

บทที่ 4

การทดสอบระบบ

การทดสอบระบบ (Testing System) เป็นการทดสอบกระบวนการการทำงานของระบบเพื่อทำการทดสอบการใช้งานเว็บไซต์ ซึ่งได้ทำการพัฒนาจนเสร็จสมบูรณ์ เพื่อให้ทราบถึง กระบวนการทำงานของระบบว่าสามารถทำงานในแต่ละฟังก์ชันได้อย่างถูกต้อง และให้ผลลัพธ์ตามที่ ต้องการหรือไม่ โดยมีการนำข้อมูลไปยังระบบเพื่อให้ทำงานและแสดงผลหรือออกมาโดยใช้ฟังก์ชันในส่วนต่าง ๆ ของระบบในการทดสอบดังนี้

4.1 การทดสอบระบบเว็บไซต์ WorayuthIT

เว็บไซต์ WorayuthIT จะมีผู้ใช้หลายประเภท โดยแบ่งกลุ่มผู้ใช้งาน ออกเป็น 8 กลุ่ม คือ ผู้ดูแลระบบ บรรณาธิการ ผู้เขียน ผู้ร่วมเขียน สมาชิก ผู้สอน ผู้เรียน และผู้ใช้งานทั่วไป การทดสอบเว็บไซต์ WorayuthIT ในส่วนของฟังก์ชันการทำให้สำคัญต่าง ๆ ดังนี้

ตารางที่ 4.1 ทดสอบการเข้าสู่ระบบ

ทดสอบ	ข้อมูลนำเข้า	ผลลัพธ์ที่ได้	ผลการทดสอบ					
			Admin	Editor	Author	Contributor	Instructor	Subscriber
1	Step 1 กรอก Username หรือ Email ถูกต้อง	ไปหน้ากรอก Password ได้	/	/	/	/	/	/
	Step 2 กรอก Password ถูกต้อง	เข้าสู่ระบบได้	/	/	/	/	/	/
2	Step 1 กรอก Username หรือ Email ไม่ถูกต้อง	ไปหน้ากรอก Password ได้	/	/	/	/	/	/
3	Step 1 กรอก Username หรือ Email ถูกต้อง	ไปหน้ากรอก Password ได้	/	/	/	/	/	/
	Step 2 กรอก Password ไม่ถูกต้อง	เข้าสู่ระบบไม่ได้/มีข้อความแจ้งเตือน	/	/	/	/	/	/
4	ไม่กรอก ทั้ง Username และ Password	เข้าสู่ระบบไม่ได้/มีข้อความแจ้งเตือน	/	/	/	/	/	/

ตารางที่ 4.2 ทดสอบการเข้าสู่ระบบด้วย Two-Factor Authentication TOTP

ทดสอบ	ข้อมูลนำเข้า	ผลลัพธ์ที่ได้	ผลการทดสอบ					
			Admin	Editor	Author	Contributor	Instructor	Subscriber
1	Step 1 กรอก Username หรือ Email ถูกต้อง	ไปหน้า กรอก Password ได้	/	/	/	/	/	/
	Step 2 กรอก Password ถูกต้อง Step 3 กรอก OPT ถูกต้อง	เข้าสู่ระบบได้/มี ข้อความแจ้งเตือน	/	/	/	/	/	/
2	Step 1 กรอก Username หรือ Email ไม่ถูกต้อง	ไปหน้ากรอก Password ไม่ได้	/	/	/	/	/	/
3	Step 1 กรอก Username หรือ Email ถูกต้อง	ไปหน้า กรอก Password ได้	/	/	/	/	/	/
	Step 2 กรอก Password ไม่ถูกต้อง Step 3 กรอก OPT ถูกต้อง	เข้าสู่ระบบไม่ได้/มี ข้อความแจ้งเตือน	/	/	/	/	/	/
4	ไม่ กรอก ทั้ง Username และ Password	เข้าสู่ระบบไม่ได้/มี ข้อความแจ้งเตือน	/	/	/	/	/	/
5	Step 1 กรอก Username หรือ Email ถูกต้อง	ไปหน้ากรอก Password และ OTP ได้	/	/	/	/	/	/
	Step 2 กรอก Password ถูกต้อง Step 3 กรอก OPT ไม่ถูกต้อง	เข้าสู่ระบบไม่ได้/มี ข้อความแจ้งเตือน	/	/	/	/	/	/

