บทที่ 4
ผลการดำเนินงาน

ในบทนี้จะเป็นการกล่าวถึงผลการทดสอบการจำลองการโจมตีด้วยเทคนิค SSL Stripping Attack ในเครือข่าย LAN เดียวกัน ซึ่งผลการทดสอบการโจมตี ณ วันที่ 6 มิถุนายน พ.ศ.2564 การทำงานของโปรแกรมที่ใช้ในการตรวจหาช่องโหว่ที่เป็นความเสี่ยงต่อการโจมตีด้วยเทคนิค Downgraded Attack และเทคนิค SSL Stripping Attack รวมถึงทดสอบเว็บไซต์ล็อกอินที่เข้ารหัสด้วย Salted - Hash Password

4.1 ผลการทดสอบการจำลองการโจมด้วยเทคนิค SSL Stripping Attack

จากการจำลองการโจมตีด้วยเทคนิค SSL Stripping Attack ได้จำลองการโจมตีทั้งหมด 3 รูปแบบ คือ

1) BetterCap
2) BetterCap เปลี่ยน Script
3) SSL Stripping Attack

4.1.1 BetterCap

ตารางที่ 4.1 เว็บไซต์ของมหาวิทยาลัย

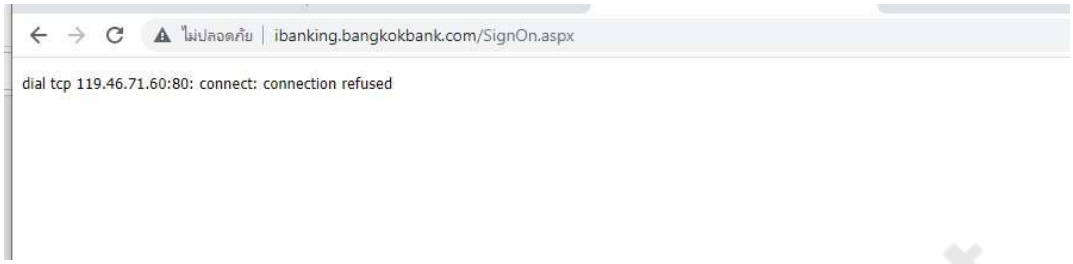
ลำดับ	เว็บไซต์		Strip	Sniff
	ชื่อ	โดเมน		
1	มหาวิทยาลัยมหาสารคาม	Reg.msu.ac.th	/	/
2	มหาวิทยาลัยเทคโนโลยีสุรนารี	Reg3.sut.ac.th	/	/
3	มหาวิทยาลัยขอนแก่น	Reg.kku.ac.th	X	X
4	มหาวิทยาลัยธรรมศาสตร์	Reg.tu.ac.th	/	/
5	จุฬาลงกรณ์มหาวิทยาลัย	Reg.chula.ac.th	/	/
6	มหาวิทยาลัยแม่ฟ้าหลวง	Reg.mfu.ac.ht	/	/
7	มหาวิทยาลัยบูรพา	Reg.buu.ac.th	/	/

ภาพประกอบที่ 4.1 หน้าเว็บไซต์ของมหาวิทยาลัยมหาสารคามที่สามารถ Strip ได้

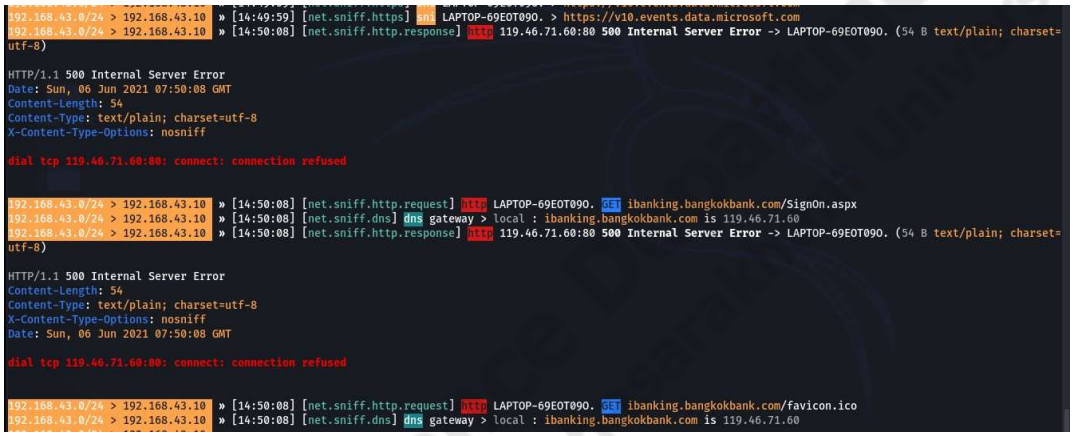
ภาพประกอบที่ 4.2 ผลการทดสอบเว็บไซต์มหาวิทยาลัยมหาสารคาม

ตารางที่ 4.2 เว็บไซต์ของธนาคาร

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	ธนาคารกรุงเทพ	HTTPS://ibanking.bangkokbank.com/SignOn.aspx	/	X
2	ธนาคารไทยพาณิชย์	HTTPS://www.scbeasy.com/v1.4/site/presignon/index.asp	X	X
3	ธนาคารกรุงไทย	HTTPS://www.ktbnetbank.com/consumer/	X	X
4	ธนาคารกสิกร	HTTPS://online.kasikornbankgroup.com/K-Online/	X	X
5	ธนาคารทหารไทย	HTTPS://www.ttbdirect.com/tmb/kdw1.31.2	/	X



ภาพประกอบที่ 4.3 ตัวอย่างหน้าเว็บธนาคารกรุงเทพไม่สามารถ Sniff ได้



ภาพประกอบที่ 4.4 ผลการ test หน้าเว็บธนาคารกรุงเทพไม่สามารถ Sniff ได้

ตารางที่ 4.3 เว็บไซต์ของหน่วยงานภาครัฐ

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	เว็บไซต์กลางบริการอิเล็กทรอนิกส์	accounts.egov.go.th/Citizen/Account/Login	/	/
2	กระทรวงสาธารณสุข	accounts.mail.go.th	X	X
3	กระทรวงมหาดไทย	Moi.go.th	/	/
4	กระทรวงดิจิทัล	Mdes.go.th	X	X

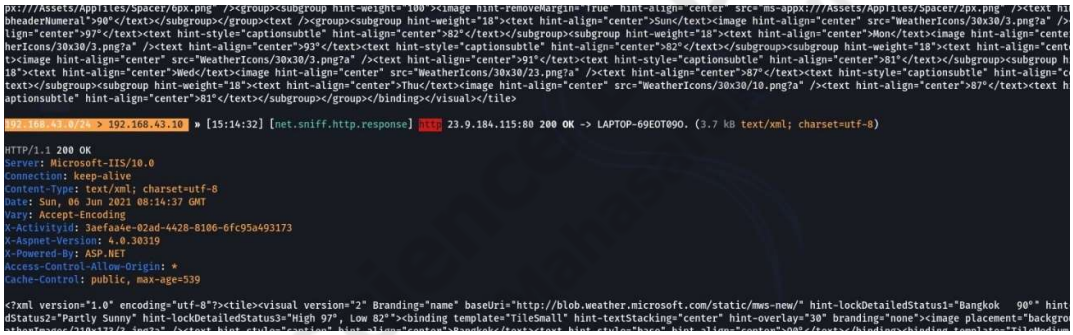
ภาพประกอบที่ 4.5 หน้าเว็บหน่วยงานกระทรวงสาธารณสุขไม่สามารถ Strip ได้

ภาพประกอบที่ 4.6 ผลการ test เว็บไซต์หน่วยงานกระทรวงสาธารณสุขที่ไม่สามารถ Strip ได้

ตารางที่ 4.4 เว็บไซต์ทั่วไป

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	Pantip	Pantip.com	X	X
2	Stack Overflow	Stackoverflow.com	X	X

