการสื่อสาร	23
ภาพประกอบที่ 3.4 ป้องกันการแทรกกลางการสื่อสารด้วย HSTS	23
ภาพประกอบที่ 3.5 การแทรกกลางการสื่อสารด้วย BetterCap	24
ภาพประกอบที่ 3.6 วิธีลงทะเบียน HSTS Preload.....	25
ภาพประกอบที่ 3.7 การทำงานของ HSTS Preload บน Browser.....	25
ภาพประกอบที่ 3.8 รูปแบบการป้องกันการปลด HTTPS ด้วย ISAN Enforcer	26
ภาพประกอบที่ 3.9 การจำลองอุปกรณ์ของเหยื่อ และ Hacker บน Linux OS.....	27
ภาพประกอบที่ 3.10 หน้าจอของเหยื่อ	27

สารบัญภาพประกอบ (ต่อ)

	หน้า
ภาพประกอบที่ 3.11 หน้าจอของ Hacker	28
ภาพประกอบที่ 3.12 หมายเลข IP ทั้งหมดบนเครือข่าย LAN เดียวกัน	28
ภาพประกอบที่ 3.13 การระบุเป้าหมายที่ต้องการโจมตี	29
ภาพประกอบที่ 3.14 การปลด HTTPS	29
ภาพประกอบที่ 3.15 Data Packet	29
ภาพประกอบที่ 3.16 Data Packet เมื่อเข้าสู่เว็บไซต์	30
ภาพประกอบที่ 3.17 หน้าเข้าสู่ระบบของเว็บไซต์ปลายทางของอุปกรณ์เหยื่อ	30
ภาพประกอบที่ 3.18 เข้าสู่ระบบสำเร็จ	31
ภาพประกอบที่ 3.19 ผลการดักจับข้อมูล Username และ Password	31
ภาพประกอบที่ 3.20 ตัวอย่างเว็บไซต์ที่ Preload HTTPS Header	32
ภาพประกอบที่ 3.21 ตัวอย่างเว็บไซต์ที่ไม่ได้ Preload HSTS Header	32
ภาพประกอบที่ 3.22 ตัวอย่าง Header ของเว็บไซต์	32
ภาพประกอบที่ 3.23 ตัวอย่าง Algorithm ที่ใช้ในการเข้ารหัส	33
ภาพประกอบที่ 3.24 กลไกการทำงานของ ISAN Enforcer	34
ภาพประกอบที่ 3.25 ISAN Enforcer Script	36
ภาพประกอบที่ 3.26 การเข้ารหัสด้วยอัลกอริทึม SHA – 512	37
ภาพประกอบที่ 3.27 ฟังก์ชันตรวจสอบ Header	38
ภาพประกอบที่ 3.28 ฟังก์ชันตรวจสอบหาช่องโหว่ต่อเทคนิค Downgraded Attack	39
ภาพประกอบที่ 3.29 ฟังก์ชันรับข้อมูล Certificate Authority	40
ภาพประกอบที่ 3.30 ตรวจสอบหา HSTS Preload บน Mozilla Firefox	40
ภาพประกอบที่ 3.31 เพิ่ม Domain name และตรวจสอบ Domain name	42
ภาพประกอบที่ 4.1 หน้าเว็บไซต์ของมหาวิทยาลัยมหาสารคามที่สามารถ Strip ได้	44
ภาพประกอบที่ 4.2 ผลการทดสอบเว็บไซต์มหาวิทยาลัยมหาสารคาม	44
ภาพประกอบที่ 4.3 ตัวอย่างหน้าเว็บธนาคารกรุงเทพไม่สามารถ Sniff ได้	45
ภาพประกอบที่ 4.4 ผลการ test หน้าเว็บธนาคารกรุงเทพไม่สามารถ Sniff ได้	45
ภาพประกอบที่ 4.5 หน้าเว็บหน่วยงานกระทรวงสาธารณสุขไม่สามารถ Strip ได้	46
ภาพประกอบที่ 4.6 ผลการ test เว็บไซต์หน่วยงานกระทรวงสาธารณสุขที่ไม่สามารถ Strip ได้	46
ภาพประกอบที่ 4.7 หน้าเว็บไซต์ Pantip ไม่สามารถ Strip ได้	47

สารบัญภาพประกอบ (ต่อ)

