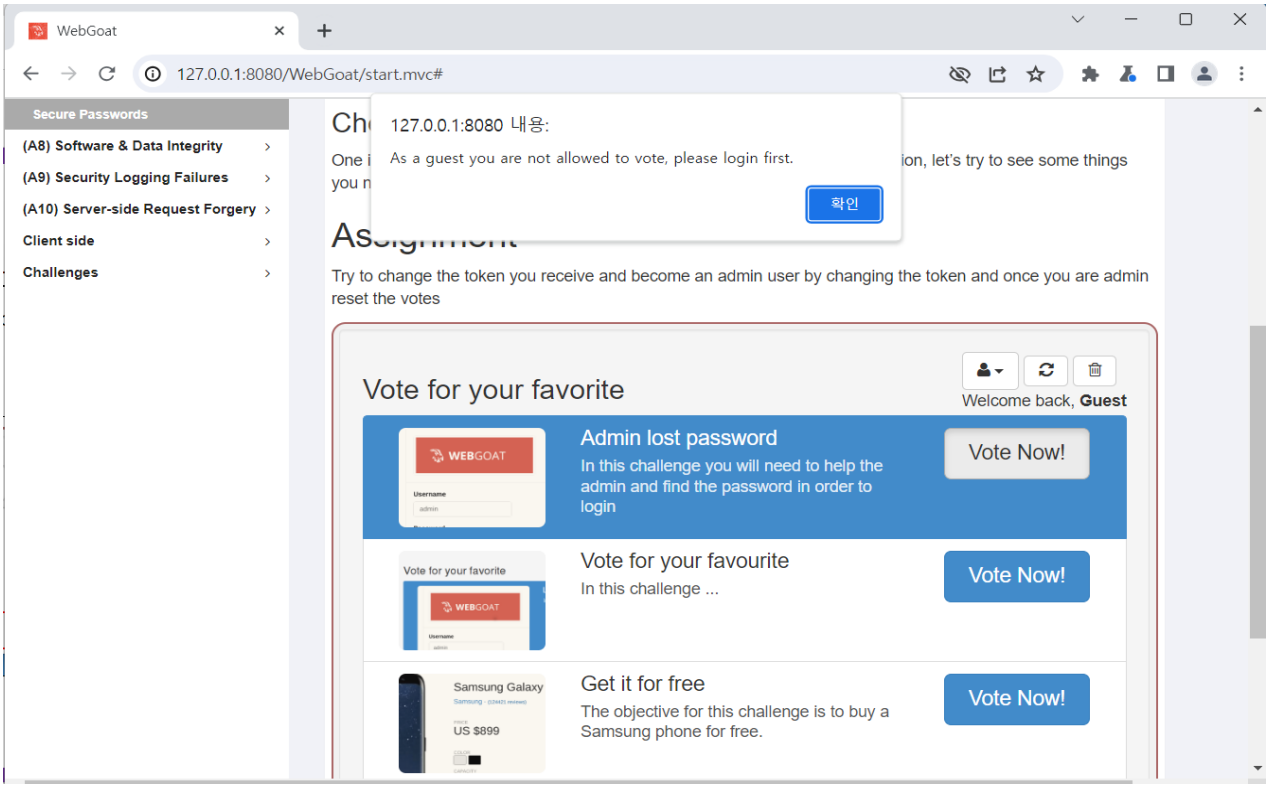
인터넷응용보안 13주차 과제

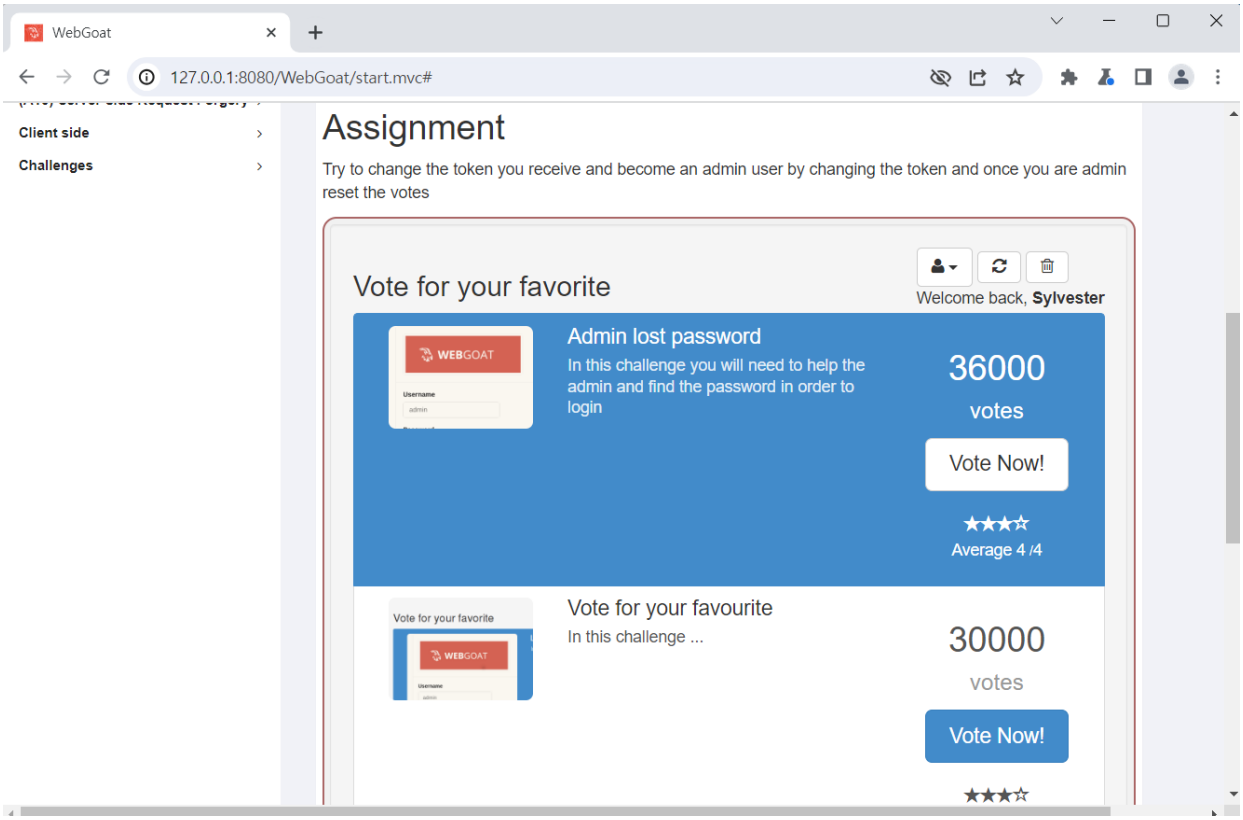