ภาพประกอบที่ 4.7 หน้าเว็บไซต์ Pantip ไม่สามารถ Strip ได้

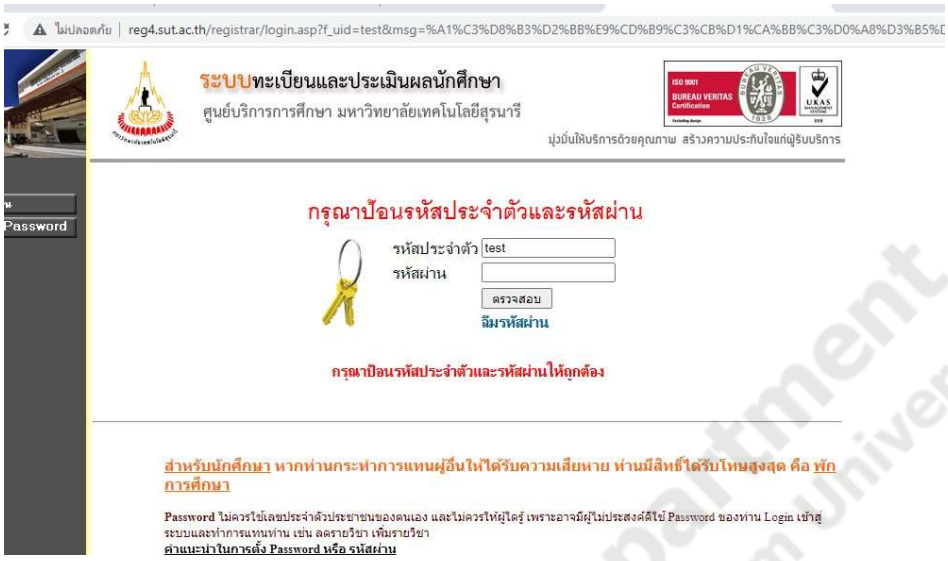


ภาพประกอบที่ 4.8 ผล test เว็บไซต์ Pantip ไม่สามารถ Strip ได้

4.1.2 BetterCap เปลี่ยน Script

ตารางที่ 4.5 เว็บไซต์ของมหาวิทยาลัย

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	มหาวิทยาลัยมหาสารคาม	Reg.msu.ac.th	/	/
2	มหาวิทยาลัยเทคโนโลยีสุรนารี	Reg3.sut.ac.th	/	/
3	มหาวิทยาลัยขอนแก่น	Reg.kku.ac.th	X	X
4	มหาวิทยาลัยธรรมศาสตร์	Reg.tu.ac.th	/	/
5	จุฬาลงกรณ์มหาวิทยาลัย	Reg.chula.ac.th	/	/
6	มหาวิทยาลัยแม่ฟ้าหลวง	Reg.mfu.ac.ht	X	X
7	มหาวิทยาลัยบูรพา	Reg.buu.ac.th	/	/

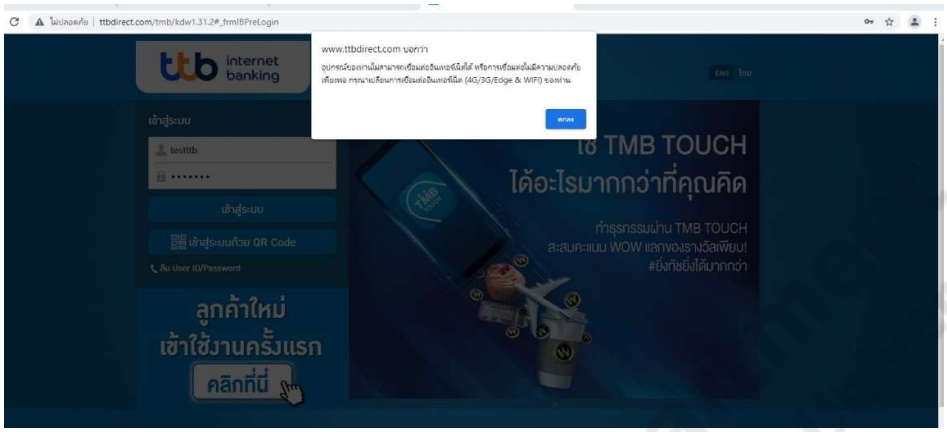


ภาพประกอบที่ 4.9 หน้าเว็บมหาวิทยาลัยเทคโนโลยีสุรนารีสามารถ Strip ได้

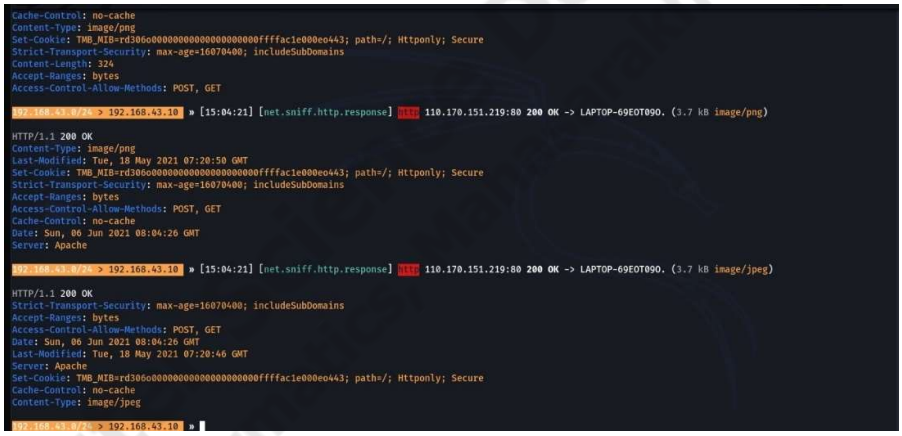
ภาพประกอบที่ 4.10 ผล test เว็บไซต์มหาวิทยาลัยเทคโนโลยีสุรนารี

ตารางที่ 4.6 เว็บไซต์ของธนาคาร

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	ธนาคารกรุงเทพ	ibanking.bangkokbank.com/SignOn.aspx	/	X
2	ธนาคารไทยพาณิชย์	www.scbeasy.com/v1.4/site/presignon/index.asp	/	X
3	ธนาคารกรุงไทย	www.ktbnetbank.com/consumer/	X	X
4	ธนาคารกสิกร	online.kasikornbankgroup.com/K-Online/	X	X
5	ธนาคารทหารไทย	www.ttbdirect.com/tmb/kdw1.31.2	/	X



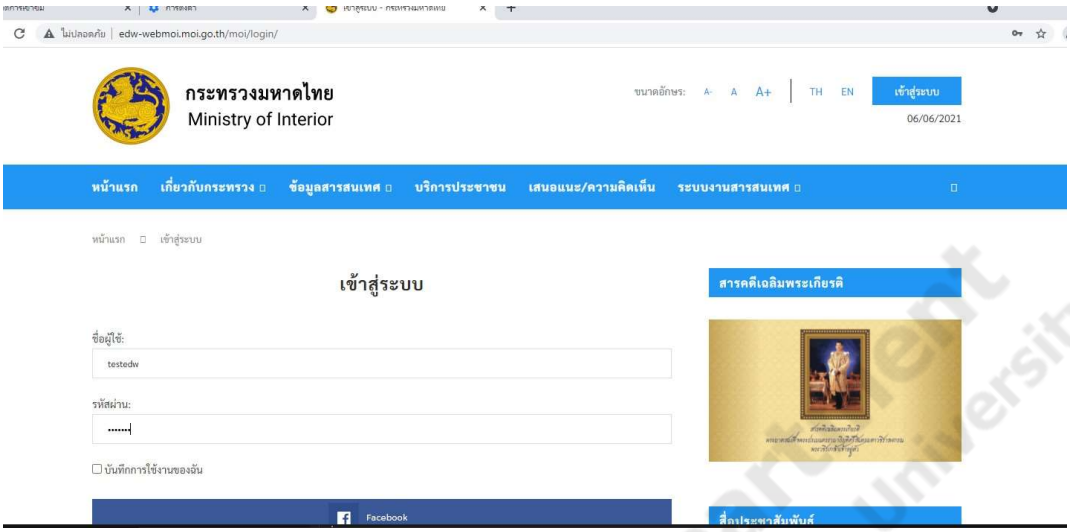
ภาพประกอบที่ 4.11 หน้าเว็บธนาคารทหารไทยสามารถ Strip ได้



