

## 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 ผลการทดสอบการจำลองการโจมตีด้วยเทคนิค SSL Stripping Attack

จากการจำลองการโจมตีด้วยเทคนิค SSL Stripping Attack ได้จำลองการโจมตีทั้งหมด 3 รูปแบบ คือ

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

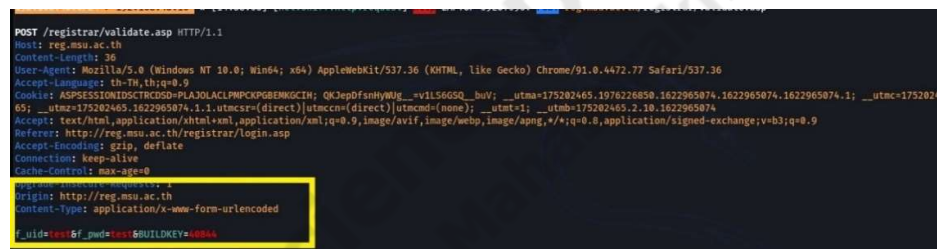
##### 4.1.1 BetterCap

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.th	/	/
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

```

192.168.43.0/24 > 192.168.43.10 » [14:49:59] [net.sniff.https] https://v10.events.data.microsoft.com
192.168.43.0/24 > 192.168.43.10 » [14:50:08] [net.sniff.http.response] 119.46.71.60:80 500 Internal Server Error -> LAPTOP-69EOT090. (54 B text/plain; charset=utf-8)

HTTP/1.1 500 Internal Server Error
Date: Sun, 06 Jun 2021 07:50:08 GMT
Content-Length: 54
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff

dial tcp 119.46.71.60:80: connect: connection refused

192.168.43.0/24 > 192.168.43.10 » [14:50:08] [net.sniff.http.request] 119.46.71.60:80 ibanking.bangkokbank.com/SignOn.aspx
192.168.43.0/24 > 192.168.43.10 » [14:50:08] [net.sniff.dns] dns gateway > local: ibanking.bangkokbank.com is 119.46.71.60
192.168.43.0/24 > 192.168.43.10 » [14:50:08] [net.sniff.http.response] 119.46.71.60:80 500 Internal Server Error -> LAPTOP-69EOT090. (54 B text/plain; charset=utf-8)

HTTP/1.1 500 Internal Server Error
Content-Length: 54
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Sun, 06 Jun 2021 07:50:08 GMT

dial tcp 119.46.71.60:80: connect: connection refused

192.168.43.0/24 > 192.168.43.10 » [14:50:08] [net.sniff.http.request] 119.46.71.60:80 ibanking.bangkokbank.com/favicon.ico
192.168.43.0/24 > 192.168.43.10 » [14:50:08] [net.sniff.dns] dns gateway > local: ibanking.bangkokbank.com is 119.46.71.60

```

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

```

b.wargaming.net/notifications/api/v1/incoming {}
92.223.29.19:80 -> 192.168.43.10 * [15:07:41] [net.sniff.http.response] HTTP/1.1 200 OK -> LAPTOP-69E0T090. (1 B application/json)
HTTP/1.1 200 OK
Keep-Alive: timeout=200
Server: openresty
Content-Length: 1
Connection: keep-alive
Content-Type: application/json
Date: Sun, 06 Jun 2021 08:07:46 GMT
0
  
```

ภาพประกอบที่ 4.6 ผลการ test เว็บไซต์หน่วยงานกระทรวงสาธารณสุขที่สามารถ 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

```

px:///Assets/App/ites/spacer/px.png /><group><subgroup hint-weight="100"><image hint-removeMargin="true" hint-align="center" src="ms-appx:///Assets/App/ites/spacer/2px.png /><text hi
bheaderNumber">90</text></subgroup></group><text /><group><subgroup hint-weight="18"><text hint-align="center">Sun</text><image hint-align="center" src="WeatherIcons/30x30/3.png?</
lign="center">97</text><text hint-style="captionsubtle" hint-align="center">82</text></subgroup><subgroup hint-weight="18"><text hint-align="center">Mon</text><image hint-align="cente
herIcons/30x30/3.png?</text><text hint-align="center">93</text><text hint-style="captionsubtle" hint-align="center">82</text></subgroup><subgroup hint-weight="18"><text hint-align="cent
t"><image hint-align="center" src="WeatherIcons/30x30/3.png?</text><text hint-align="center">91</text><text hint-style="captionsubtle" hint-align="center">81</text></subgroup><subgroup h
is"><text hint-align="center">Wed</text><image hint-align="center" src="WeatherIcons/30x30/23.png?</text><text hint-align="center">87</text><text hint-style="captionsubtle" hint-align="c
text"></subgroup><subgroup hint-weight="18"><text hint-align="center">Thu</text><image hint-align="center" src="WeatherIcons/30x30/10.png?</text><text hint-align="center">87</text><text h
captionsubtle" hint-align="center">81</text></subgroup></group></binding></visual></tile>

192.168.43.10 -> 192.168.43.10 [15:14:32] [net.sniff.http.response] 200 OK -> LAPTOP-69E0T090. (3.7 KB text/xml; charset=utf-8)

HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
Connection: keep-alive
Content-Type: text/xml; charset=utf-8
Date: Sun, 06 Jun 2021 08:14:37 GMT
Vary: Accept-Encoding
X-ActivityId: 3ae6a4e-02ad-4428-b106-6fc95a493173
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=539

<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Bangkok 90" hint
dStatus2="Partly Sunny" hint-lockDetailedStatus3="High 97", Low 82"><binding template="TileSmall" hint-textStacking="center" hint-overlay="30" branding="none"><image placement="backgro

```

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

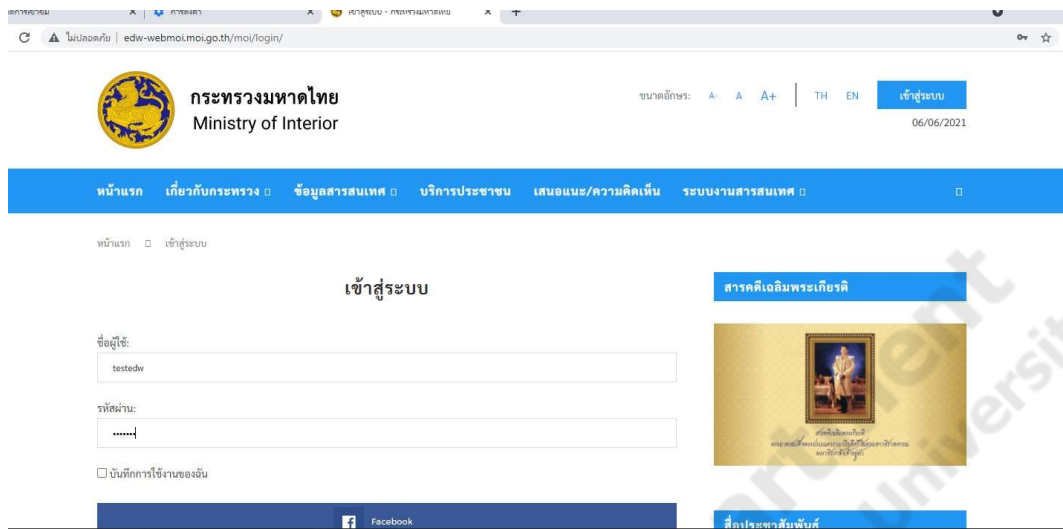
```
POST /registrar/validate.asp HTTP/1.1
Host: reg4.sut.ac.th
Connection: Keep-alive
Referer: http://reg4.sut.ac.th/registrar/login.asp
Accept-Encoding: gzip, deflate
Origin: http://reg4.sut.ac.th
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Content-Length: 36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept-Language: th-TH,th;q=0.9
Cookie: ASPSESSIONIDQAO8TOCC=NFPJDDKBEMPJBAOHEOLMKLJD
f_uid=test&f_pwd=test&BUILDKEY=P8830
```