202121556 곽지현

JWT singing

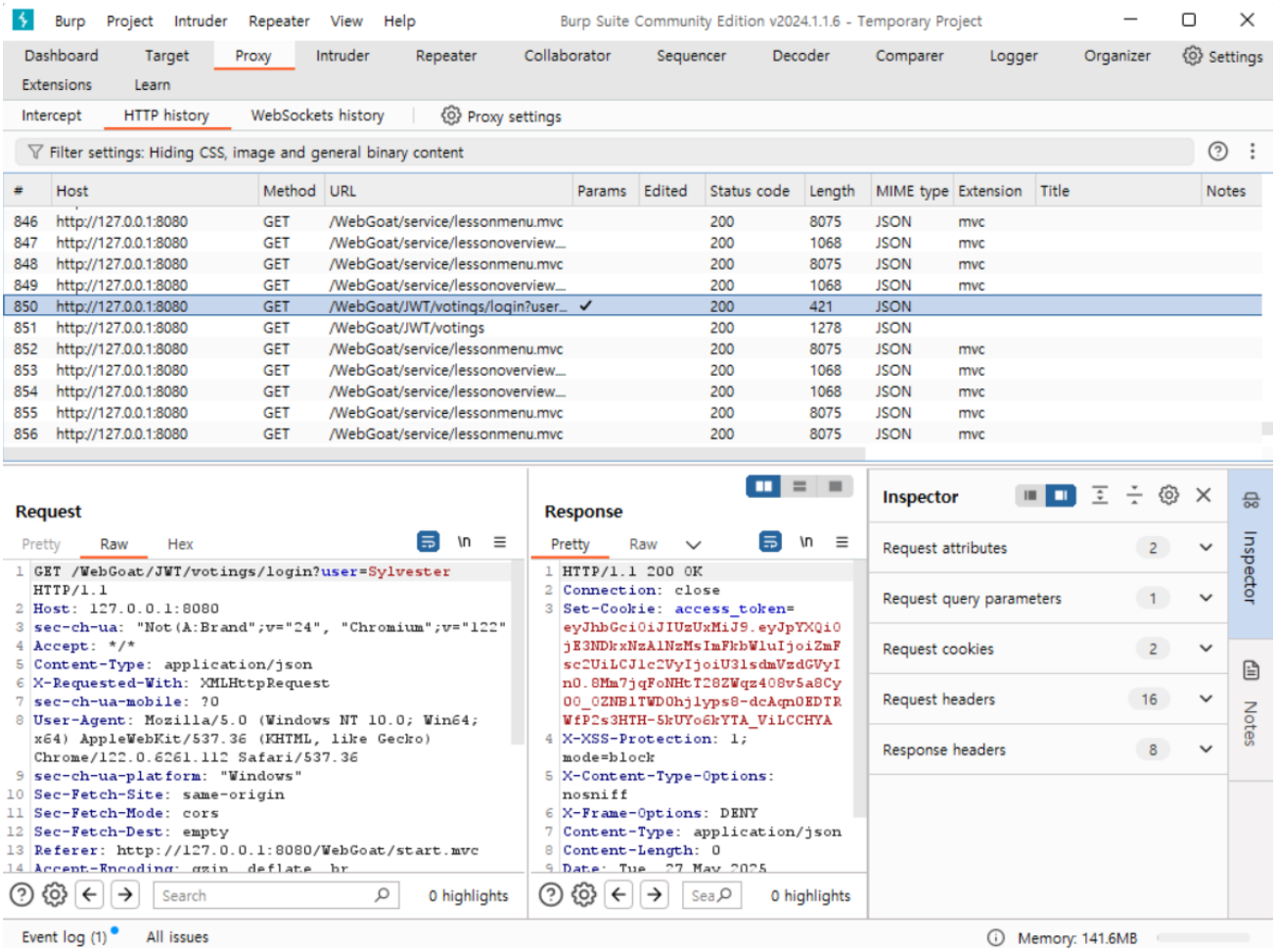
Vote Now! 버튼을 크릭 -> 로그인을 먼저 하라고 메시지가 뜬다.