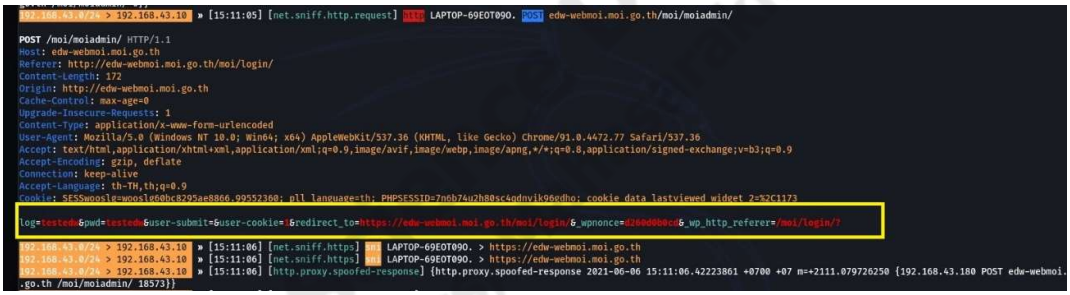
ภาพประกอบที่ 4.12 ผล test ธนาคารทหารไทย ไม่สามารถ Sniff ได้

ตารางที่ 4.7 เว็บไซต์ของหน่วยงานภาครัฐ

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	เว็บไซต์กลางบริการอิเล็กทรอนิกส์	accounts.egov.go.th/Citizen/Account/Login	/	/
2	กระทรวงสาธารณสุข	accounts.mail.go.th	X	X
3	กระทรวงมหาดไทย	Moi.go.th	/	/
4	กระทรวงดิจิทัล	Mdes.go.th	X	X



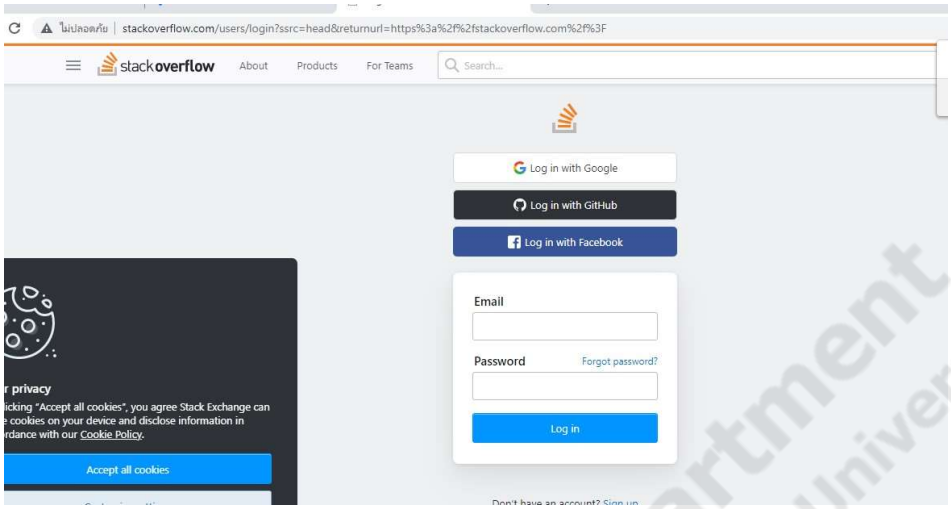
ภาพประกอบที่ 4.13 หน้าเว็บกระทรวงมหาดไทยสามารถ Strip ได้



ภาพประกอบที่ 4.14 ผล test กระทรวงมหาดไทยสามารถ Sniff ได้

ตารางที่ 4.8 เว็บไซต์ทั่วไป

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	Pantip	Pantip.com	X	X
2	Stack Overflow	Stackoverflow.com	/	X



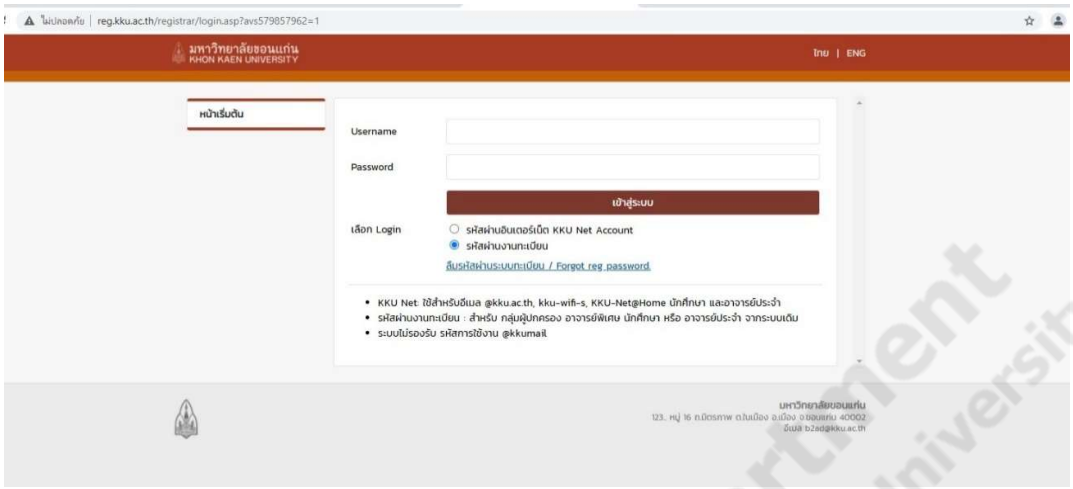
ภาพประกอบที่ 4.15 หน้าเว็บ Stack Overflow สามารถ Strip ได้

ภาพประกอบที่ 4.16 ผล test เว็บ Stack Overflow ไม่สามารถ Sniff ได้

4.1.3 SSL Strip Moxie Marlinspike's Script

ตารางที่ 4.9 เว็บไซต์ของมหาวิทยาลัย

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	มหาวิทยาลัยมหาสารคาม	Reg.msu.ac.th	/	/
2	มหาวิทยาลัยเทคโนโลยีสุรนารี	Reg3.sut.ac.th	/	/
3	มหาวิทยาลัยขอนแก่น	Reg.kku.ac.th	/	/
4	มหาวิทยาลัยธรรมศาสตร์	Reg.tu.ac.th	/	/
5	จุฬาลงกรณ์มหาวิทยาลัย	Reg.chula.ac.th	/	/
6	มหาวิทยาลัยแม่ฟ้าหลวง	Reg.mfu.ac.ht	/	/
7	มหาวิทยาลัยบูรพา	Reg.buu.ac.th	/	/