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 4.13 หน้าเว็บกระทรวงมหาดไทยสามารถ Strip ได้

```

192.168.43.10 > 192.168.43.10 [15:11:05] [net.sniff.http.request] [LAPTOP-69E0T090.] [edw-webmoi.moi.go.th/moi/moiaadmin/
POST /moi/moiaadmin/ HTTP/1.1
Host: edw-webmoi.moi.go.th
Referer: http://edw-webmoi.moi.go.th/moi/login/
Content-Length: 172
Origin: http://edw-webmoi.moi.go.th
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=7n6b7a1z80xc4adnvl1b6a0ho; cookie_data_lastviewed/widget/2/87C1173
log=token&pwd=test&user-submit=&user-cookie=&redirect_to=https://edw-webmoi.moi.go.th/moi/login/&wnonce=4264080ac6&up_http_referer=/moi/login/?
192.168.43.0/26 > 192.168.43.10 [15:11:06] [net.sniff.https] [LAPTOP-69E0T090.] > https://edw-webmoi.moi.go.th
192.168.43.0/26 > 192.168.43.10 [15:11:06] [net.sniff.https] [LAPTOP-69E0T090.] > https://edw-webmoi.moi.go.th
192.168.43.0/26 > 192.168.43.10 [15:11:06] [http.proxy.spoofed-response] [http.proxy.spoofed-response 2021-06-06 15:11:06.42223861 +0700 +07 m=+2111.079726250 {192.168.43.180 POST edw-webmoi.
go.th /moi/moiaadmin/ 18573}]

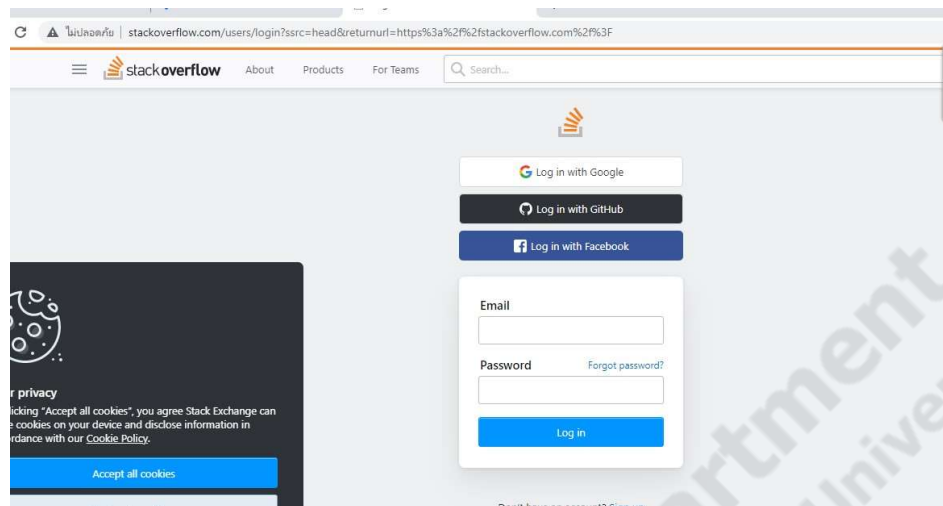
```

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

```

HTTP/1.1 200 OK
Content-Length: 1
Connection: keep-alive
Content-Type: application/json
Date: Sun, 06 Jun 2021 08:22:46 GMT
Keep-Alive: timeout=200
Server: openresty

0
192.168.43.0/24 > 192.168.43.10 > [15:22:41] [net.sniff.http.request] [1] LAPTOP-69E0T900. [2] wgcp5-asia-nsdb.wargaming.net/notifications/api/v1/incoming?account_id=2030594866
192.168.43.0/24 > 192.168.43.10 > [15:22:41] [net.sniff.dns] [1] gateway > local : fe-sg2.wgcrowd.io is 92.223.29.19, 92.223.29.20
192.168.43.0/24 > 192.168.43.10 > [15:22:41] [net.sniff.http.request] [1] local [2] wgcp5-asia-nsdb.wargaming.net/notifications/api/v1/incoming?account_id=2030594866
192.168.43.0/24 > 192.168.43.10 > [15:22:41] [net.sniff.http.response] [1] 92.223.29.19:80 200 OK -> local (1.8 application/json)

HTTP/1.1 200 OK
Keep-Alive: timeout=200
Server: openresty
Date: Sun, 06 Jun 2021 08:22:46 GMT
Content-Type: application/json
Content-Length: 1
Connection: keep-alive

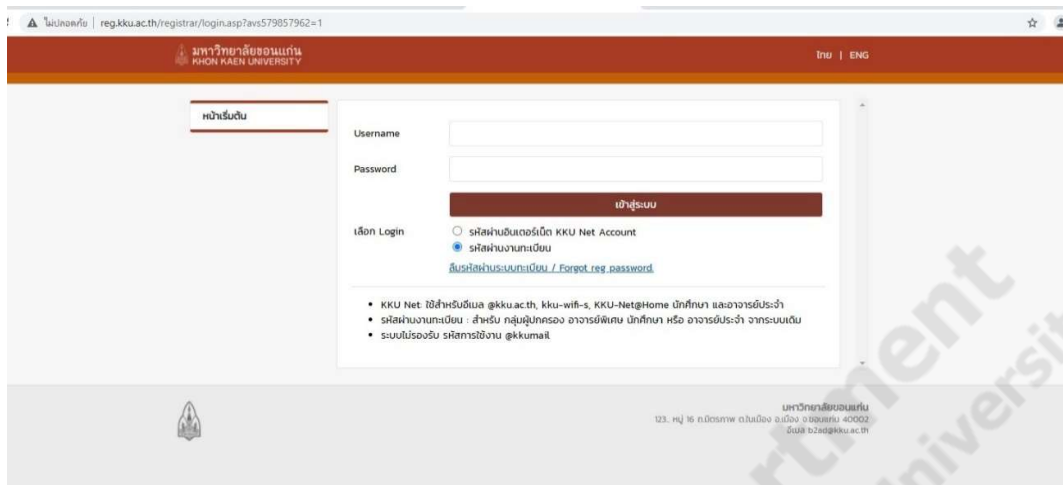
```