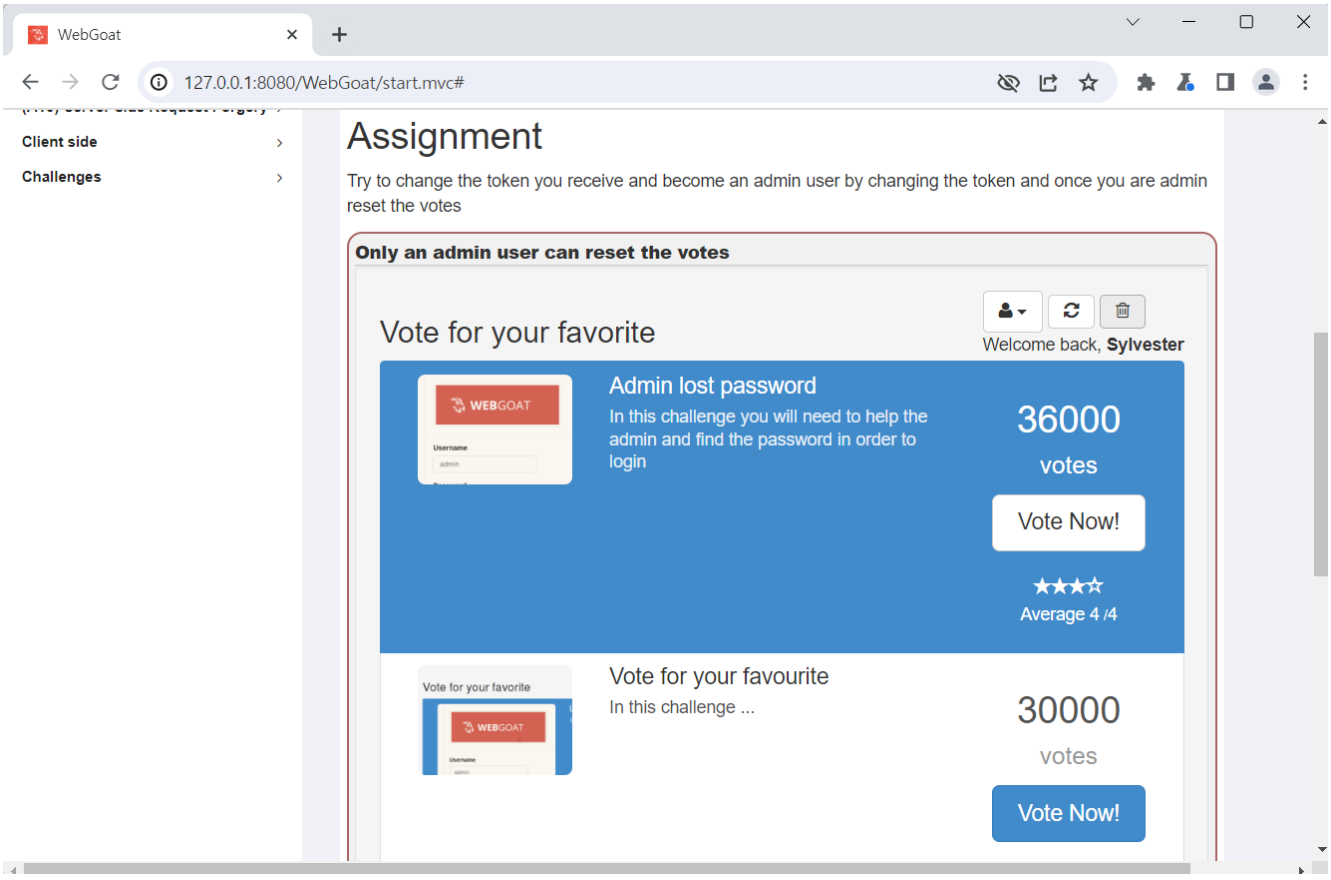
계정을 Sylvester로 변경 후 투표



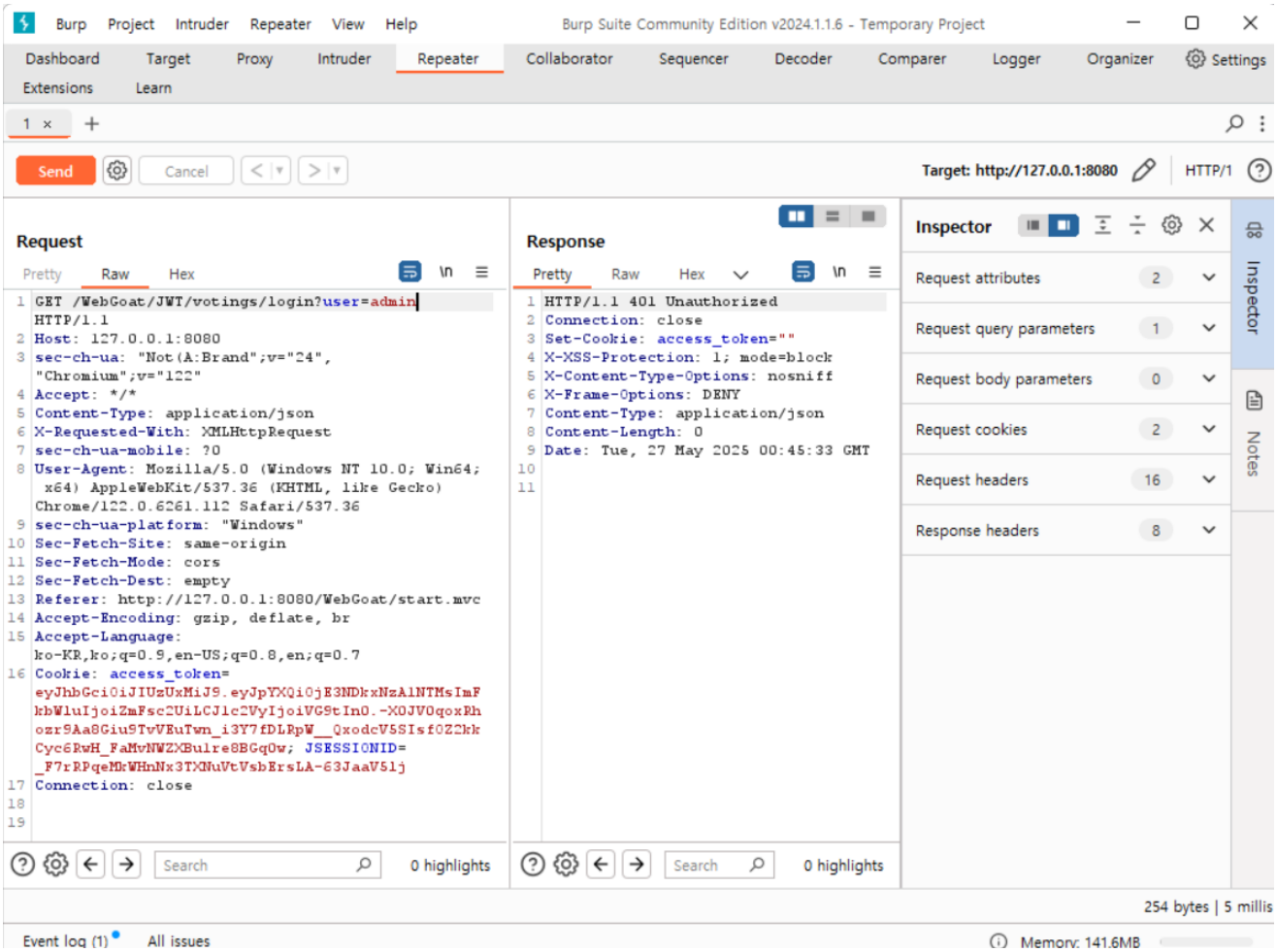
HTTP history로 가서 /WebGoat/JWT/votings/login URI 요청 확인



