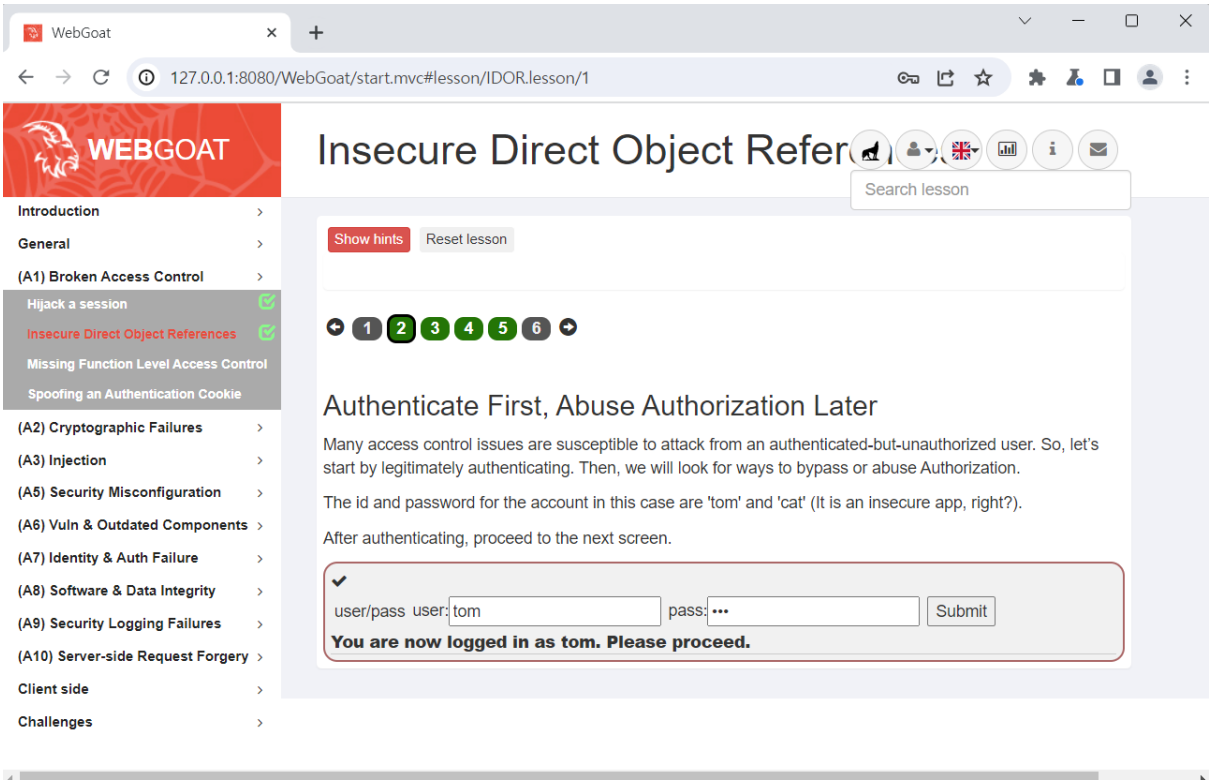
인터넷응용보안 4주차 과제

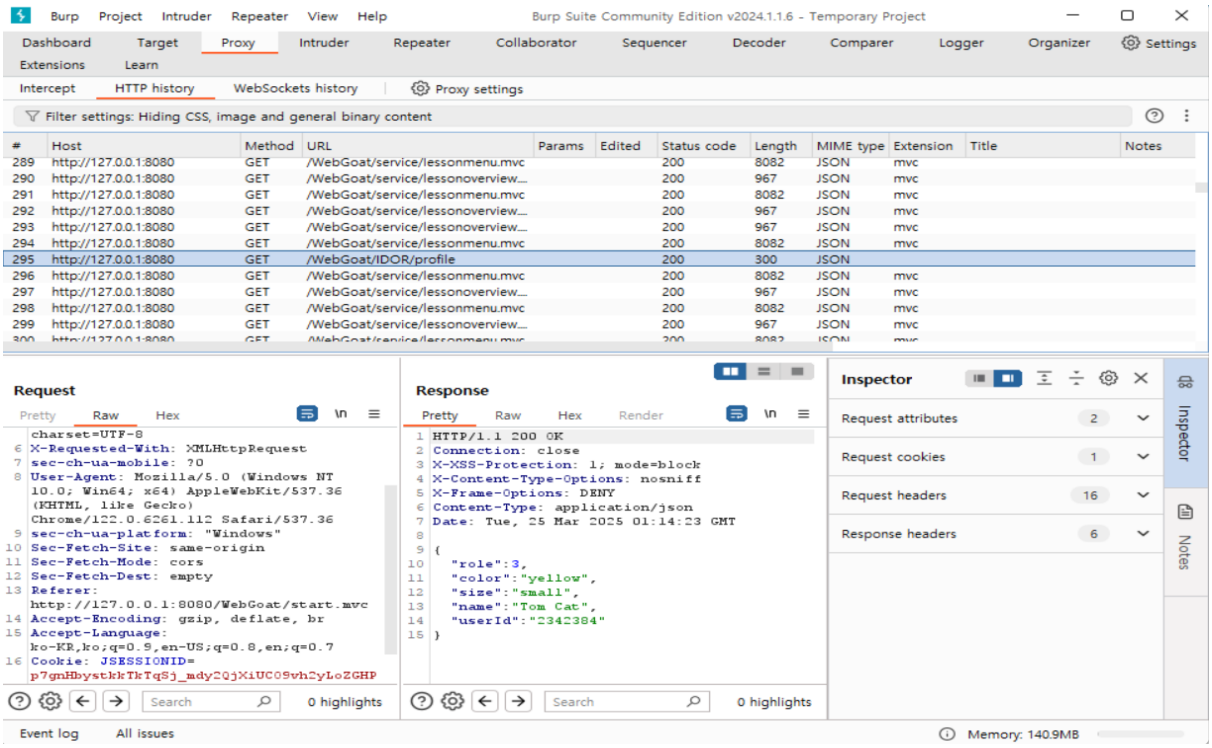
202121556 곽지현