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

```

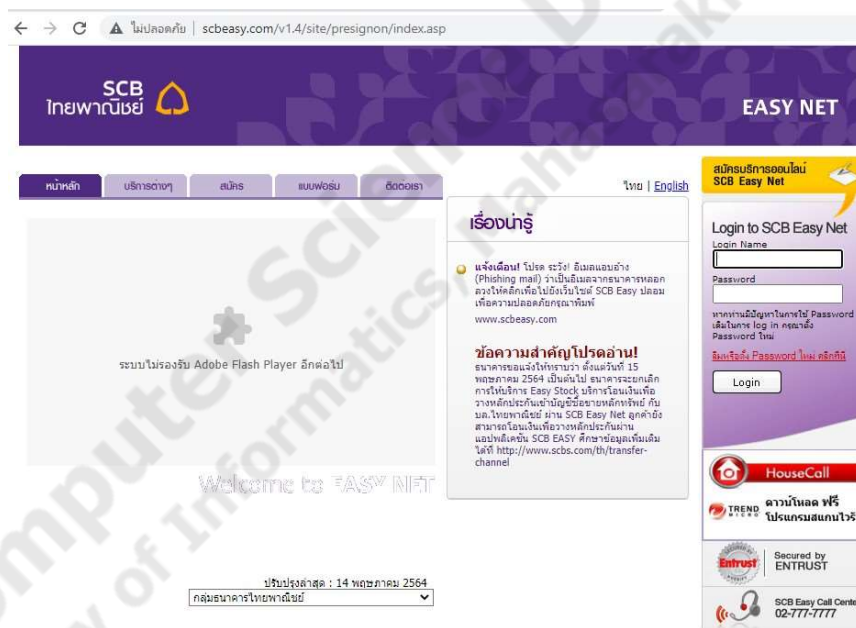
root@10:~# cat sslstrip.log
2021-06-07 03:30:57,287 POST Data (reg.msu.ac.th):
f_uid=testmsu&f_pwd=testmsu&BUILDKEY=17531
2021-06-07 03:32:38,859 POST Data (reg.kku.ac.th):
f_uid=testkku&f_pwd=testkku&BUILDKEY=68593&stdreportstudentcode=&CheckAuth=2
2021-06-07 03:33:07,870 POST Data (reg6.sut.ac.th):
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=0LU9&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=0LU9&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

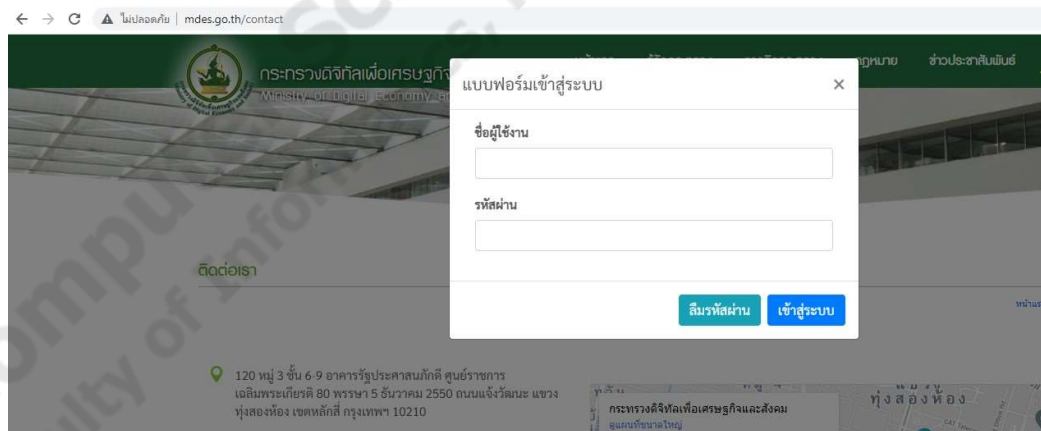
```

SHIENvbw0g0GhZWRKAgEPDXrChWlFfPRkcmI2IGf0ZC6b0z5kaXKpb2522GQCAG8PTg1TAgu000zvj0XjPunkY
YW5kIFByaXZhY3lkZAIDdw8WAh8CBTJDb3B5cm1naHQgMjAwMSBCYW5na29rIEJhbmsgUHVibGJjIENvbXBhbn
kgTGltaXRlZGRkZKtaId%2BMdqroYD%2FLj1Wr2b5hI90Gu8H0a03u0dBC0q0W&DES_JSE=1&VIEWSTAGE
NERATOR=20EA22A4&EVENTVALIDATION=%2FwEdAAdeV8EdDCaVpt4sTVnbg5Bc%2FgzvmJobGx8akGHjbfD
78HvqANYzq6105T0P7uub0RedYzXKYA17n120z7qBlInCrc63mHFIvMI7v60W6vV7hN1D0ahBRh0ArFoV2z21E05
k40XrLDUHF%2FiI90smpdnzKUR%2FLK9xDK%2B59JqWfCa0MuBnpbHfoawuYs%2FBY8eIcpTu8%3D&txiID=te
stibanking&txiPwd=testibanking&btnLogOn=Log+On
2021-06-07 03:41:22 140 SECURE POST Data (www.scbeasy.com):
LANG=T&LOGIN=testscb&PASSWD=testscb&lgIn.x=53&lgIn.y=13
2021-06-07 03:41:32,689 SECURE POST Data (www.scbeasy.com):
LANG=T&FBP_CASE=3
root@10:~#
    
```

ภาพประกอบที่ 4.20 ผล test ธนาคารไทยพาณิชย์ และธนาคารกรุงเทพที่สามารถ Sniff ได้

ตารางที่ 4.11 เว็บไซต์ของหน่วยงานภาครัฐ

ลำดับ	Website		Strip	Sniff
	ชื่อ	โดเมน		
1	เว็บไซต์กลางบริการ อิเล็กทรอนิกส์	accounts.egov.go.th/Citizen/Account/L ogin	/	/
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