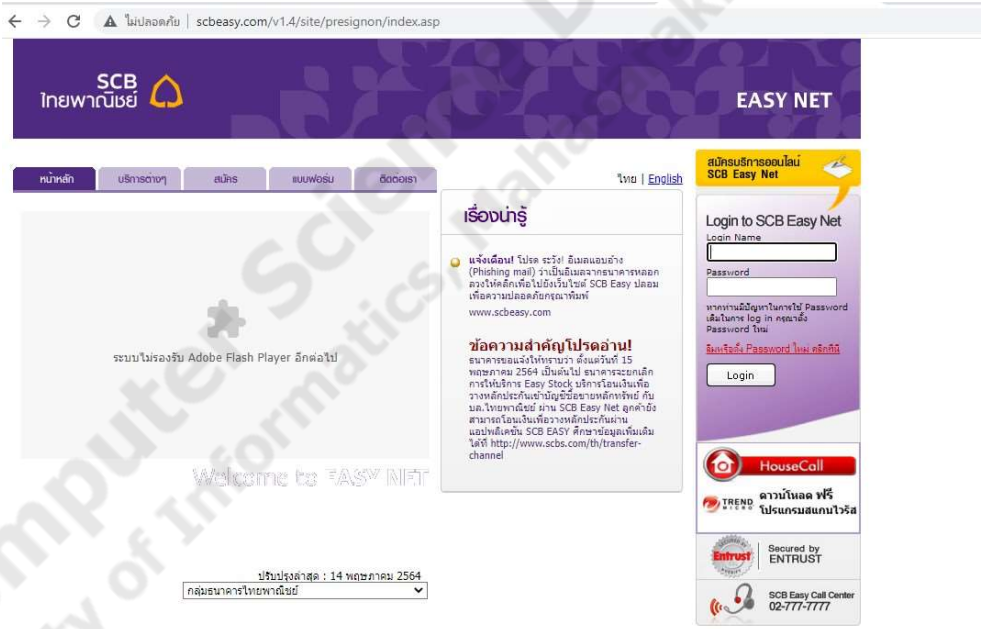
ภาพประกอบที่ 4.17 ตัวอย่างหน้าเว็บไซต์มหาวิทยาลัยขอนแก่นสามารถ Strip ได้

```
root@10:~# cat sslstrip.log
2021-06-07 03:30:57,287 POST Data (reg.msu.ac.th):
f_uid=testmsu&f_pwd=testmsu&BUILDKEY=17531
2021-06-07 03:32:38,859 POST Data (reg.kku.ac.th):
f_uid=testkku&f_pwd=testkku&BUILDKEY=68593&stdreportstudentcode=&CheckAuth=2
2021-06-07 03:33:07,870 POST Data (reg6.sut.ac.th):
f_uid=testsut&f_pwd=testsut&BUILDKEY=30479
2021-06-07 03:33:48,425 SECURE POST Data (web.reg.tu.ac.th):
lang=th&f_uid=testtu&f_pwd=testtu
2021-06-07 03:35:13,039 POST Data (www2.reg.chula.ac.th):
userid=testchula&programsystem=S&password=testchula&code=OLU9&submitLogon.x=32&s
ubmitLogon.y=11&language=T
2021-06-07 03:35:13,165 SECURE POST Data (www2.reg.chula.ac.th):
userid=testchula&programsystem=S&password=testchula&code=OLU9&submitLogon.x=32&s
ubmitLogon.y=11&language=T
2021-06-07 03:35:32,712 POST Data (reg.mfu.ac.th):
f_uid=testmfu&f_pwd=testmfu&BUILDKEY=25471
2021-06-07 03:36:11,989 POST Data (reg.buu.ac.th):
f_uid=testbuu&f_pwd=testbuu&BUILDKEY=63262
```

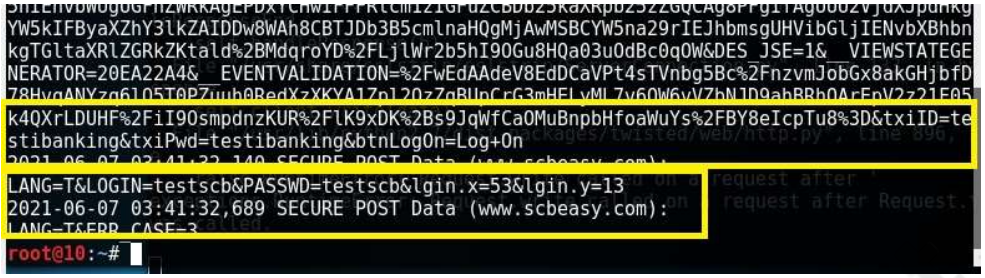
ภาพประกอบที่ 4.18 ผล test เว็บไซต์ของทุกมหาวิทยาลัยในการทดลองสามารถ Sniff ได้

ตารางที่ 4.10 เว็บไซต์ธนาคาร

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	ธนาคารกรุงเทพ	ibanking.bangkokbank.com/SignOn.aspx	/	/
2	ธนาคารไทยพาณิชย์	www.scbeasy.com/v1.4/site/presignon/index.asp	/	/
3	ธนาคารกรุงไทย	www.ktbnetbank.com/consumer/	X	X
4	ธนาคารกสิกร	online.kasikornbankgroup.com/K-Online/	/	/
5	ธนาคารทหารไทย	www.ttbdirect.com/tmb/kdw1.31.2	X	X



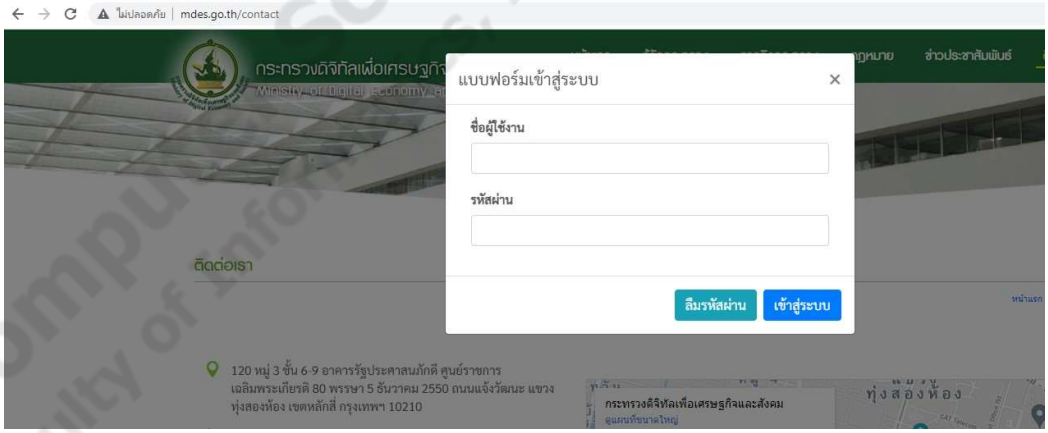
ภาพประกอบที่ 4.19 หน้าเว็บธนาคารไทยพาณิชย์สามารถ Strip ได้



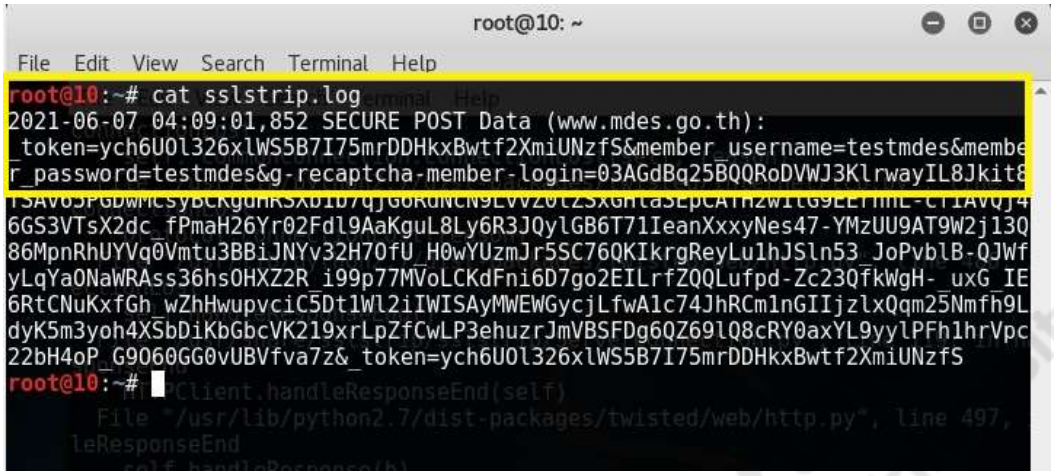
ภาพประกอบที่ 4.20 ผล test ธนาคารไทยพาณิชย์ และธนาคารกรุงเทพที่สามารถ Sniff ได้

ตารางที่ 4.11 เว็บไซต์ของหน่วยงานภาครัฐ

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	เว็บไซต์กลางบริการอิเล็กทรอนิกส์	accounts.egov.go.th/Citizen/Account/Login	/	/
2	กระทรวงสาธารณสุข	accounts.mail.go.th	X	X
3	กระทรวงมหาดไทย	Moi.go.th	/	/
4	กระทรวงดิจิทัล	www.mdes.go.th/contact	/	/



ภาพประกอบที่ 4.21 หน้าเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคมสามารถ Strip ได้