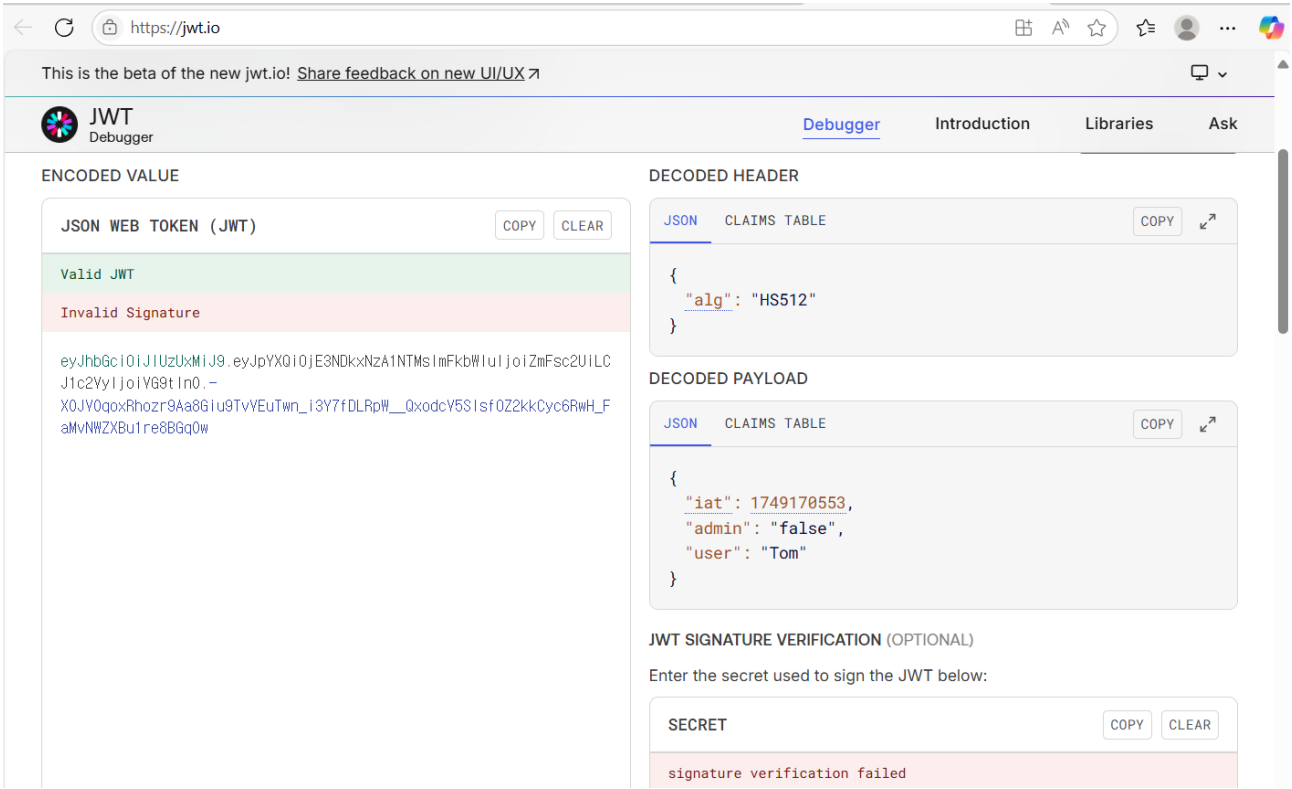
쓰레기통 버튼을 클릭 -> admin user만이 리셋할 수 있다고 메시지가 표시됨