	หน้า
ภาพประกอบที่ 4.8 ผล test เว็บไซต์ Pantip ไม่สามารถ Strip ได้.....	47
ภาพประกอบที่ 4.9 หน้าเว็บมหาวิทยาลัยเทคโนโลยีสุรนารีสามารถ Strip ได้.....	48
ภาพประกอบที่ 4.10 ผล test เว็บไซต์มหาวิทยาลัยเทคโนโลยีสุรนารี.....	48
ภาพประกอบที่ 4.11 หน้าเว็บธนาคารทหารไทยสามารถ Strip ได้	49
ภาพประกอบที่ 4.12 ผล test ธนาคารทหารไทย ไม่สามารถ Sniff ได้	49
ภาพประกอบที่ 4.13 หน้าเว็บกระทรวงมหาดไทยสามารถ Strip ได้	50
ภาพประกอบที่ 4.14 ผล test กระทรวงมหาดไทยสามารถ Sniff ได้	50
ภาพประกอบที่ 4.15 หน้าเว็บ Stack Overflow สามารถ Strip ได้.....	51
ภาพประกอบที่ 4.16 ผล test เว็บไซต์ Stack Overflow ไม่สามารถ Sniff ได้.....	51
ภาพประกอบที่ 4.17 ตัวอย่างหน้าเว็บไซต์มหาวิทยาลัยขอนแก่นสามารถ Strip ได้.....	52
ภาพประกอบที่ 4.18 ผล test เว็บไซต์ของทุกมหาวิทยาลัยในการทดลองสามารถ Sniff ได้	52
ภาพประกอบที่ 4.19 หน้าเว็บธนาคารไทยพาณิชย์สามารถ Strip ได้.....	53
ภาพประกอบที่ 4.20 ผล test ธนาคารไทยพาณิชย์ และธนาคารกรุงเทพที่สามารถ Sniff ได้.....	54
ภาพประกอบที่ 4.21 หน้าเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคมสามารถ Strip ได้.....	54
ภาพประกอบที่ 4.22 ผล test กระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคมสามารถ Sniff ได้	55
ภาพประกอบที่ 4.23 เว็บไซต์ที่สามารถ Strip ได้ จำแนกตามวิธีการโจมตี และประเภทของเว็บไซต์ ..55	
ภาพประกอบที่ 4.24 เว็บไซต์ที่สามารถ Sniff ได้ จำแนกตามวิธีการโจมตี และประเภทของเว็บไซต์ ..56	
ภาพประกอบที่ 4.25 ตัวอย่างแสดงผลการสแกนความปลอดภัยของเว็บไซต์.....	56
ภาพประกอบที่ 4.26 ตัวอย่างหน้า Register.....	57
ภาพประกอบที่ 4.27 หน้า Register กรณีที่ไม่กรอกข้อมูลในการลงทะเบียน	57
ภาพประกอบที่ 4.28 หน้า Register กรณีไม่กรอก Username ในการลงทะเบียน	58
ภาพประกอบที่ 4.29 หน้า Register กรณีไม่กรอก Password ในการลงทะเบียน	58
ภาพประกอบที่ 4.30 หน้า Register กรณีกรอกข้อมูล Username ที่มีอยู่ในฐานข้อมูล.....	59
ภาพประกอบที่ 4.31 กรณีลงทะเบียนสำเร็จจะรีเทิร์นกลับมาที่หน้าล็อกอิน	59
ภาพประกอบที่ 4.32 หน้าล็อกอินกรณีล็อกอินสำเร็จ.....	60
ภาพประกอบที่ 4.33 หน้าล็อกอินกรณีไม่กรอก Password	60
ภาพประกอบที่ 4.34 หน้าล็อกอิน กรณีไม่กรอก Username	61
ภาพประกอบที่ 4.35 หน้าล็อกอิน กรณีกรอกข้อมูลผิด.....	61

สารบัญภาพประกอบ (ต่อ)

	หน้า
ภาพประกอบที่ 4.36 หน้าล็อกอิน กรณีกรอก 'or '1' = 1' (inject key) ที่ Password.....	62
ภาพประกอบที่ 4.37 ตัวอย่างการสแกน SSL จากเว็บไซต์ SSL Checker	62
ภาพประกอบที่ 4.38 ตัวอย่างการสแกนจาก เว็บไซต์ SSL Checker	63
ภาพประกอบที่ 4.39 ตัวอย่างการทดสอบจากเว็บไซต์	63
ภาพประกอบที่ ก-1 ติดตั้ง testssl.sh.....	71
ภาพประกอบที่ ก-2 ติดตั้ง whois.....	71
ภาพประกอบที่ ก-3 เปิด Folder sslScan.....	72
ภาพประกอบที่ ก-4 Run sslScan	72
ภาพประกอบที่ ก-5 ตัวอย่างโปรแกรม HTTPS Scan	72
ภาพประกอบที่ ข-1 ส่วนการทำงานของโปรแกรม	74
ภาพประกอบที่ ข-2 Interface เมื่อประมวลผลเสร็จสิ้น.....	74
ภาพประกอบที่ ค-1 ความเสี่ยงต่อการถูก Strip ด้วยการโจมตีด้วยเทคนิค SSL Stripping Attack	86