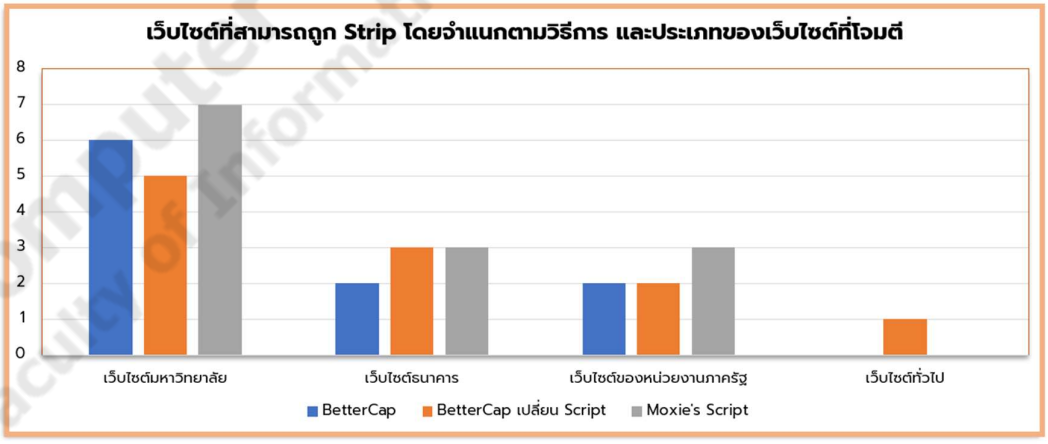


ภาพประกอบที่ 4.22 ผล test กระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคมสามารถ Sniff ได้

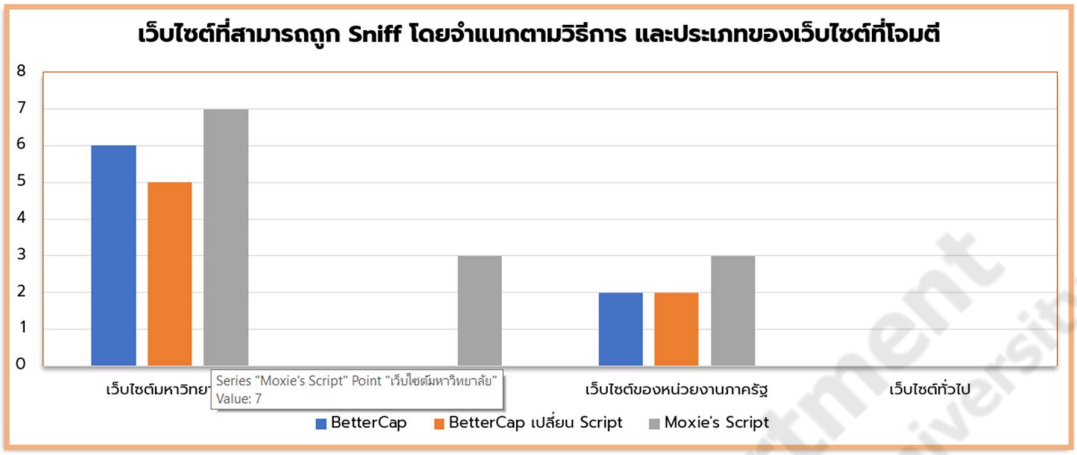
ตารางที่ 4.12 เว็บไซต์ทั่วไป

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	Pantip	Pantip.com	X	X
2	Stack Overflow	Stackoverflow.com	X	X

4.2 เทียบผลการทดสอบ



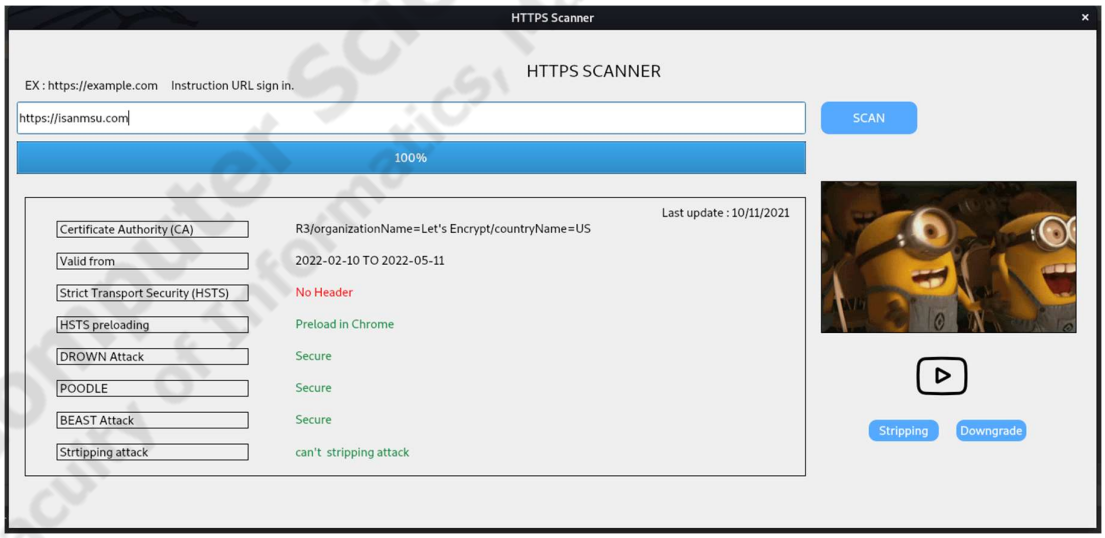
ภาพประกอบที่ 4.23 เว็บไซต์ที่สามารถ Strip ได้ จำแนกตามวิธีการโจมตี และประเภทของเว็บไซต์



ภาพประกอบที่ 4.24 เว็บไซต์ที่สามารถ Sniff ได้ จำแนกตามวิธีการโจมตี และประเภทของเว็บไซต์

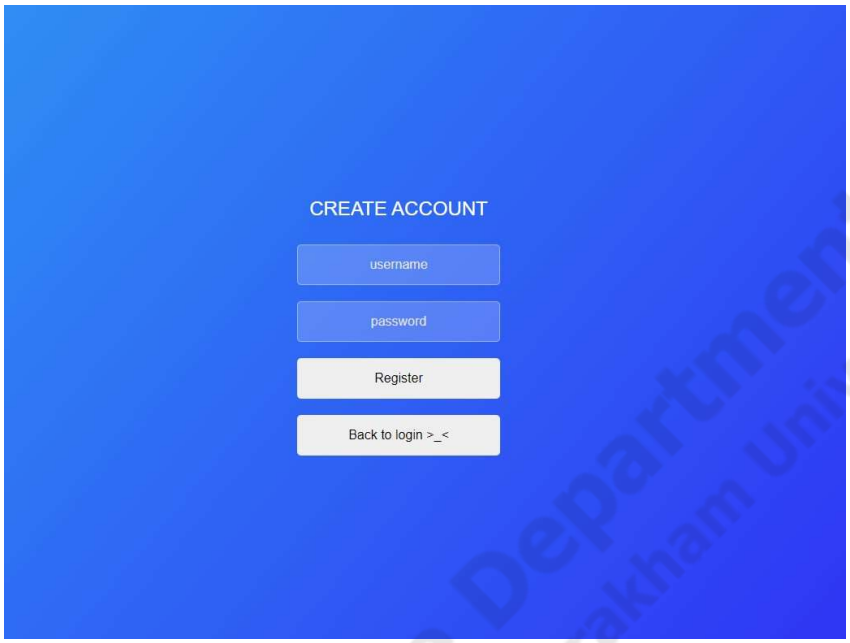
จากภาพประกอบที่ 4.23 และภาพประกอบที่ 4.24 ผลการทดสอบการโจมตี เห็นได้ชัดว่าการโจมตีของ Moxie Marlinspike มีประสิทธิภาพในการโจมตีมากที่สุดที่ใช้ในการโจมตี SSL Stripping Attack