ตารางที่ 4.3 ทดสอบการสมัครสมาชิก

ทดสอบ	ข้อมูลนำเข้า	ผลลัพธ์ที่ได้
1	กรอกข้อมูลและรูปแบบถูกต้องทั้งหมด	สมัครสมาชิกสำเร็จ
2	กรอกรูปแบบ Email ไม่ถูกต้อง หรือ Email ซ้ำ	สมัครสมาชิกไม่สำเร็จ
3	กรอก Username ไม่ครบหรือน้อยกว่า 6 ตัวอักษร	สมัครสมาชิกไม่สำเร็จ
4	กรอกรูปแบบรหัสผ่านไม่ถูกต้องตามรูปแบบที่กำหนด	สมัครสมาชิกไม่สำเร็จ
5	ไม่ยืนยัน Recaptcha	สมัครสมาชิกไม่สำเร็จ
6	ไม่ใส่ข้อมูล	สมัครสมาชิกไม่สำเร็จ

ตารางที่ 4.4 ทดสอบการขอยืนยันบัญชี

ทดสอบ	ข้อมูลนำเข้า	ผลลัพธ์ที่ได้
1	ป้อน Email และ ยืนยัน reCaptcha ถูกต้อง	ส่ง Link ไปยัง Email เพื่อเปลี่ยนยืนยันบัญชี
2	ป้อน Email ไม่ถูกต้อง	ไม่พบข้อมูล
3	ป้อน Email ถูกต้อง ไม่ยืนยัน Recaptcha	ต้องยืนยัน Recaptcha

ตารางที่ 4.5 ทดสอบการใช้งาน TOTP 2FA

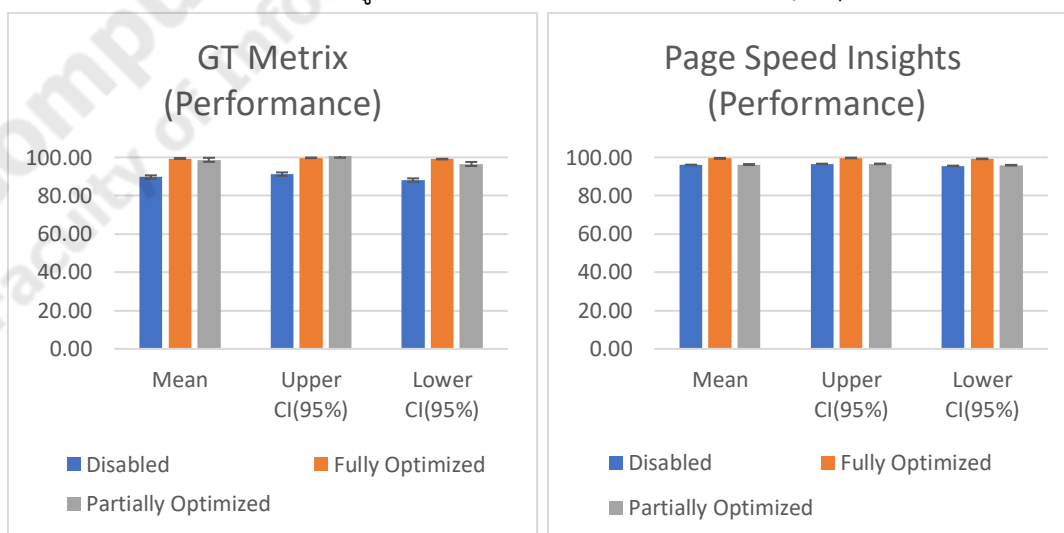
ทดสอบ	ข้อมูลนำเข้า	ผลลัพธ์ที่ได้
1	Step 1 แสกน QR Code โดยใช้ Authy	สำเร็จ แสดงหมายเลข OTP และชื่อผู้ใช้ใน Authy
2	Step 1 ป้อน Secret Key โดยใช้ Authy	สำเร็จ แสดงหมายเลข OTP และชื่อผู้ใช้ใน Authy
3	Step 2 ป้อน OTP ถูกต้อง	เปิด/ปิดใช้งาน 2FA ได้
4	Step 2 ป้อน OTP ไม่ถูกต้อง	เปิด/ปิดใช้งาน 2FA ไม่ได้
5	Step 2 ไม่กรอก OTP	เปิด/ปิดใช้งาน 2FA ไม่ได้