Repeater로 보내고 Sylvester를 admin으로 수정 후 Send 버튼 클릭 -> 실패

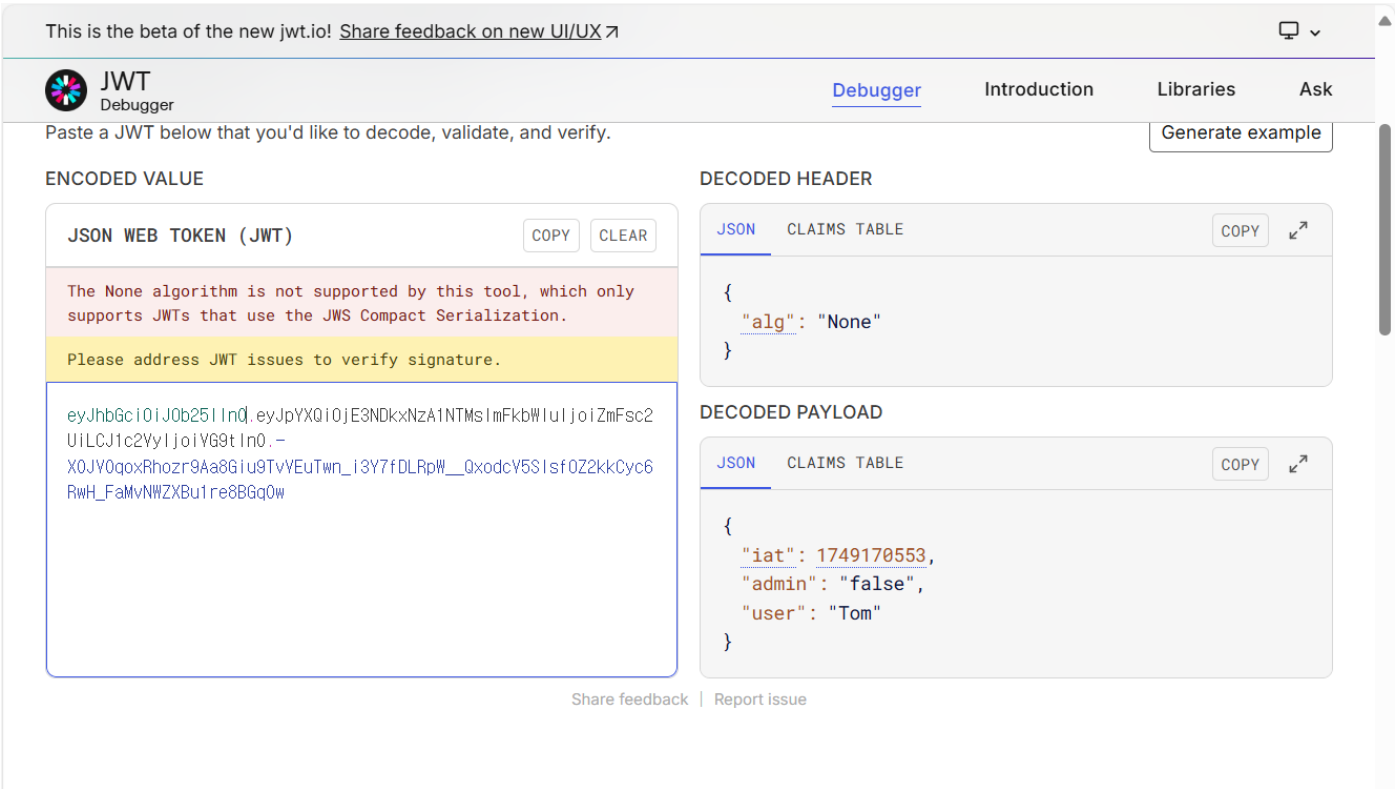


요청의 access_tokern 값을 복사하여 jwt.io 페이지에서 디코딩 -> admin 필드가 false로 되어 있는 것을 확인