4.3 ผลการตรวจสอบการป้องกันกับเว็บไซต์อื่น ๆ

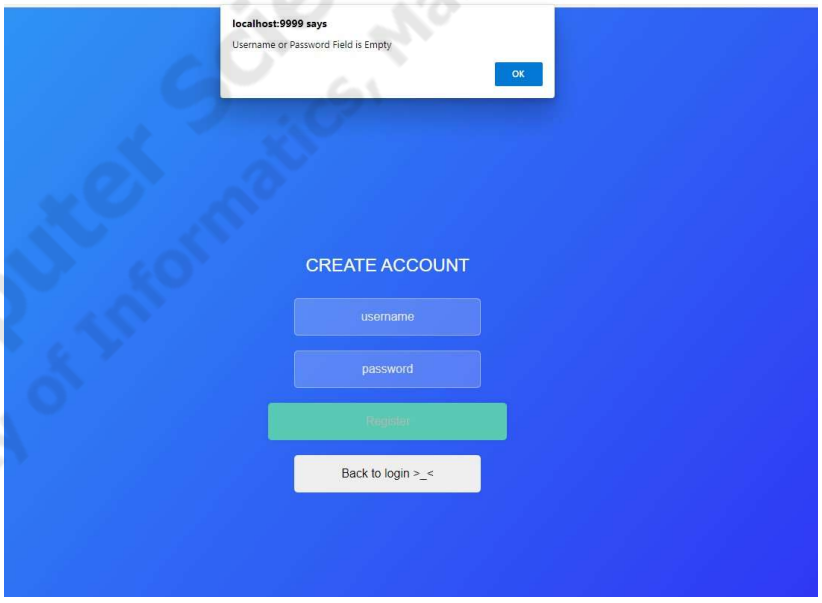


ภาพประกอบที่ 4.25 ตัวอย่างแสดงผลการแสกนความปลอดภัยของเว็บไซต์

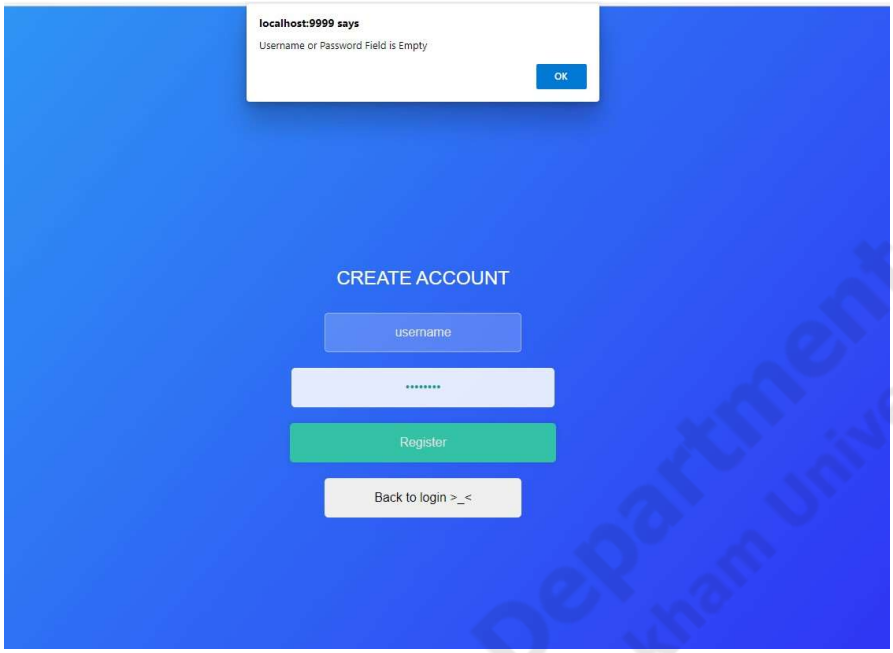
4.4 ทดสอบหน้าล็อกอิน Salted – Hash Password



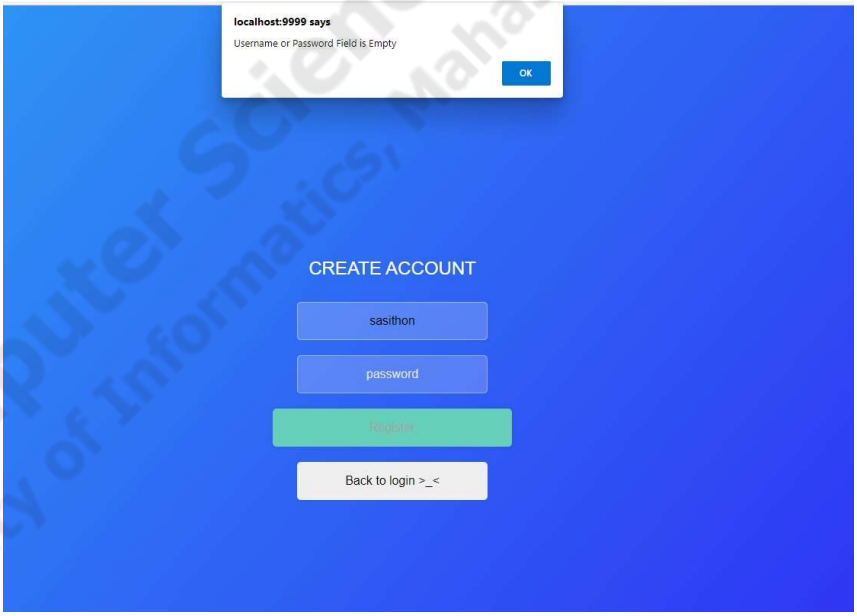
ภาพประกอบที่ 4.26 ตัวอย่างหน้า Register



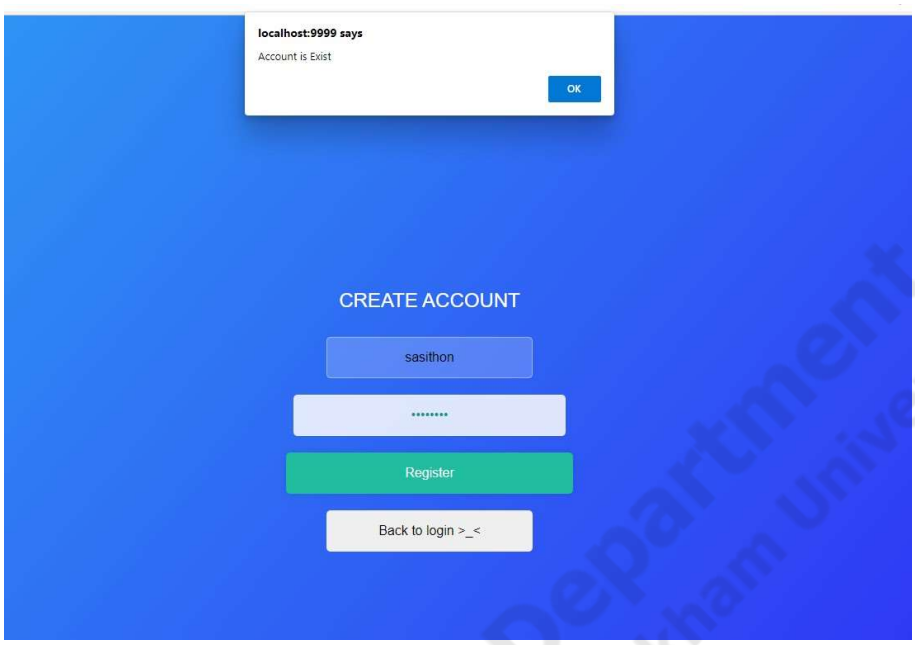
ภาพประกอบที่ 4.27 หน้า Register กรณีที่ไม่กรอกข้อมูลในการลงทะเบียน



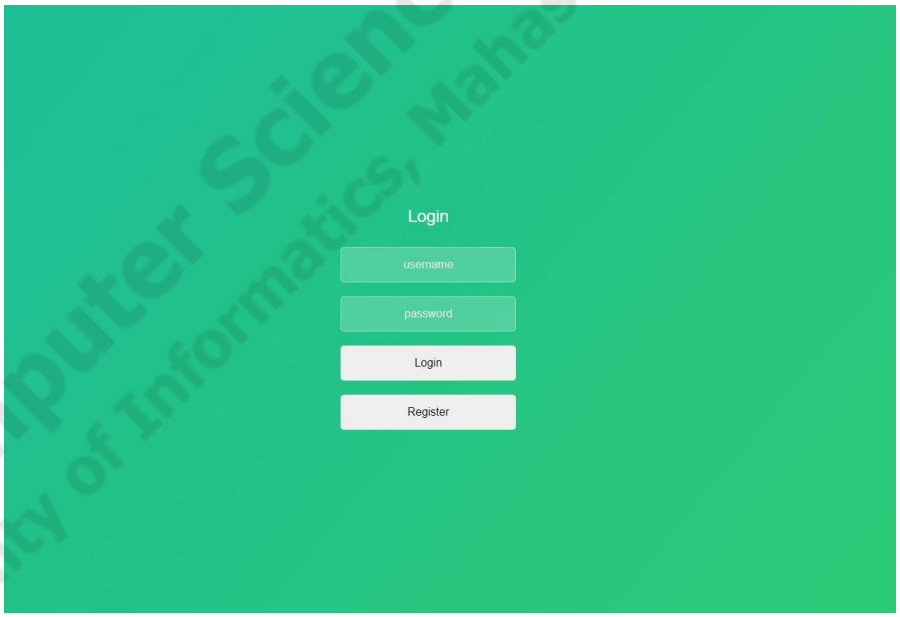
ภาพประกอบที่ 4.28 หน้า Register กรณีไม่กรอก Username ในการลงทะเบียน