4.2 สรุปผลการทดสอบประสิทธิภาพเว็บไซต์ worayuthit.com

ตารางที่ 4.6 ตารางเปรียบเทียบประสิทธิภาพ

รายการ	GTMetrix			PageSpeed Insights		
	Disabled	Optimize	Partially Optimize Fully	Disable	Optimize	Partially Optimize Fully
Mean	89.70	98.73	99.43	96.10	96.26	99.47
Standard Error	0.76	1.07	0.16	0.25	0.17	0.11
Confidence Level(95.0%)	1.55	2.18	0.34	0.51	0.35	0.23
Upper CI(95%)	91.25	100.91	99.77	96.61	96.61	99.70
Lower CI(95%)	88.15	96.55	99.10	95.59	95.91	99.23

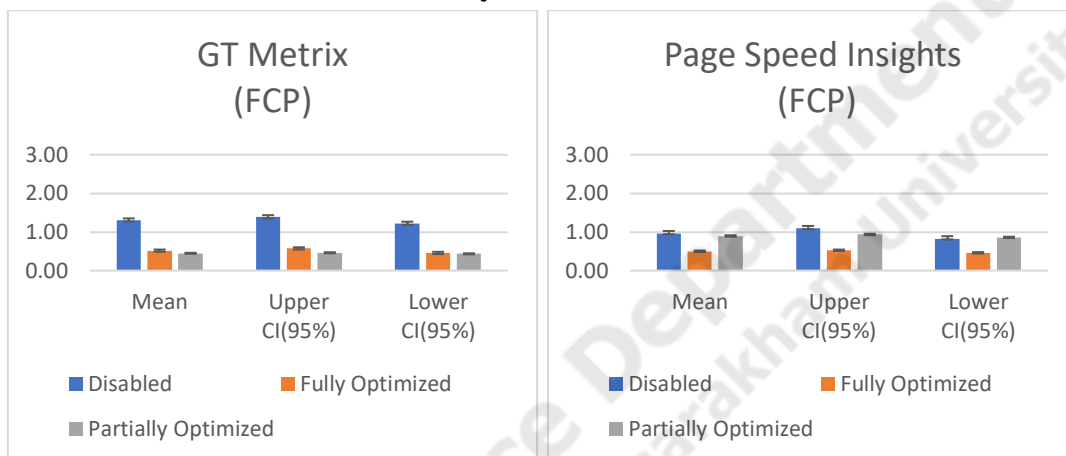
สรุปค่าหลังจากคำนวณ Confidence Level (95.0%) จากตารางข้างต้นสามารถสรุปได้ว่าการปรับปรุง (Optimization) ได้ส่งผลให้ค่า Mean เพิ่มขึ้นอย่างมีนัยสำคัญ และค่า Mean หลังการปรับปรุงมีความเชื่อมั่น 95% อยู่ในช่วง Confidence Interval ที่แตกต่างจากค่า Mean ก่อนการปรับปรุง ดังนั้นสามารถสรุปว่าการปรับปรุงนี้มีผลมากต่อค่า Mean และมีความแตกต่างที่มีนัยสำคัญ ข้อสังเกต หากใช้ Google page speed Insights วัดประสิทธิภาพ Partially Optimized สังเกตเห็นว่า ตัวปลั๊กอินไม่ได้ทำงานเต็มที่สมบูรณ์จึงทำให้คะแนนที่ได้ต่ำกว่าตัว Fully Optimized



ภาพประกอบที่ 4.1 ผลสรุปค่าความเชื่อมั่น Performance

สรุปผลโดยหน่วยเป็นคะแนน (Score) ซึ่งค่า Disabled กับค่า Fully Optimized จะเห็นว่าค่าคะแนนของ Fully Optimized สูงกว่า Disabled อย่างเห็นได้ชัด แสดงว่าหลังจากทำการ Fully Optimized แล้วทำให้คะแนนเพิ่มขึ้น แตกต่างอย่างเห็นได้ชัด รวมถึง Partially Optimized ด้วยในส่วนของ GTmetrix