```

root@10: ~
File Edit View Search Terminal Help
root@10:~# cat sslstrip.log
2021-06-07 04:09:01,852 SECURE POST Data (www.mdes.go.th):
  token=yeh6U0L326xLWS5B7I75mrDDHkxBwtf2XmiUNzfS&member_username=testmdes&membe
  r_password=testmdes&g-recaptcha-member-login=03AGdBq25BQQRodVWJ3KlRwayIL8Jkit8
  r5AV0vJpGdWmCsybCKgUHRsXb1b7qj60RdNcN9LvvZ0tZ5XGhtA5epCArhzw1tG9LErmmL-CFlAVQJ4
  6GS3VTsX2dc fPmaH26Yr02Fd19AaKguL8Ly6R3JQyLGB6T71IeanXxyNes47-YMzUU9AT9W2j13Q
  86MpnRhUYVq0Vmtu3BBiJNYv32H70fU_H0wYUzmJr5SC76QKIKrgReyLu1hJSlN53_JoPvb1B-QJWf
  yLqYa0NaWRAs36hs0HXZ2R_i99p77MVoLCKdFn16D7go2EILrfZ0QLufpd-Zc23QfkWgH- uxG IE
  6RtCNuXxfGh_wZhWupvcic5Dt1wL2iIWISayMWEWGycjLfwA1c74JhRCm1nGIijzlxQqm25Nmfh9L
  dyK5m3yoh4XSbDiKbGbcVK219xrLpZfCwLP3ehuzrJmVBSFDg6QZ69LQ8cRY0axYL9yyLPFh1hrVpc
  22bH4oP_G9060GG0vUBVfva7z&_token=yeh6U0L326xLWS5B7I75mrDDHkxBwtf2XmiUNzfS
root@10:~# █Client.handleResponseEnd(self)
  File "/usr/lib/python2.7/dist-packages/twisted/web/http.py", line 497,
  leResponseEnd
  File "/usr/lib/python2.7/dist-packages/twisted/web/http.py", line 497,
  leResponseEnd