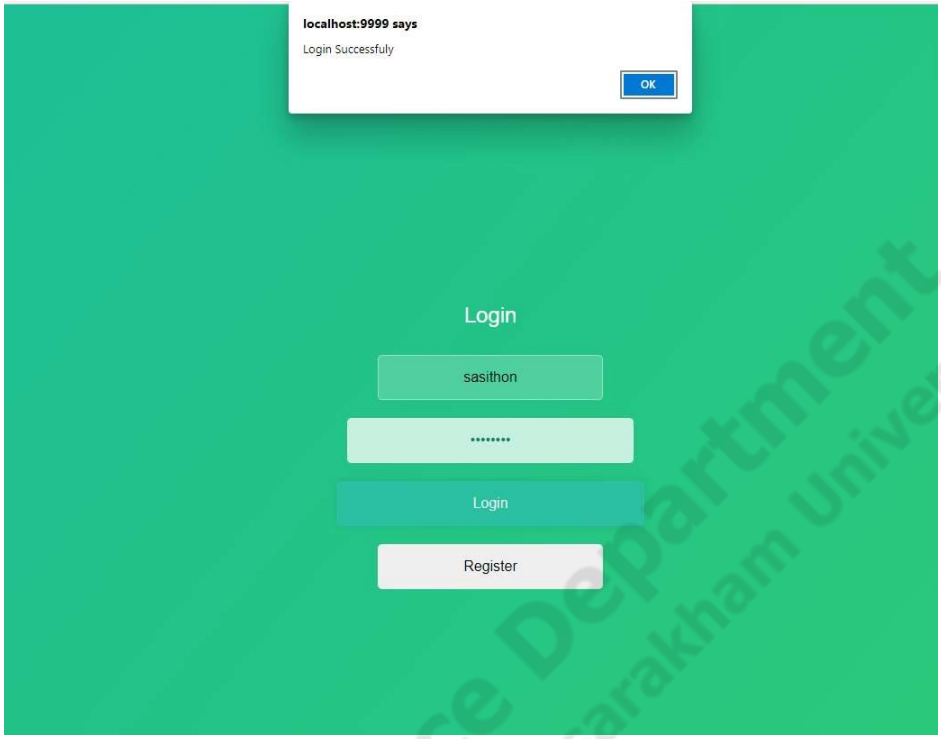
ภาพประกอบที่ 4.29 หน้า Register กรณีไม่กรอก Password ในการลงทะเบียน



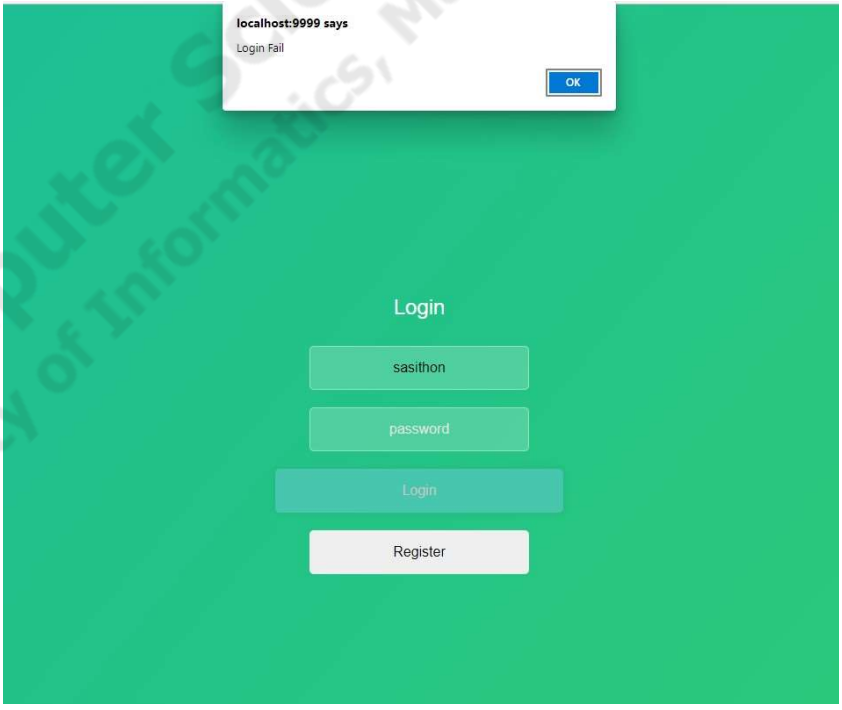
ภาพประกอบที่ 4.30 หน้า Register กรณีกรอกข้อมูล Username ที่มีอยู่ในฐานข้อมูล



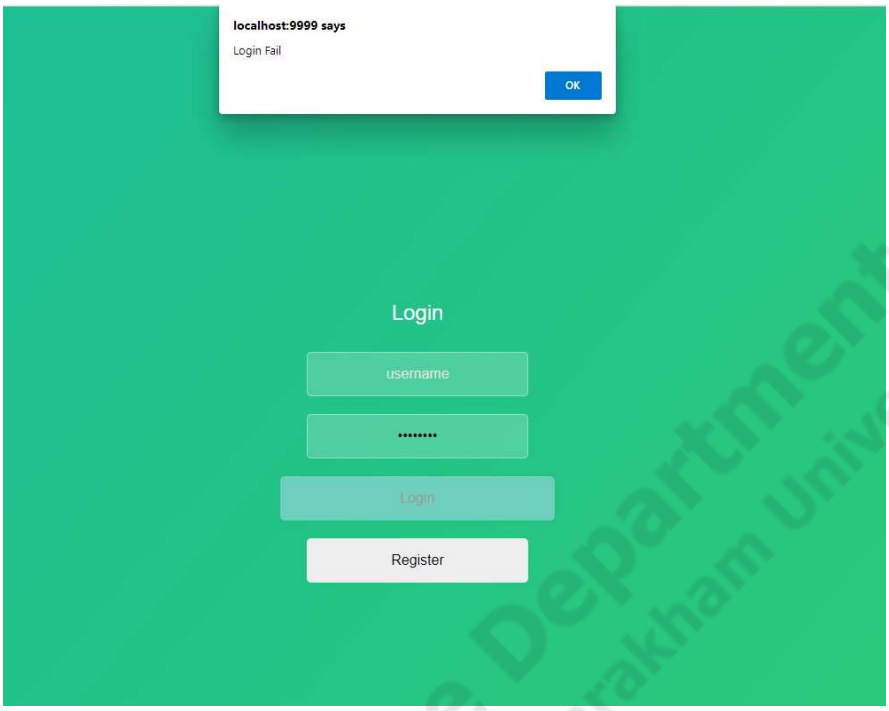
ภาพประกอบที่ 4.31 กรณีลงทะเบียนสำเร็จจะรีเทิร์นกลับมาที่หน้าล็อกอิน