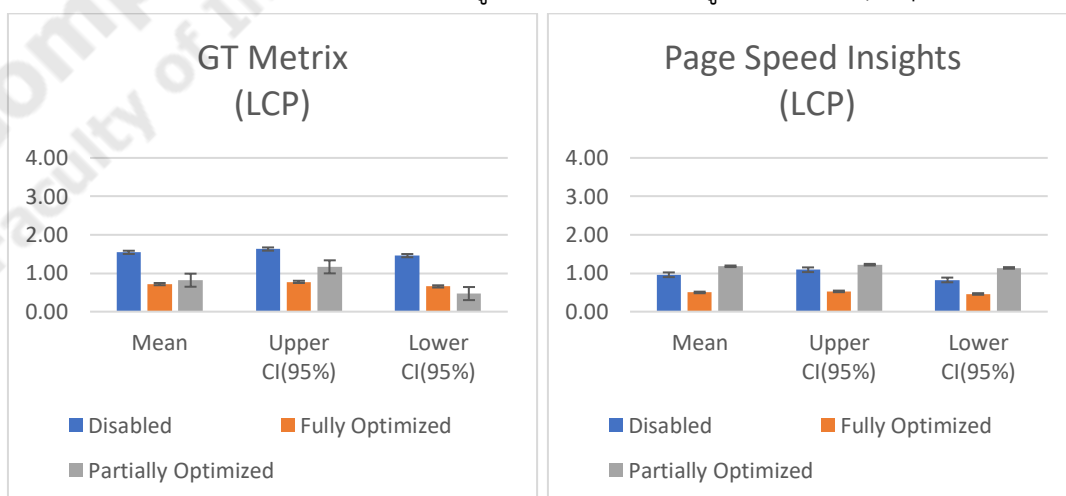
ข้อสังเกต หากใช้ Google page speed Insights วัดประสิทธิภาพ Partially Optimized สังเกตเห็นว่า ตัวปลั๊กอินไม่ได้ทำงานเต็มที่สมบูรณ์จึงทำให้คะแนนที่ได้ต่ำกว่า Fully Optimized



ภาพประกอบที่ 4.2 ผลสรุปค่าความเชื่อมั่น FCP

สรุปผลโดยหน่วยเป็นวินาที ซึ่งค่า Disabled กับค่า Fully Optimized จะเห็นว่าค่า Fully Optimized ต่ำกว่า Disabled อย่างเห็นได้ชัด แสดงว่าหลังจากทำการ Fully Optimized แล้วทำให้ลดเวลาที่ใช้ในการโหลดเนื้อหาแรกบนหน้าเว็บ แตกต่างอย่างเห็นได้ชัด รวมถึง Partially Optimized ด้วยในส่วนของ GTmetrix

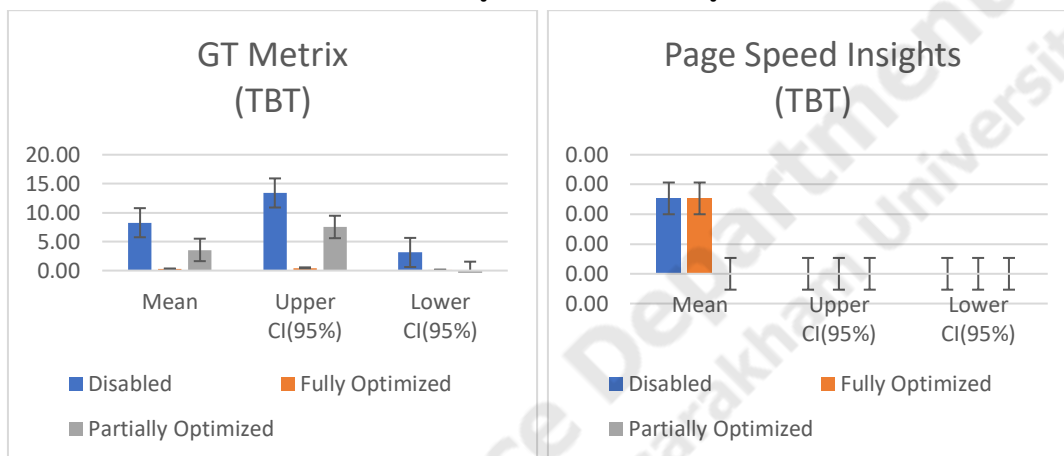
ข้อสังเกต หากใช้ Google page speed Insights วัดประสิทธิภาพ Partially Optimized สังเกตเห็นว่า ตัวปลั๊กอินไม่ได้ทำงานเต็มที่สมบูรณ์เลยทำให้ค่าที่ได้สูงกว่าตัว Fully Optimized