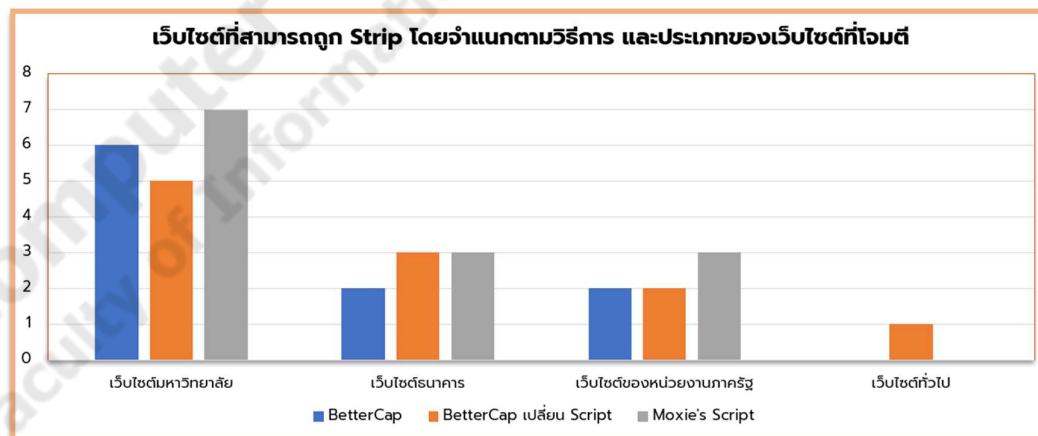
```

ภาพประกอบที่ 4.22 ผล test กระทบวงดิจิทัลเพื่อเศรษฐกิจ และสังคมสามารถ Sniff ได้

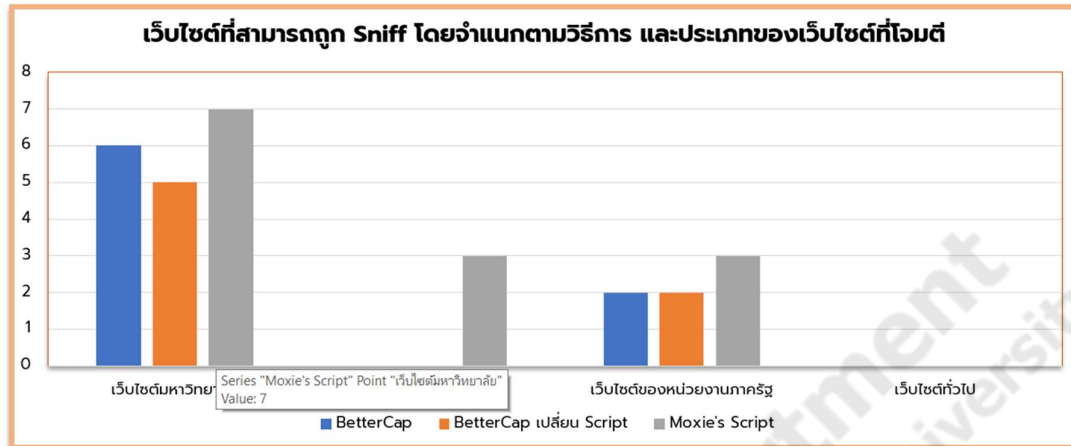
ตารางที่ 4.12 เว็บไซต์ทั่วไป

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

#### 4.2 เที่ยบผลการทดสอบ



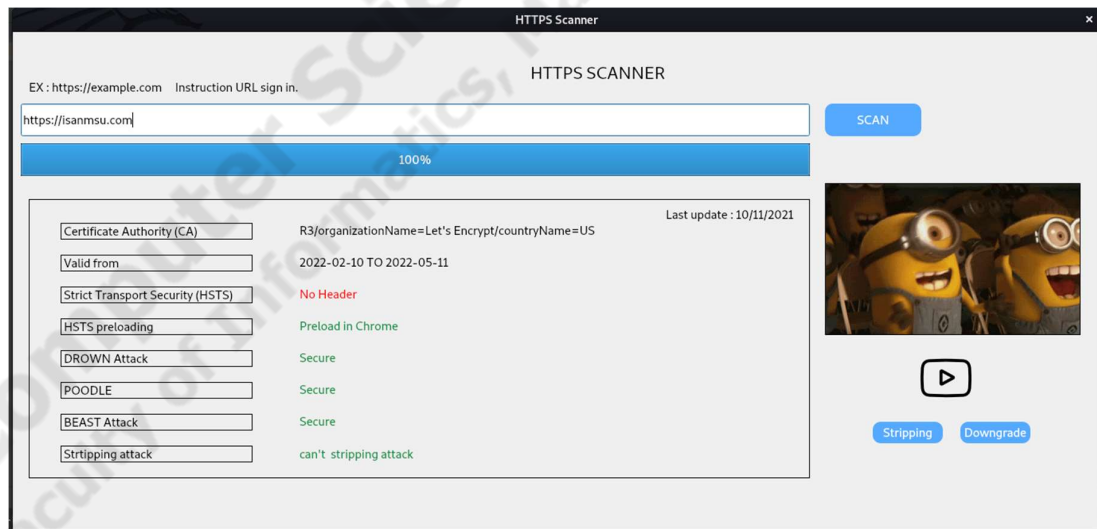
ภาพประกอบที่ 4.23 เว็บไซต์ที่สามารถ Strip ได้ จำแนกตามวิธีการโจมตี และประเภทของเว็บไซต์



ภาพประกอบที่ 4.24 เว็บไซต์ที่สามารถ Sniff ได้ จำแนกตามวิธีการโจมตี และประเภทของเว็บไซต์

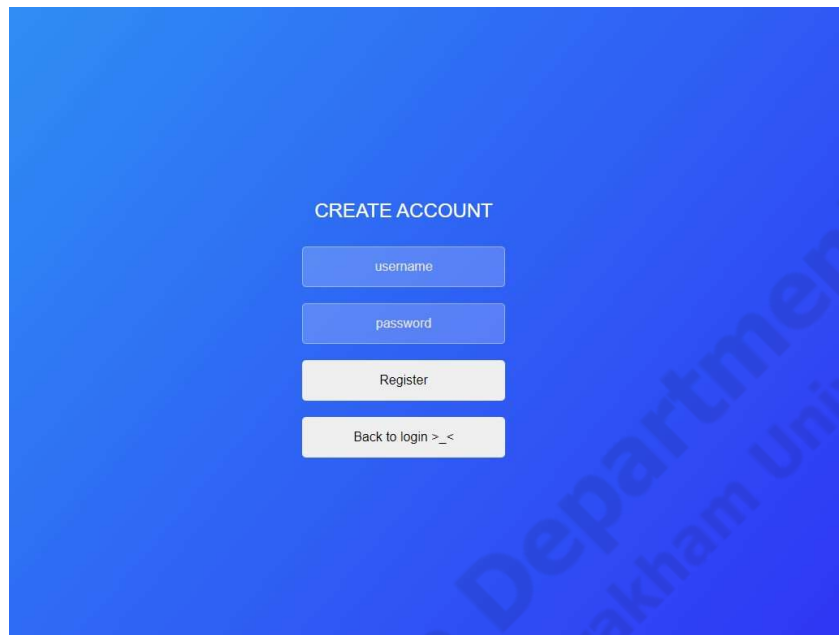
จากภาพประกอบที่ 4.23 และภาพประกอบที่ 4.24 ผลการทดสอบการโจมตี เห็นได้ชัดว่าการโจมตีของ Moxie Marlinspike มีประสิทธิภาพในการโจมตีมากที่สุดที่ใช้การโจมตี SSL Stripping Attack

#### 4.3 ผลการตรวจสอบการป้องกันกับเว็บไซต์อื่น ๆ



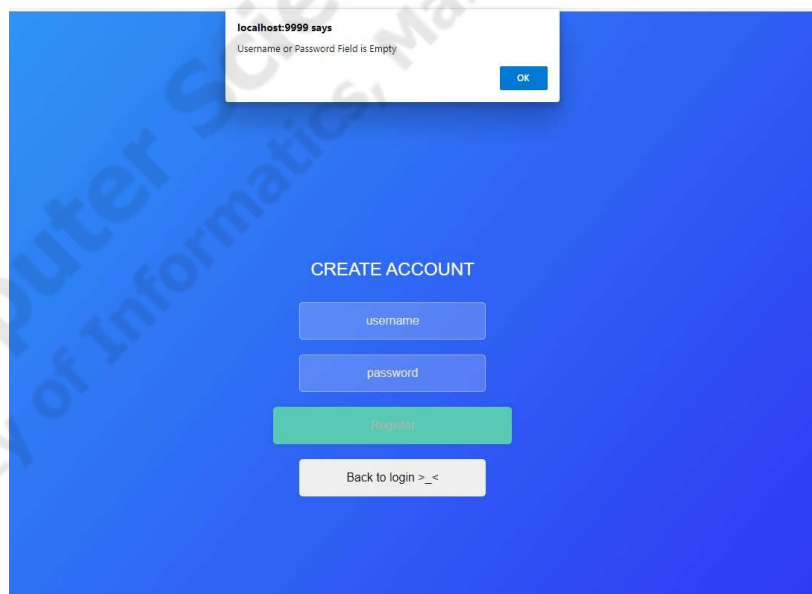
ภาพประกอบที่ 4.25 ตัวอย่างแสดงผลการสแกนความปลอดภัยของเว็บไซต์