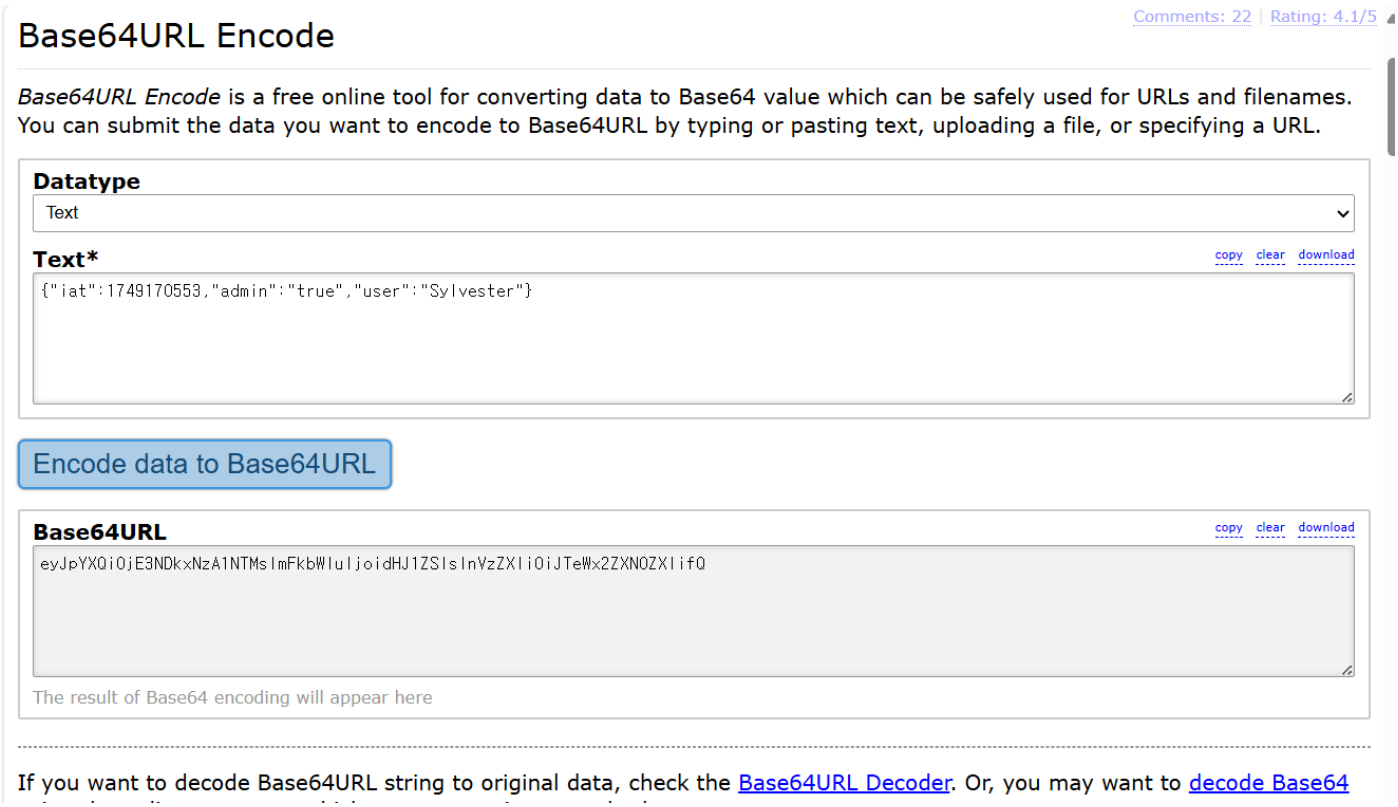


Base64 URL 인코딩 사이트로 이동 -> {"alg":"None"} 으로 입력하고 인코딩 -> 인코딩 된 값 복사

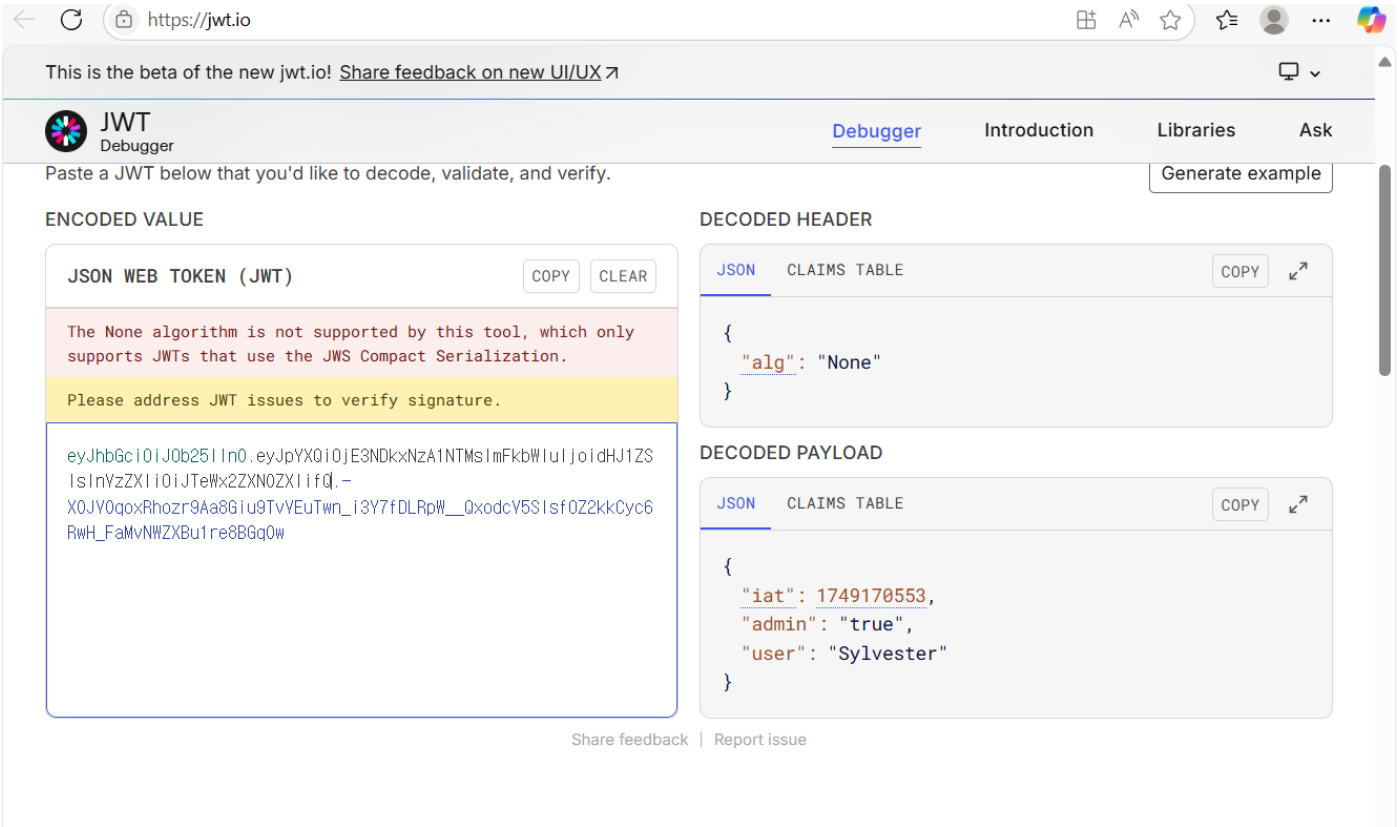
복사한 인코딩 값을 헤더 부분에 붙여 넣고 디코드된 정보가 alg : None 인지 확인