ภาพประกอบที่ 4.3 ผลสรุปค่าความเชื่อมั่น LCP

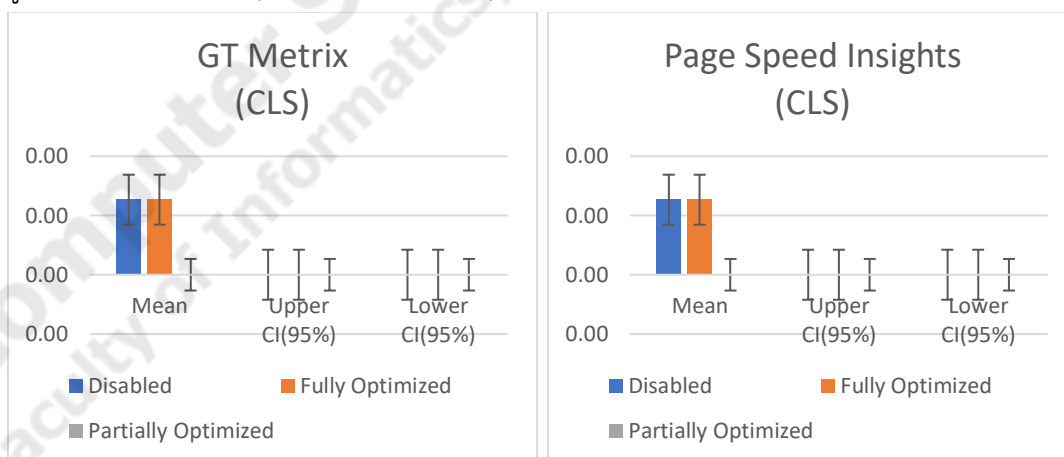
สรุปผลโดยหน่วยเป็น วินาที (Sec) ซึ่งค่า Disabled กับค่า Fully Optimized จะเห็นว่าค่า Fully Optimized ต่ำกว่า Disabled อย่างเห็นได้ชัด แสดงว่าหลังจากทำการ Fully Optimized แล้ว ทำให้ลดเวลาที่ใช้ในการโหลดเนื้อหาที่ใหญ่ที่สุดบนหน้าเว็บเร็วขึ้นเห็นได้ชัด รวมถึง Partially Optimized ด้วยในส่วนของ GTmetrix

ข้อสังเกต หากใช้ Google page speed Insights วัดประสิทธิภาพ Partially Optimized จะสังเกตเห็นว่า ตัวปลั๊กอินไม่ได้ทำงานเต็มที่สมบูรณ์เลยทำให้ค่าที่ได้สูงกว่าตัว Fully Optimized



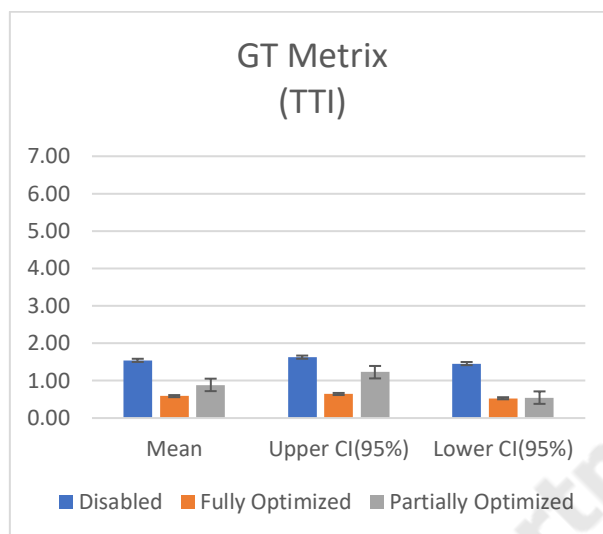
ภาพประกอบที่ 4.4 ผลสรุปค่าความเชื่อมั่น TBT

สรุปผลโดยหน่วยเป็นมิลลิวินาที (ms) ซึ่งเว็บไซต์ไม่ได้มีการบล็อกหน้าเว็บ จึงทำให้ค่าที่ได้มาไม่สูง หรือมีค่าน้อยมาก ๆ ในส่วนของ Page Speed Insights ที่แทบหาความแตกต่างไม่เจอ