#### 4.4 ทดสอบหน้าล็อกอิน Salted – Hash Password



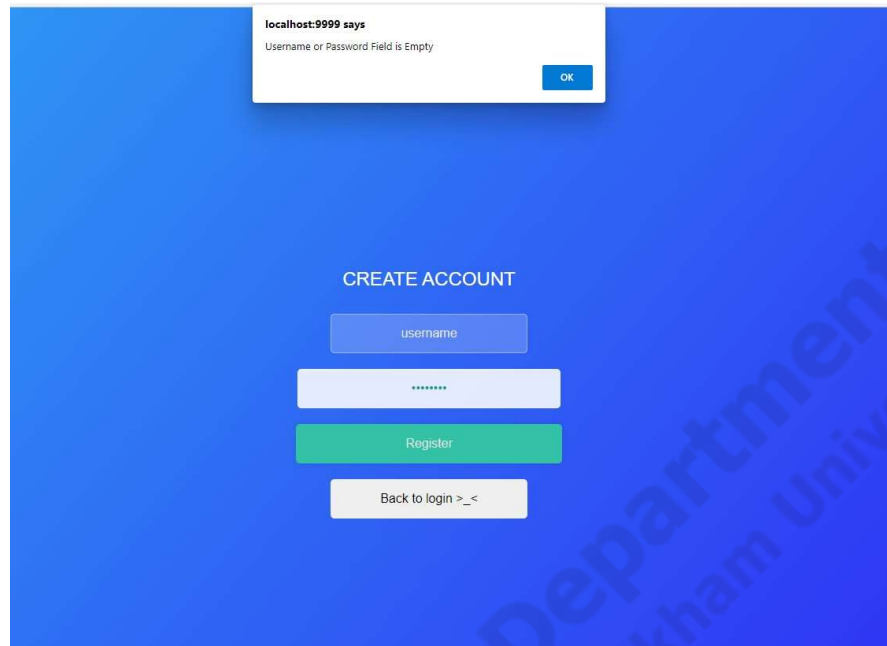
A screenshot of a web application's registration page. The background is a solid blue color. At the top center, the text "CREATE ACCOUNT" is displayed in white. Below this, there are four input fields stacked vertically: "username", "password", "Register", and "Back to login >\_<". The "Register" button is highlighted in a light gray color, while the others are in a light blue color.

ภาพประกอบที่ 4.26 ตัวอย่างหน้า Register

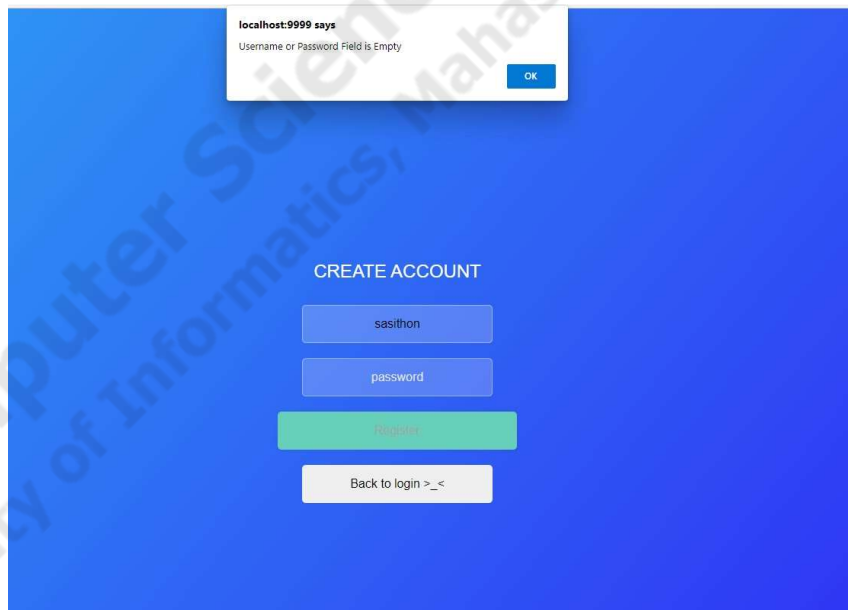


A screenshot of the same registration page as in Figure 4.26, but with an error message displayed. The error message is a white box with a blue border, containing the text "localhost:9999 says" and "Username or Password Field is Empty". Below the error message, the "Register" button is highlighted in a light green color, indicating it is the source of the error.

