**รายละเอียด**

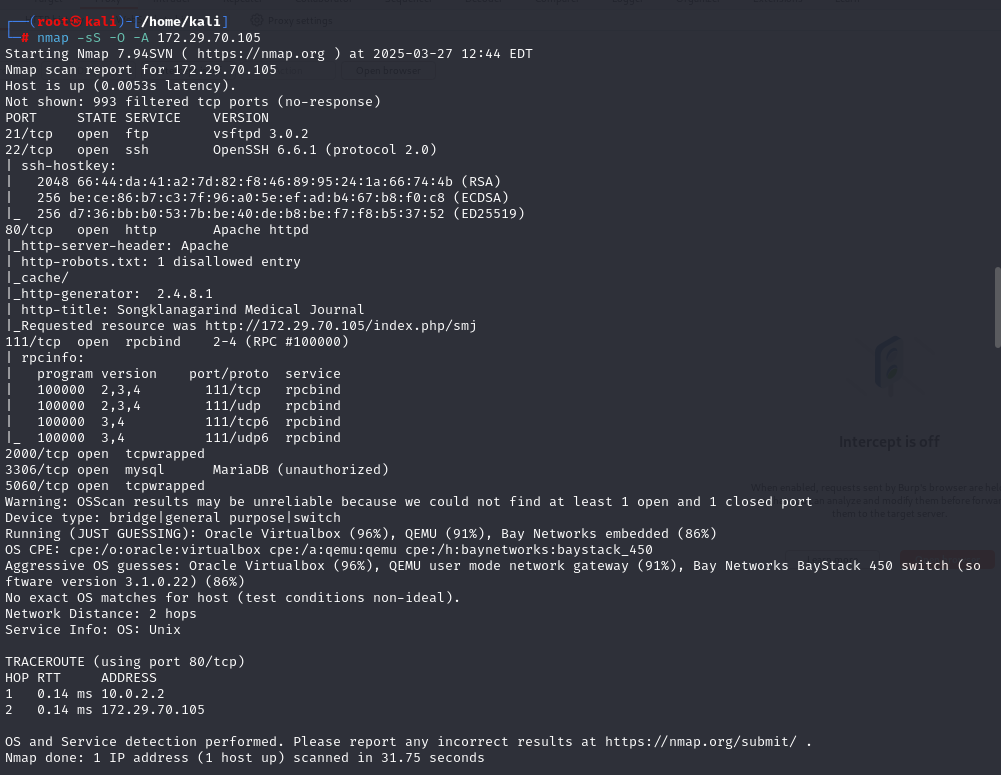
Prince of Songkla University วิทยาเขตปัตตานี

Domain: smj.medicine.psu.ac.th

Public Ip: 202.29.147.116

IPจริง: 172.29.70.105

Server: Apache



**ช่องโหว่1 : CSRF (Cross-Site Request Forgery)**

คำอธิบาย

เว็บที่ปลอดภัยจาก CSRF จะต้องใช้ **CSRF Token** ในฟอร์มทุกครั้งที่มีการส่งข้อมูลสำคัญ เช่น การเข้าสู่ระบบ การเปลี่ยนแปลงข้อมูลส่วนตัว หรือการทำธุรกรรมที่สำคัญ

POST /update-profile HTTP/1.1

Host: yourwebsite.com

Content-Type: application/x-www-form-urlencoded

csrf\_token=unique\_token\_12345 \*\*\*จะต้องมีถึงจะป้องกันได้\*\*\*

[username=new\_user&email=user@example.com](mailto:username=new_user&email=user@example.com)

1.ทดลอง ส่ง ข้อมูลซ้ำ

A screenshot of a computer

AI-generated content may be incorrect.