ภาพประกอบที่ 4.5 ผลสรุปค่าความเชื่อมั่น CLS

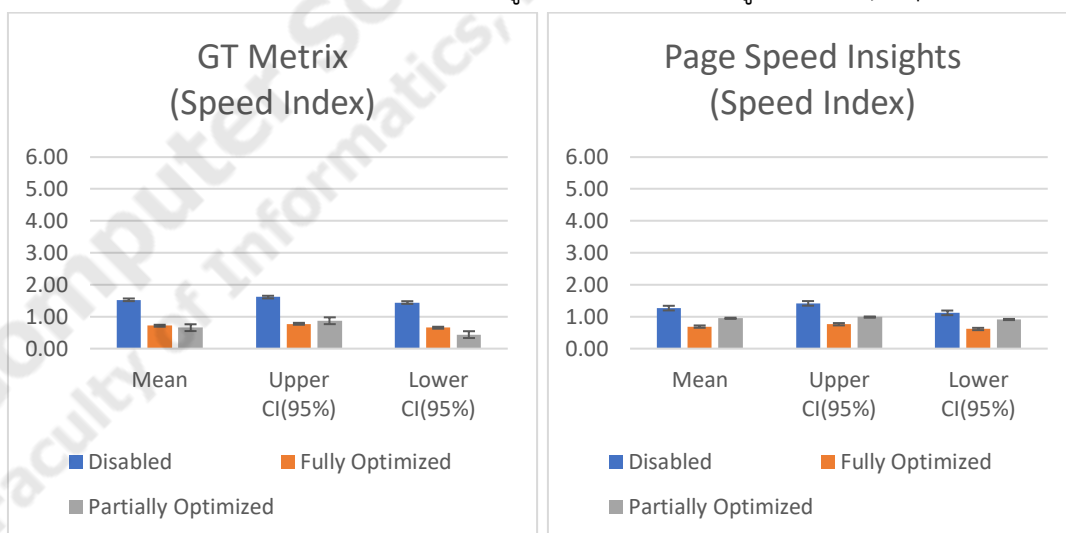
สรุปผลโดยหน่วยเป็นวินาที (sec) ซึ่งเว็บไซต์ไม่ได้มีการบล็อกหน้าเว็บ จึงทำให้ค่าที่ได้น้อยมาก ๆ ใน Disabled และ Fully Optimized, Partially Optimized นั้นไม่มีค่าเลย ทั้งใน GTmetrix และ Google Page Speed Insights



ภาพประกอบที่ 4.6 ผลสรุปค่าความเชื่อมั่น TTI

สรุปผลโดยหน่วยเป็นวินาที (Sec) ซึ่งค่า Disabled กับค่า Fully Optimized จะเห็นว่าค่า Fully Optimized ต่ำกว่า Disabled อย่างเห็นได้ชัด แสดงว่าหลังจากทำการ Fully Optimized แล้ว ทำให้ลดเวลาที่ใช้ในการทำให้หน้าเว็บเป็นแอคทีฟและปรากฏผลสามารถใช้ได้จริง เร็วขึ้นเห็นได้ชัด รวมถึง Partially Optimized

ข้อควรสังเกต Partially Optimized ในส่วนของ GTmetrix มีค่าที่สูงกว่า Fully Optimized อาจจะเป็นเพราะว่าปลั๊กอินไม่ได้ทำงานอย่างสมบูรณ์ ทำให้แสดงค่าที่สูงกว่า Fully Optimized



ภาพประกอบที่ 4.7 ผลสรุปค่าความเชื่อมั่น Speed Index

โดยให้หน่วยเป็น วินาที (Sec) จากกราฟ Disabled vs Fully Optimized จะเห็นว่าค่า Fully Optimized ต่ำกว่า Disabled อย่างเห็นได้ชัด แสดงว่าหลังจากทำการ Fully Optimized แล้วทำให้ลดความเร็วในการแสดงเนื้อหาบนหน้าเว็บ เป็นค่าที่วัดความเร็วในการโหลดและแสดงเนื้อหา เร็วขึ้นเห็นได้ชัดรวมถึง Partially Optimized ด้วยในส่วนของ GTmetrix

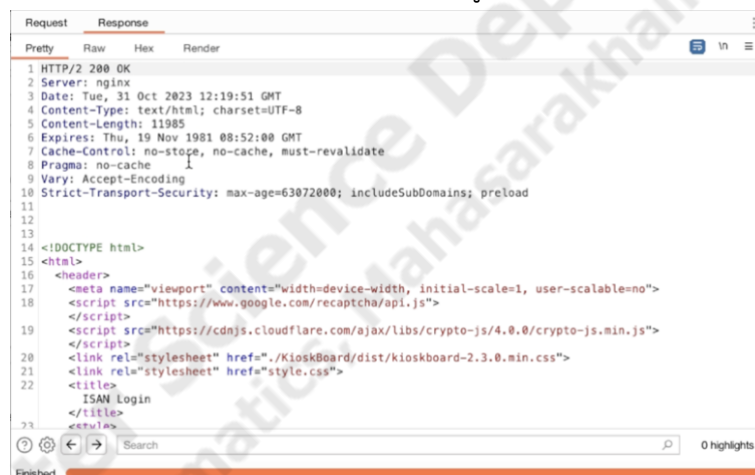
ข้อควรสังเกต หากใช้ Google page speed Insights วัดประสิทธิภาพ Partially Optimized จะสังเกตเห็นว่า ตัวบ่งชี้กินไม่ได้ทำงานเต็มที่สมบูรณ์เลยทำให้ค่าที่ได้สูงกว่าตัว Fully Optimized