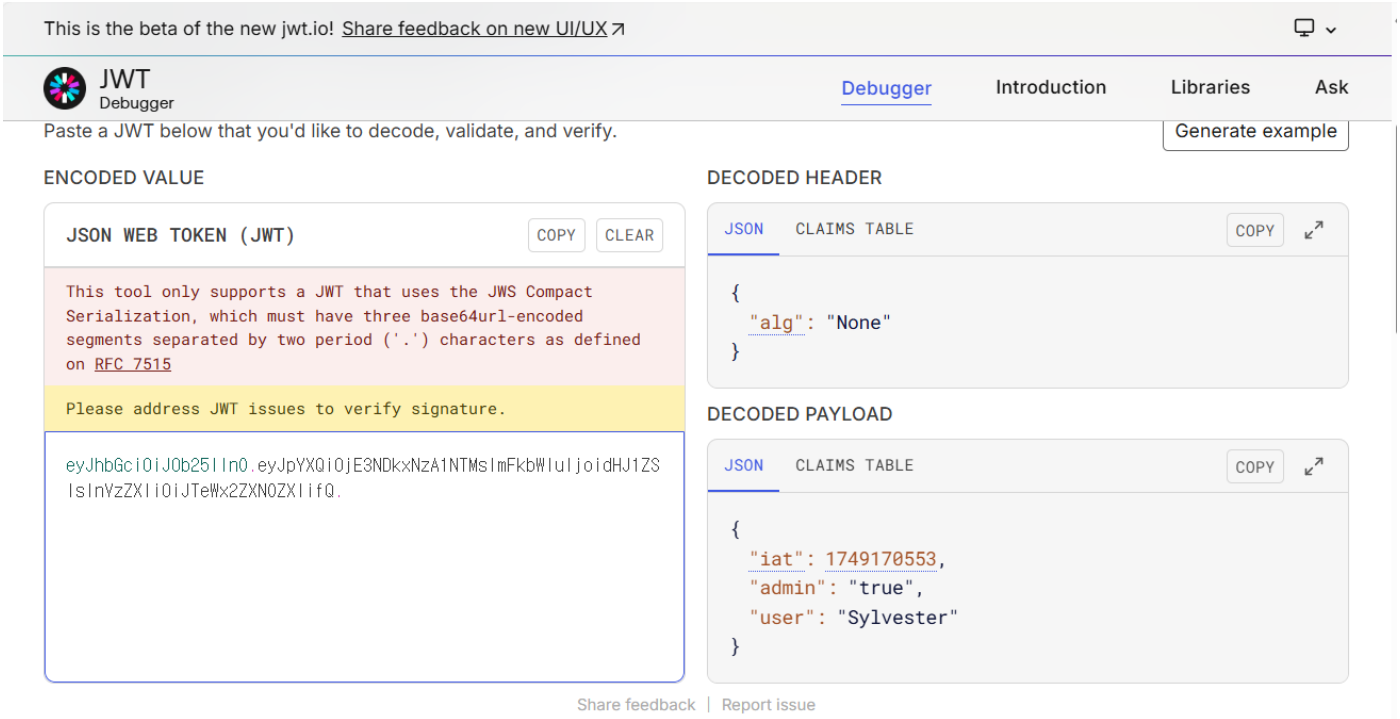
Base64 URL 인코딩 사이트에서 Payload 부분을 변경 -> admin을 true로 변경 -> 인코딩된 값 복사



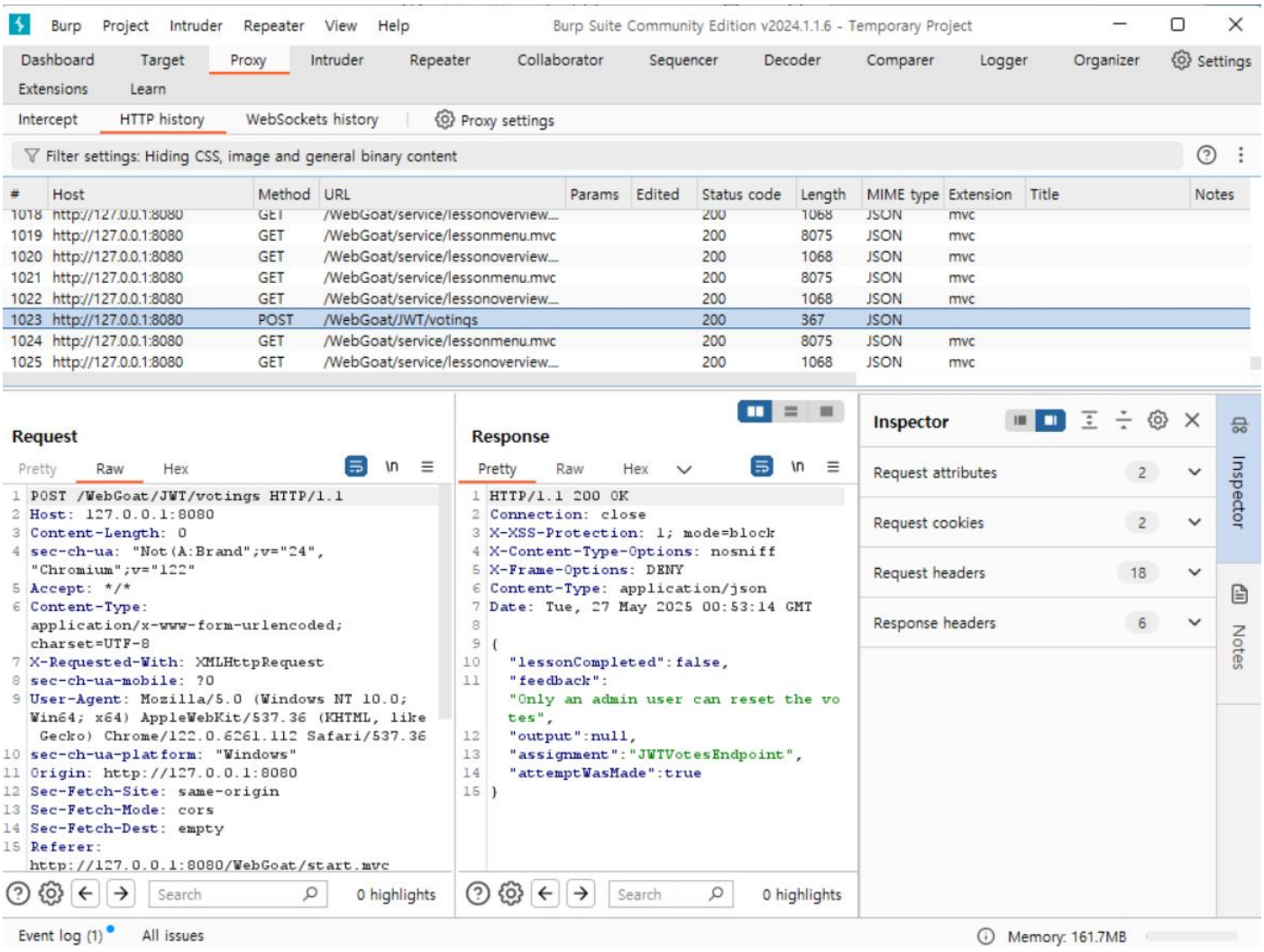
복사한 인코딩 값을 Payload 부분에 붙여 넣고 디코드된 정보에서 admin:ture 인지 확인