2.ทดลองลบ **Referer** และ **Origin**

**Referer**: เป็น HTTP header ที่บ่งชี้ว่าผู้ใช้มาจากหน้าเว็บไหนเมื่อทำการร้องขอไปยังเซิร์ฟเวอร์ใหม่ ดังนั้นถ้าลบไปแล้วจะไม่สามารถยืนยันได้ว่าหน้าเว็ปนั้นมาจากหน้าเว็ปที่ถูกต้องไหม เช่น ผู้ใช้เข้ามายังหน้าlogin พอกด reset รหัสผ่าน ก็จะเป็น path ที่เข้ามา ถ้ามันป้องกันได้จริง พอลบไปแล้ว ต้องไม่สามารถ ส่ง request ไปได้

Origin: ตรวจสอบว่ามาจาก web ตัวเองหรือไม่ ใช้ตรวจสอบว่า request นี้มาจากเว็ปอื่นหรือไม่

A screenshot of a computer

AI-generated content may be incorrect.

ระบบยอมรับคำขอจากที่มาแปลกๆหรือไม่คุ้นเคยได้

**ประเภทช่องโหว่**: CSRF (Cross-Site Request Forgery)

**ลิงค์ช่องโหว่:**

<http://smj.medicine.psu.ac.th/index.php/smj/login/requestResetPassword>

<http://smj.medicine.psu.ac.th/index.php/smj/login/signIn>

\*\*มีช่อง search ด้วยแต่คาดว่าไม่ค่อยอันตรายเท่าไหร่

**คำอธิบาย:** เป็นการโจมตีโดยส่ง request ปลอมไปยังเครื่องเป้าหมาย

**วิธีการโจมตี:**

**1.เข้าweb ตาม path ที่โจทตี**

**2.ทำการส่ง request ไปยังserver (กรอกอีเมลล์แล้วกดส่ง)**

**3.ดักจับpakage แล้วส่งไปrepeater**

**4.ลบ origin และ Referer** ออก

**ตัวอย่างการดำเนินการ:**

**http://smj.medicine.psu.ac.th/index.php/smj/login/requestResetPassword**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

[**http://smj.medicine.psu.ac.th/index.php/smj/login/signIn**](http://smj.medicine.psu.ac.th/index.php/smj/login/signIn)

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**ผลกระทบ:** ทำให้คำขออันตรายส่งมายังserver เช่น ผู้ใช้กำลังกรอกข้อมูลลงในเว็ปๆนึง แล้วพอกดส่งข้อมูลนั้นดันมาเข้าเว็บนี้ ทำให้hacker สามารถเข้าสู่ระบบได้

**ระดับความเสี่ยง:** กลาง

**วิธีป้องกัน** จำกัดการส่งได้เพียงบัญชีละหนึ่งครั้ง และระยะการส่งfeedback ต้องเว้นระยะตามที่กำหนด

|  |
| --- |
| OWASP\_2021\_A01 |
| WSTG-v42-SESS-05 |
| OWASP\_2017\_A05 |
| CWE-352 |

**ช่องโหว่2 : Mysql !!!ไม่สำเร็จเนื่องจากFirewall!!**

1.ทดลองเข้า mysql

2.1ใช้ปลั๊กอิน auxiliary/scanner/mysql/mysql\_login เพื่อทดลอง bruce force ปรากฏว่า

A screen shot of a computer

AI-generated content may be incorrect.

\*\*

ทดลอง nmap -Pn -p 3306 172.29.70.105 ปรากฏว่า

A screen shot of a computer

AI-generated content may be incorrect.

ปรากฏว่า state = filtered คือ โดน Firewall ขวางเอาไว้ port นี้ อีกอย่างถึงvpn ได้แต่อยู่คนละsubnet

**ช่องโหว่3 : Vulnerable JS Library !!!ไม่สำเร็จเนื่องจากFirewall**

CVE-2010-5312 , CVE-2011-4117, CVE-2012-6662 เกี่ยวกับการทำ XSS

1. ลองทำ Inject Payload เบื้องต้น ในช่องsearch ปรากฏว่าติด Firewall

"><img src=x onerror=alert(1)>

A screenshot of a computer

AI-generated content may be incorrect.