4.3 สรุปผลการทดสอบความมั่นคงเว็บไซต์ worayuthit.com

4.3.1 ผลการทดสอบ Brute-force attack หน้าเข้าสู่ระบบ

จากการทดสอบการโจมตีด้วย Brute-force attack ผลการโจมตีจะไม่สำเร็จได้หาก reCAPTCHA ถูกเปิดใช้งานอยู่ โดยการโจมตีได้สำเร็จนั้นต้องปิดการใช้งาน reCAPTCHA และชื่อผู้ใช้งานรหัสผ่าน และอัลกอริทึมถูกต้อง โดยมีรายละเอียดดังนี้

(1) ผลการทดสอบการ Brute-force รหัสผ่านนี้ ถึงแม้จะปิดใช้งาน reCAPTCHA และมีการใช้ชื่อบัญชีผู้ใช้งานถูกต้อง แต่ใช้รหัสผ่าน Plain text จะไม่สามารถดำเนินโจมตีให้สำเร็จได้ และจะตอบกลับด้วยหน้าที่มีการกำหนดไว้ให้ไปเมื่อการเข้าสู่ระบบล้มเหลว

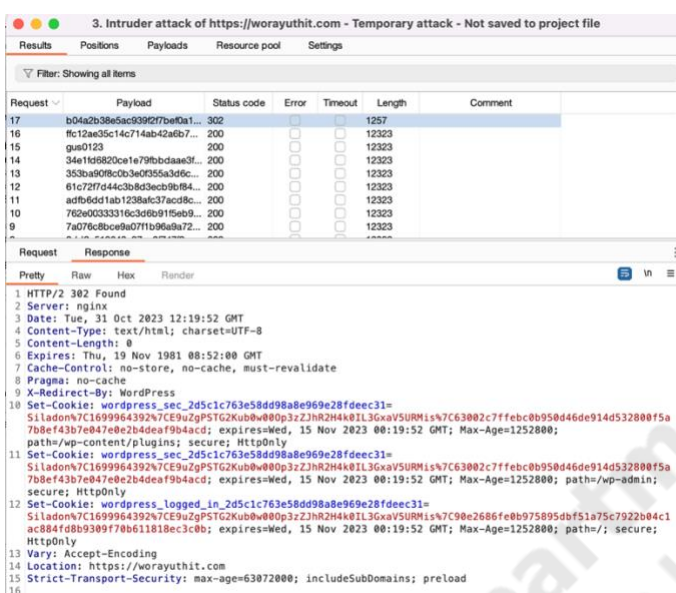


ภาพประกอบที่ 4.8 ผล Response จากการทดสอบด้วย Plain text

(2) ผลที่ได้นี้ หากใช้งานชื่อผู้ใช้งานที่ถูกต้องและรหัสผ่านที่มีการใช้งานอัลกอริทึมการเข้ารหัส (hash) ที่ถูกต้อง ซึ่งคือนำชื่อผู้ใช้งานด้วยรหัสผ่านและเข้ารหัสด้วยอัลกอริทึม SHA512 สองครั้ง จึงจะสามารถดำเนินการสำเร็จได้