ภาพประกอบที่ 4.27 หน้า Register กรณีที่ไม่กรอกข้อมูลในการลงทะเบียน

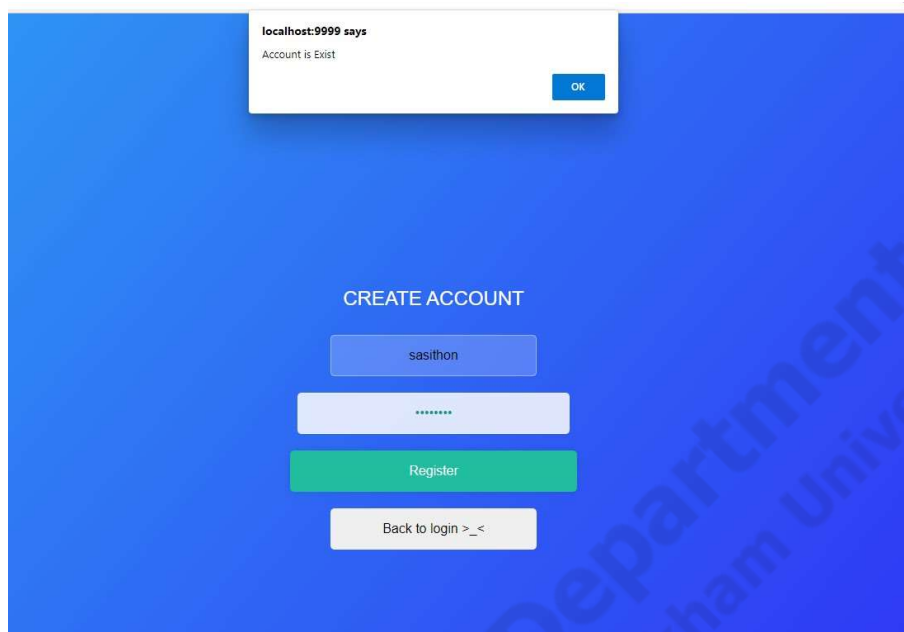


ภาพประกอบที่ 4.28 หน้า Register กรณีไม่กรอก Username ในการลงทะเบียน

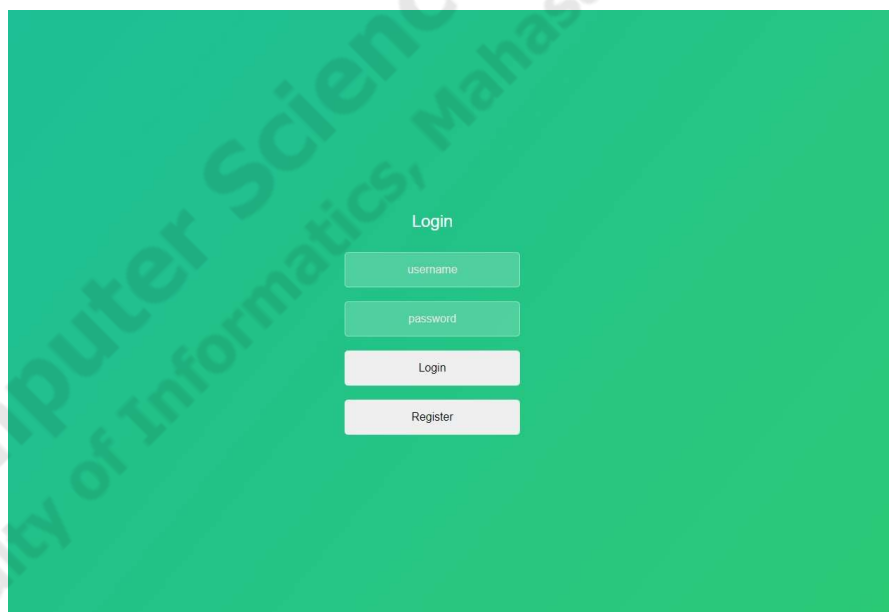


ภาพประกอบที่ 4.29 หน้า Register กรณีไม่กรอก Password ในการลงทะเบียน

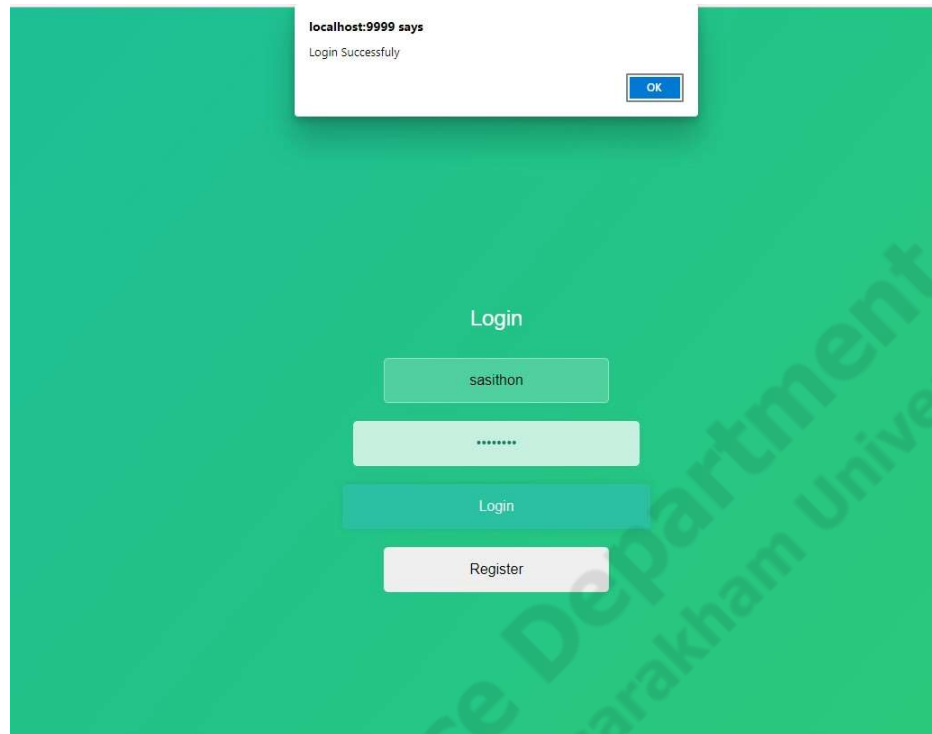




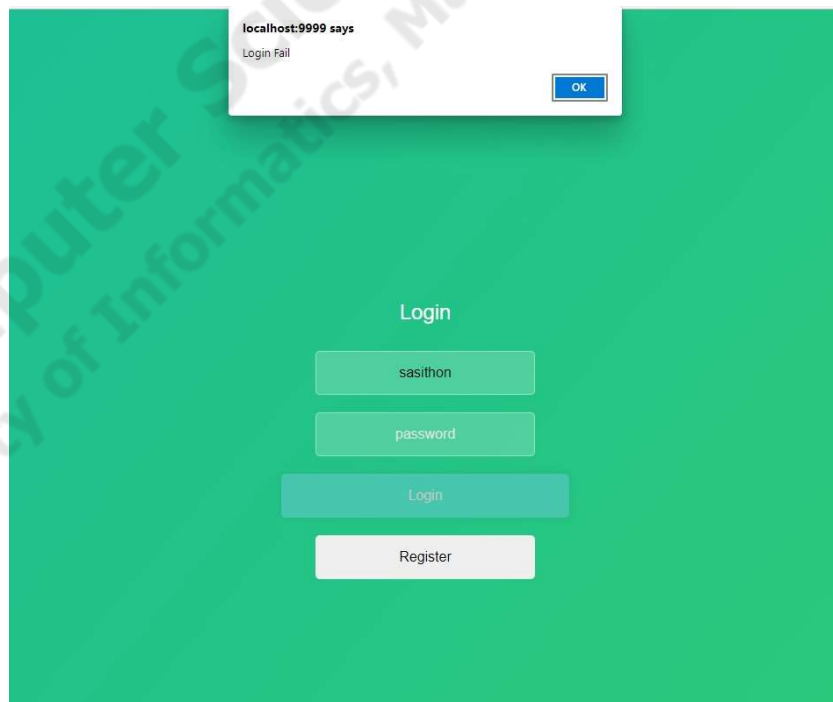
ภาพประกอบที่ 4.30 หน้า Register กรณีกรอกข้อมูล Username ที่มีอยู่ในฐานข้อมูล



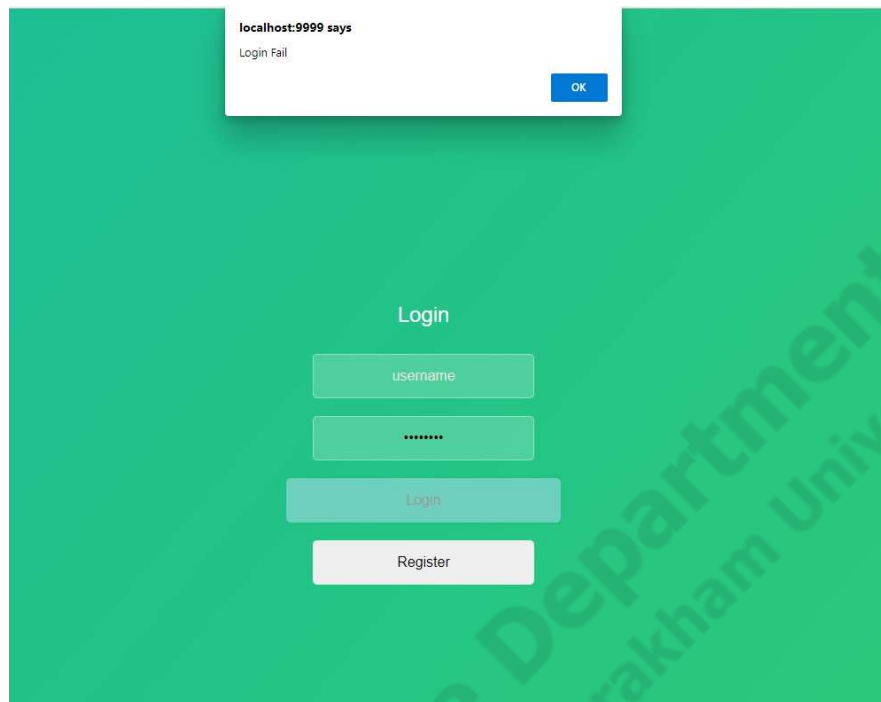
ภาพประกอบที่ 4.31 กรณีลงทะเบียนสำเร็จจะรีเทิร์นกลับมาที่หน้าล็อกอิน



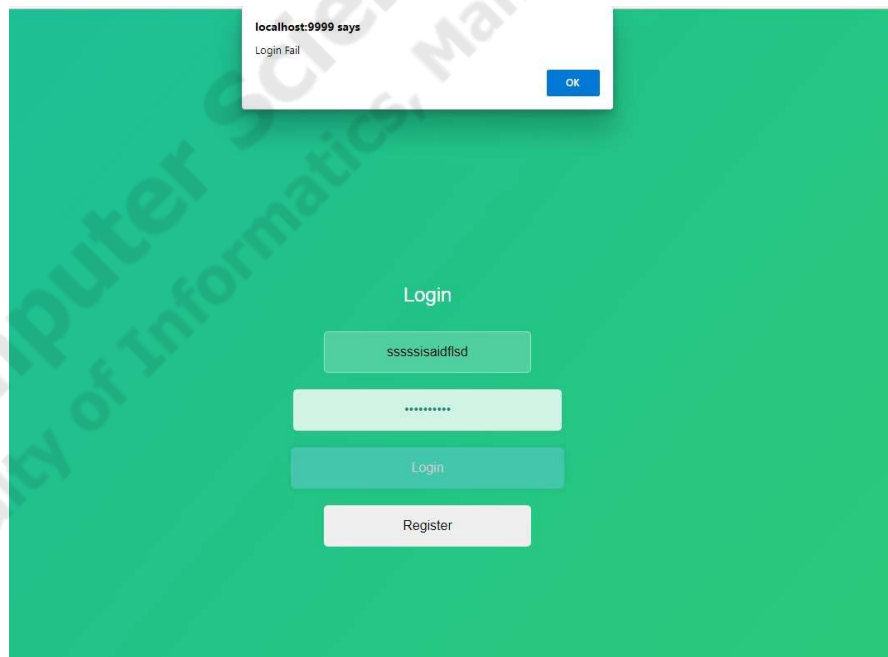
ภาพประกอบที่ 4.32 หน้าล็อกอินกรณีล็อกอินสำเร็จ



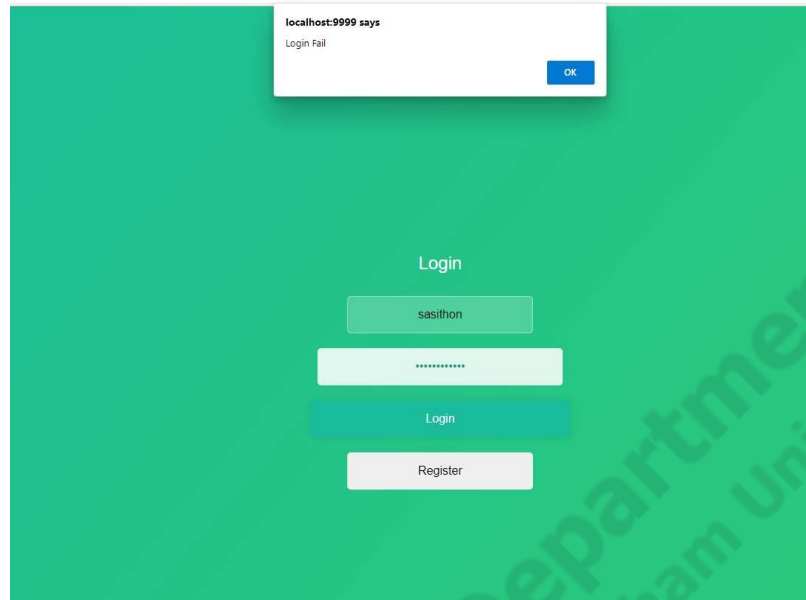
ภาพประกอบที่ 4.33 หน้าล็อกอินกรณีไม่กรอก Password