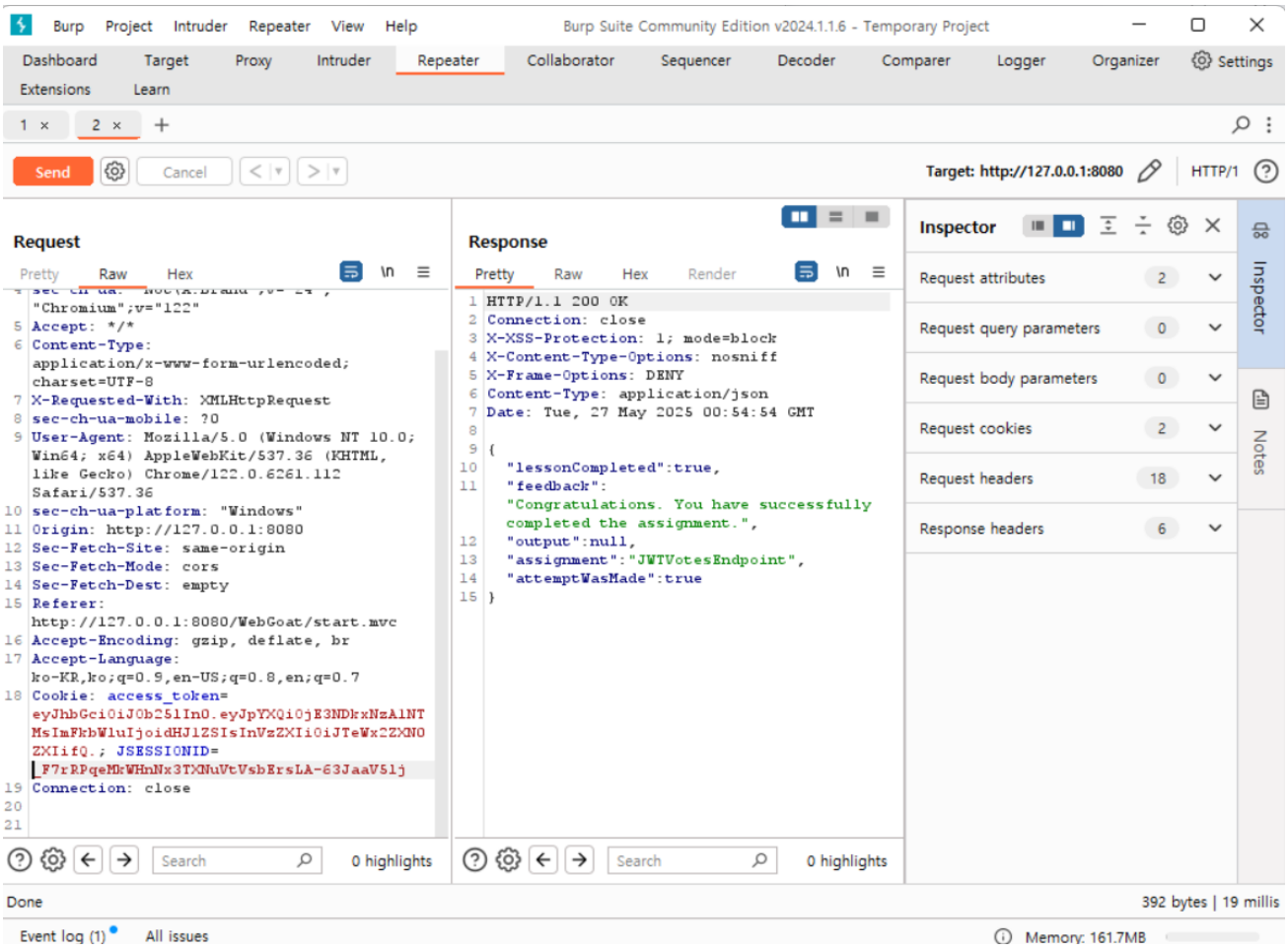
.을 두고 서명 데이터는 지운다.



쓰레기통 버튼을 클릭 -> HTTP history로 가서 POST 요청을 확인



Repeater로 보낸후 요청의 access_toker 부분을 앞에서 만든 JWT 값으로 바꾼다. -> Send 버튼 클릭



성공!