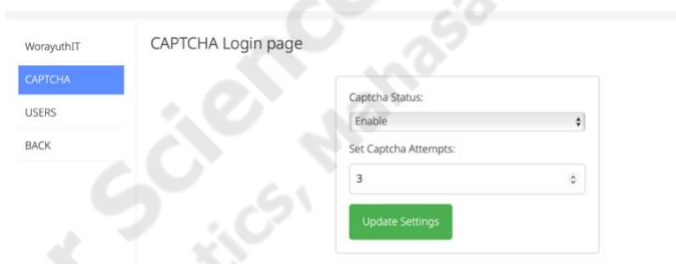


ภาพประกอบที่ 4.9 กำหนดรายการรหัสผ่านที่เข้ารหัสด้วย SHA512

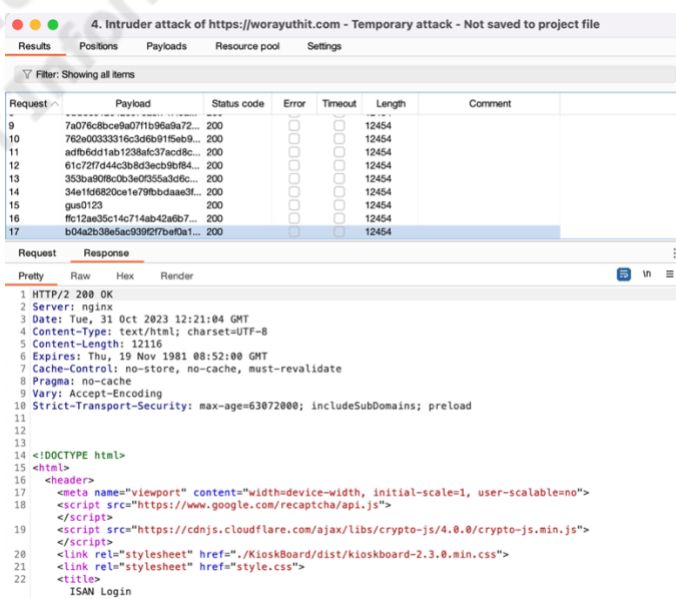


ภาพประกอบที่ 4.10 ผล Response จากการทดสอบด้วยรหัสผ่านที่เข้ารหัส 1

(3) ทดสอบด้วยการเปิดการใช้งาน reCAPTCHA ในหน้าเข้าสู่ระบบ เพื่อทดสอบหน้าเข้าสู่ระบบ โดยมีการใช้งาน reCAPTCHA ในการป้องกัน



ภาพประกอบที่ 4.11 เปิดการใช้งาน reCAPTCHA หน้าเข้าสู่ระบบ



ภาพประกอบที่ 4.12 ผล Response จากการทดสอบด้วยรหัสผ่านที่เข้ารหัส 2

4.3.2 ผลการทดสอบ SSL Strip Attack หน้าเข้าสู่ระบบ

- (1) ผลการโจมตีของหน้าเข้าสู่ระบบ

```
log=Gus01234&pwd=gus0123&wp-submit=Log In&redirect_to=http://w
```

ภาพประกอบที่ 4.13 หน้าเข้าสู่ระบบ WordPress

- (2) ผลการโจมตีหน้าเข้าสู่ระบบ โดยมีการป้องกันผ่านด้วยการเข้ารหัส

```
user_login=Gus01234&otpstatus=8&login_submission=8&password=8044725507109w02005445200fcee3fa02085f6c870a346872  
7001fAecc55cc0fba31252a08380d00a0f730c927cc75a70dc295f006f90a30c3c3d8
```

ภาพประกอบที่ 4.14 หน้าเข้าสู่ระบบ ISAN ป้องกันด้วยการเข้ารหัส

การใช้ ISAN-login.php แทน wp-login.php (default) เป็นวิธีที่ดีเพื่อป้องกันการโจมตี SSL Strip Attack โดยทำให้ยากต่อผู้ไม่ประสงค์ดีในการเข้าถึงข้อมูลการเข้าสู่ระบบของผู้ใช้ แม้จะสามารถสร้างการโจมตี SSL Strip Attack ได้แต่ยากในการถอดรหัสผ่านที่ถูก hash ไว้

ตารางที่ 4.7 แสดงผลสรุปการทดสอบความปลอดภัยเว็บไซต์ worayuthit.com

ประเภทการโจมตี	ระบบที่ใช้ในการทดสอบ	ผลจากการทดสอบ
Brute-force attack	wp-login.php (default)	ไม่มีการป้องกัน ทำให้เป็นเป้าหมายง่ายต่อการโจมตีด้วยวิธี Brute-force
	ISAN-login.php	มีการป้องกันด้วย Captcha ซึ่งช่วยลดโอกาสการโจมตี Brute-force
SSL Strip Attack	wp-login.php (default)	ไม่มีการป้องกัน
	ISAN-login.php	มีการป้องกันรหัสผ่านด้วยการ hash ทำให้ยากต่อการถอดรหัสเมื่อ SSL Strip สำเร็จ