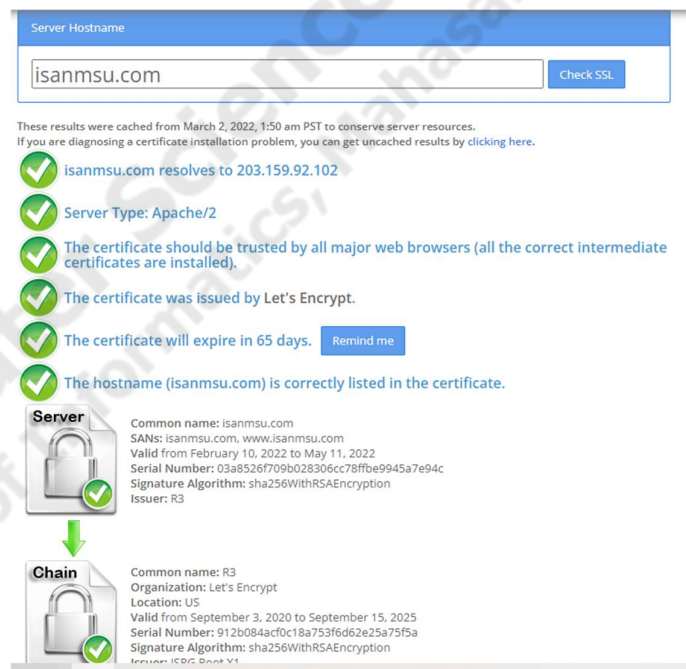
ภาพประกอบที่ 4.34 หน้าล็อกอิน กรณีไม่กรอก Username



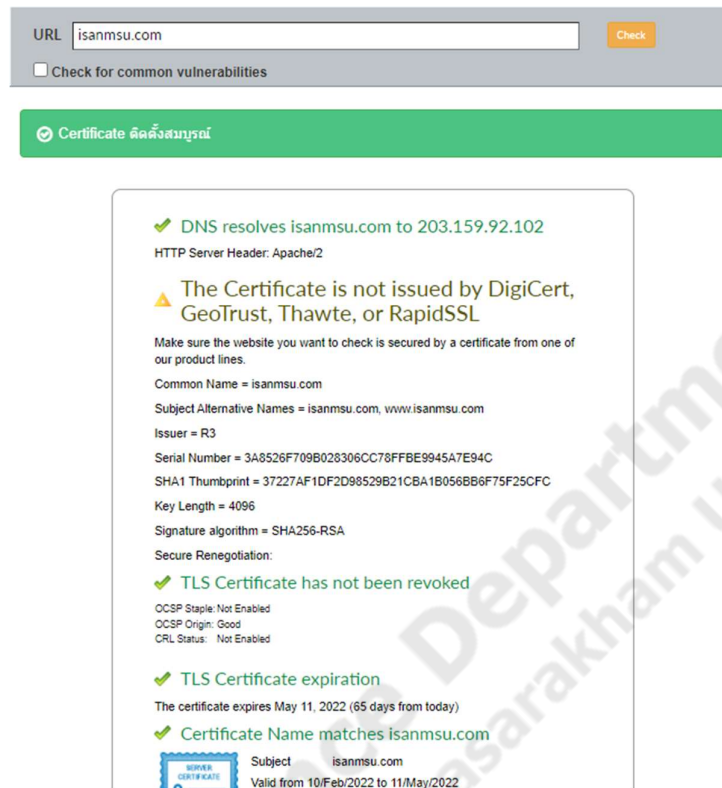
ภาพประกอบที่ 4.35 หน้าล็อกอิน กรณีกรอกข้อมูลผิด



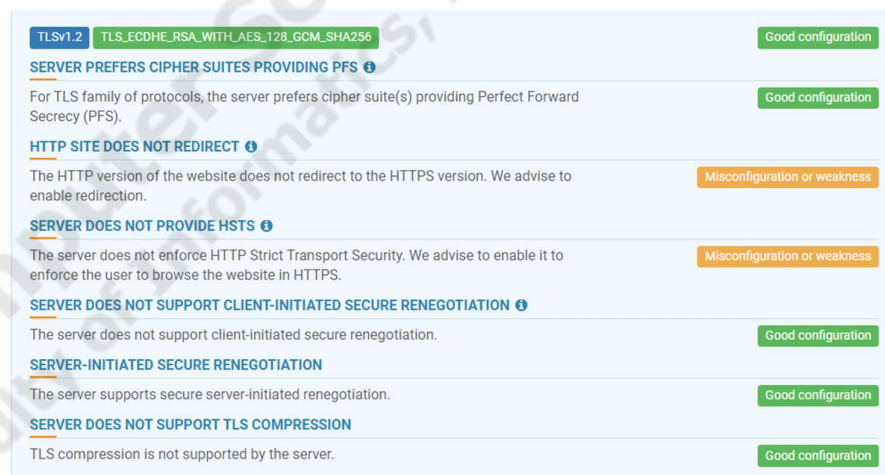
ภาพประกอบที่ 4.36 หน้าล็อกอิน กรณีกรอก 'or '1' = 1' (inject key) ที่ Password



ภาพประกอบที่ 4.37 ตัวอย่างการสแกน SSL จากเว็บไซต์ [SSL Checker](#)



ภาพประกอบที่ 4.38 ตัวอย่างการเสกนจาก เว็บไซต์ SSL Checker



ภาพประกอบที่ 4.39 ตัวอย่างการทดสอบจากเว็บไซต์

[[isanmsu.com SSL Security Test \(immunivweb.com\)](#)]

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

chromium/#hsts และได้ทำการนำเอา Preload ออกจาก Header หากทางเว็บไซต์ไหนที่มีการเช็ค แต่ที่ Header แล้วให้คำตอบว่า 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](#)

Computer Science Department  
Faculty of Informatics, Maharakham University