



# GROUP 12 SlowHttpTest simulate a DOS attack

SC362006 : Information and Communication Technology Security

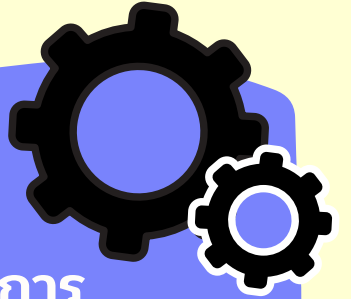


## หลักการและเหตุผล

SlowHttpTest เป็นเครื่องมือที่ใช้ในการโจมตีเว็บไซต์DOSเรียกว่า Denial Of Service ซึ่งจุดประสงค์ทั้งหมดของการโจมตีประเภทนี้คือการปิดบริการ (เซิร์ฟเวอร์) ที่รันโดยพยายามทำให้ใช้งานไม่ได้

## วัตถุประสงค์

1. เพื่อศึกษาวิธีการและหลักการทำงานของ SlowHttpTest
2. นำความรู้ที่ได้จากการศึกษานำไปต่อยอดงานอื่นๆในอนาคต
3. เพื่อศึกษาการการโจมตีเว็บไซต์DOS และ ทดสอบช่องโหว่ DoS

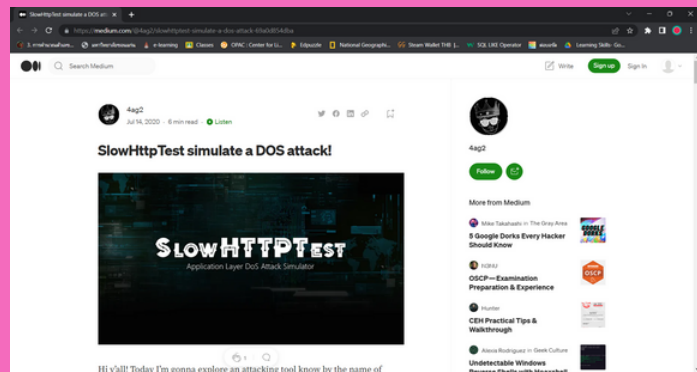


## ทฤษฎีที่เกี่ยวข้อง

การโจมตีแบบ DDoS

การโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (DDoS) มุ่งเป้าเว็บไซต์และเซิร์ฟเวอร์โดยรบกวนบริการของเครือข่าย การโจมตีแบบ DDoS พยายามทำให้ทรัพยากรของแอปพลิเคชันหมดลง ผู้กระทำผิดที่อยู่เบื้องหลังการโจมตีเหล่านี้ทำให้ไซต์มีปริมาณการใช้งานอย่างท่วมท้นผิดปกติ ส่งผลให้การทำงานของเว็บไซต์ไม่ดีหรือทำให้ออฟไลน์โดยสิ้นเชิง

## งานที่เกี่ยวข้อง



medium.com/@4ag2/slowhttpstest-simulate-a-dos-attack-69a0d854dba

## งานที่ทำ

SlowHttpTest เป็นเครื่องมือจำลอง การปฏิเสธการให้บริการ และเครื่องมือสำหรับทดสอบช่องโหว่ DoS โดยมีตัวเลือกต่างๆ อย่างที่สามารถพบได้ในหน้าคู่มือ สามารถติดตั้งได้ง่ายในสภาพแวดล้อม linux ใด ๆ ได้อย่างง่ายดายโดยใช้ตัวจัดการแพ็คเกจ (apt, pacman., etc)

## วิธีการใช้งาน

หลังจากติดตั้งเครื่องมือแล้ว เราสามารถเริ่มใช้งานได้เลย สิ่งที่น่าสนใจคือสามารถรองรับการโจมตีได้ 4 ประเภท: Slowloris , Slow Http Post , Apache Range HeaderและSlow Reader คุณลักษณะอีกอย่างหนึ่งคือสร้างเอาต์พุตเป็นไฟล์csvหรือHTML

## Source code & หน้า Interface

```

slowhttpstest -h
slowhttpstest: a tool to test for slow HTTP DoS vulnerabilities - version 1.6
Usage: slowhttpstest [options]
Test modes:
  -s slow headers a.k.a. Slowloris (default)
  -p slow http post a.k.a. SlowHttpPost
  -r apache range a.k.a. Apache Range
  -l slow read a.k.a. Slow Reader
Reporting options:
  -S generate statistics with socket state change (off)
  -f file_prefix save statistics output in file.html and file.csv (g required)
  -l level verbosity level: 0=Fatal, 1=Info, 2=Warning, 3=Debug
General options:
  -c connections target number of connections (10)
  -i seconds interval between followup data in seconds (10)
  -l seconds target test length in seconds (240)
  -r rate connections per seconds (50)
  -b bytes value of Content-Length header if needed (none)
  -v verb verb to use in request, default to GET for slow headers and POST for slow http post
  -u url absolute URL of target (http://localhost/)
  -m max length of each randomized character pair of followup data per tick, 0-255 (2)
  -k key to use as header or footer for body, where % is a random character (S)
  -f content-type value of Content-Type header (application/x-www-form-urlencoded)
  -a accept value of Accept header (text/html;q=0.8,text/plain;q=0.8,image/png,*/*;q=0.5)
Probe/Proxy options:
  -H host:port all traffic directed through HTTP proxy at host:port (off)
  -h host:port proxy traffic directed through HTTP proxy on host:port (off)
  -s seconds timeout to wait for HTTP response on probe connection, after which server is considered unresponsive (5)
Range attack specific options:
  -s start left boundary of range in range header (0)
  -b bytes limit for range header right boundary values (2000)
Slow read specific options:
  -n number of times to repeat: send request to the connection, use its multiply response size if server supports persistent connections (1)
  -i seconds interval between read operations from recv buffer in seconds (1)
  -s start of the range advertisement window size would be picked from (1)
  -b bytes end of the range advertisement window size would be picked from (1024)
  -f bytes bytes to slow read from receive buffer with single read() call (1)

```

```

Tue Jul 14 11:28:53 2020:
slowhttpstest version 1.6
- https://code.google.com/p/slowhttpstest/ -
test type: SLOW HEADERS
number of connections: 2000
URL: http://192.168.1.100:80/
verb: GET
Content-Length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 300
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy

Tue Jul 14 11:28:53 2020:
slow HTTP test status on 5th second:
initializing: 0
pending: 609
connected: 178
error: 0
closed: 0
service available: YES

```

## โปรแกรมที่ใช้



## สมาชิก

- 643020369-0 ณัฐปภัล ศรีบ้านแฮด
- 643020385-2 นายเนติร ทะแพงพันธ์
- 643020401-0 พีรพัฒน์ ไชยคำกา
- 643020360-8 ฉัตรมงคล อุตถาชน
- 643020354-3 นายกิติ โพธิ์ศรี