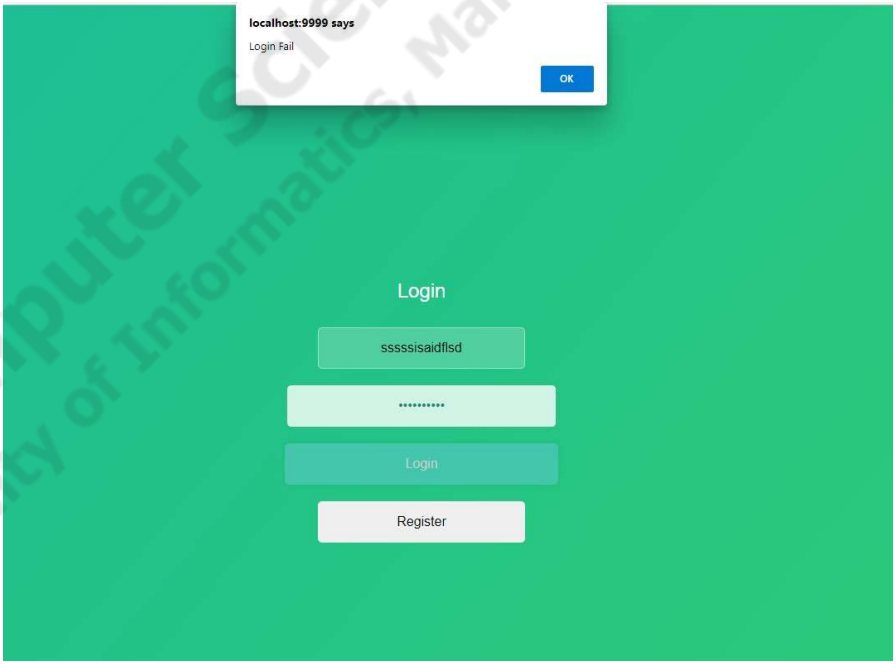
ภาพประกอบที่ 4.32 หน้าล็อกอินกรณีล็อกอินสำเร็จ



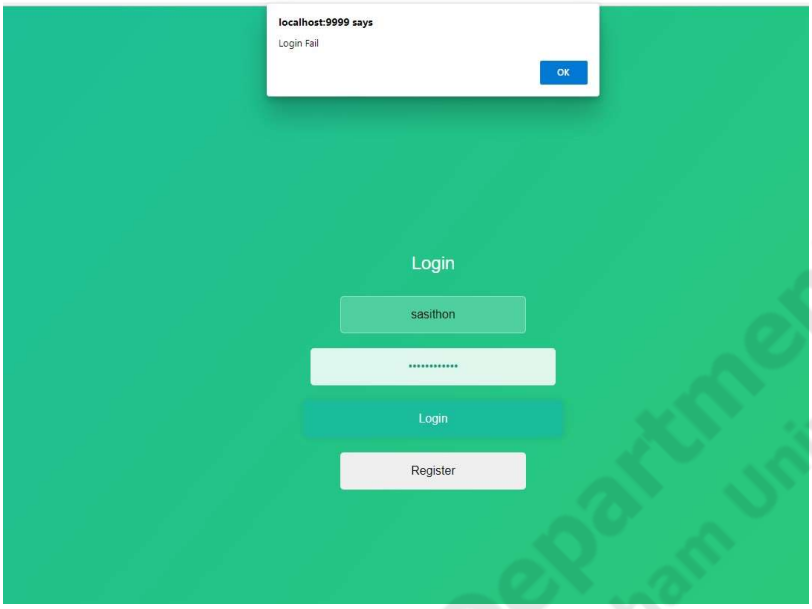
ภาพประกอบที่ 4.33 หน้าล็อกอินกรณีไม่กรอก Password



ภาพประกอบที่ 4.34 หน้าล็อกอิน กรณีไม่กรอก Username

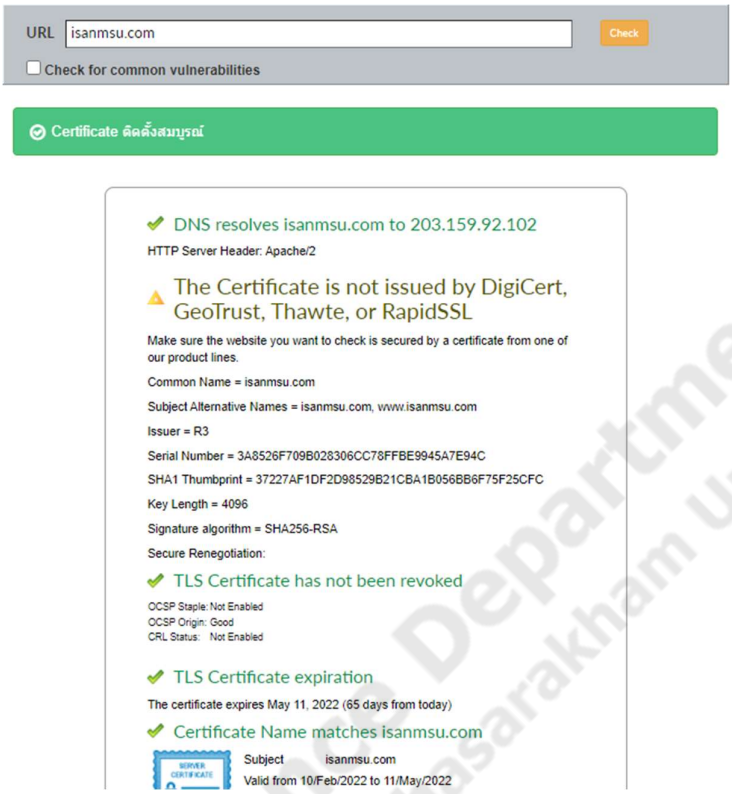


ภาพประกอบที่ 4.35 หน้าล็อกอิน กรณีกรอกข้อมูลมั่ว

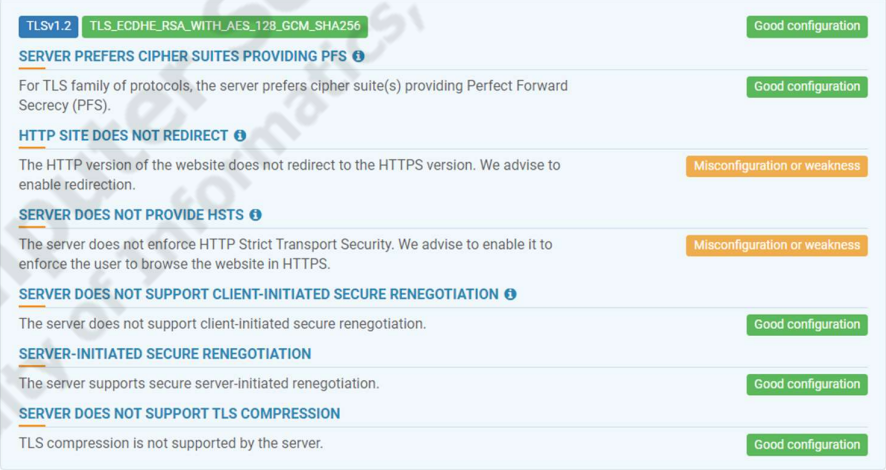


ภาพประกอบที่ 4.36 หน้าล็อกอิน กรณีกรอก ‘or ‘1’ = 1’ (inject key) ที่ Password

ภาพประกอบที่ 4.37 ตัวอย่างการแสกน SSL จากเว็บไซต์ SSL Checker



ภาพประกอบที่ 4.38 ตัวอย่างการแสกนจาก เว็บไซต์ SSL Checker



ภาพประกอบที่ 4.39 ตัวอย่างการทดสอบจากเว็บไซต์

[isanmsu.com SSL Security Test (immuniweb.com)]

จะเห็นได้ว่าทางเว็บไซต์แสดง HSTS กับทาง Header เพียงอย่างเดียวจึงทำให้ทราบผลได้อย่างไม่ถูกต้องทั้งหมดเนื่องจากทางเว็บไซต์ของ isanmsu.com หลังจากที่ได้ทำการ add domain ลง

chromium/#hshs และได้ทำการนำเอา Preload ออกจาก Header หากทางเว็บไซต์ไหนที่มีการเช็คแต่ที่ Header แล้วให้คำตอบว่า ว่า เว็บไซต์นั้นไม่ปลอดภัย เพราะว่าเจ้าของเว็บไซต์สามารถนำ Preload ออกจาก Header ได้ หาก add ลงใน list chromium/#hsts แล้ว สามารถเช็ค list ได้ที่ link transport_security_state_static.json - Chromium Code Search