Insecure Direct Object References

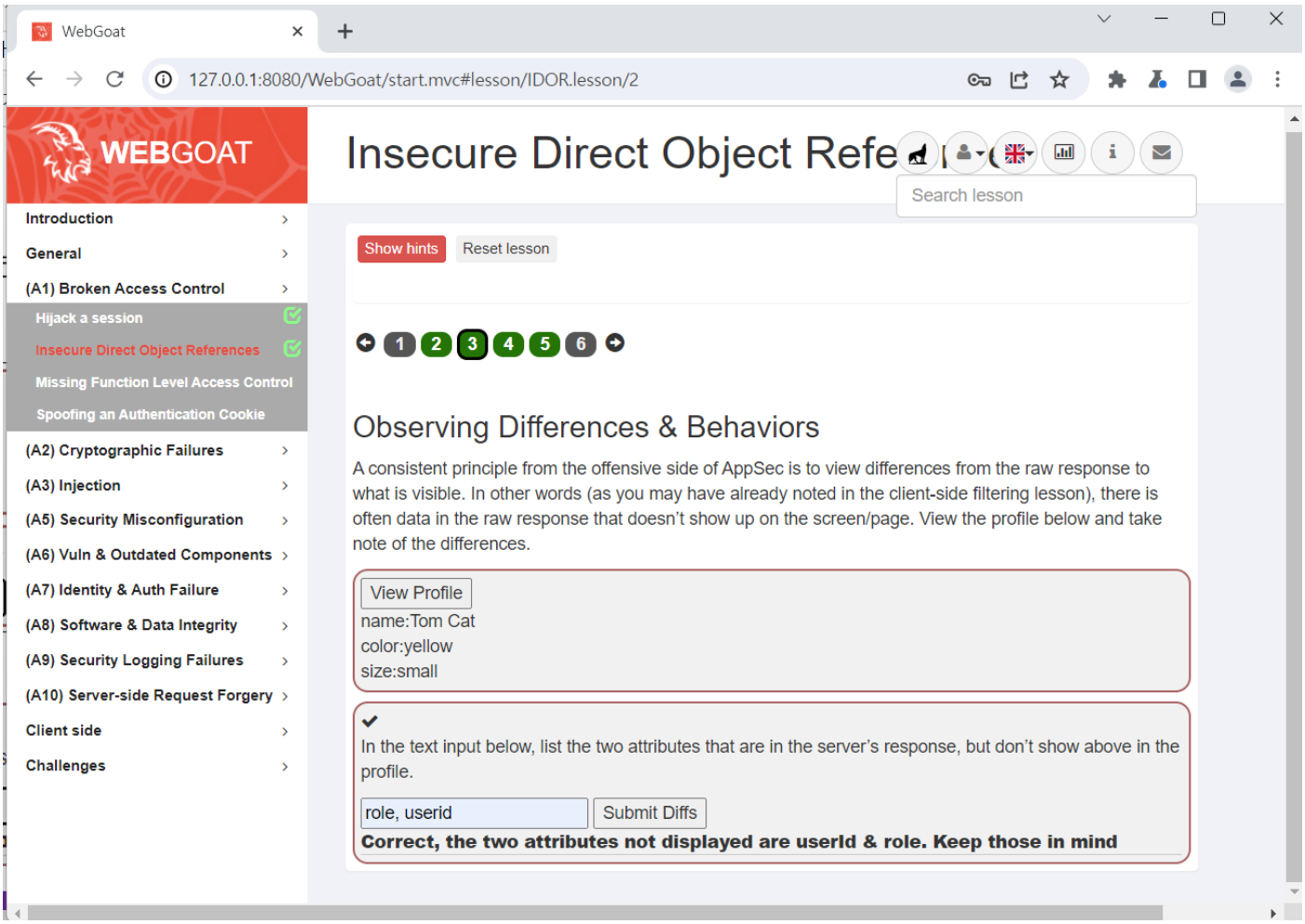
2번 문제. tom, cat을 입력하여 로그인에 성공



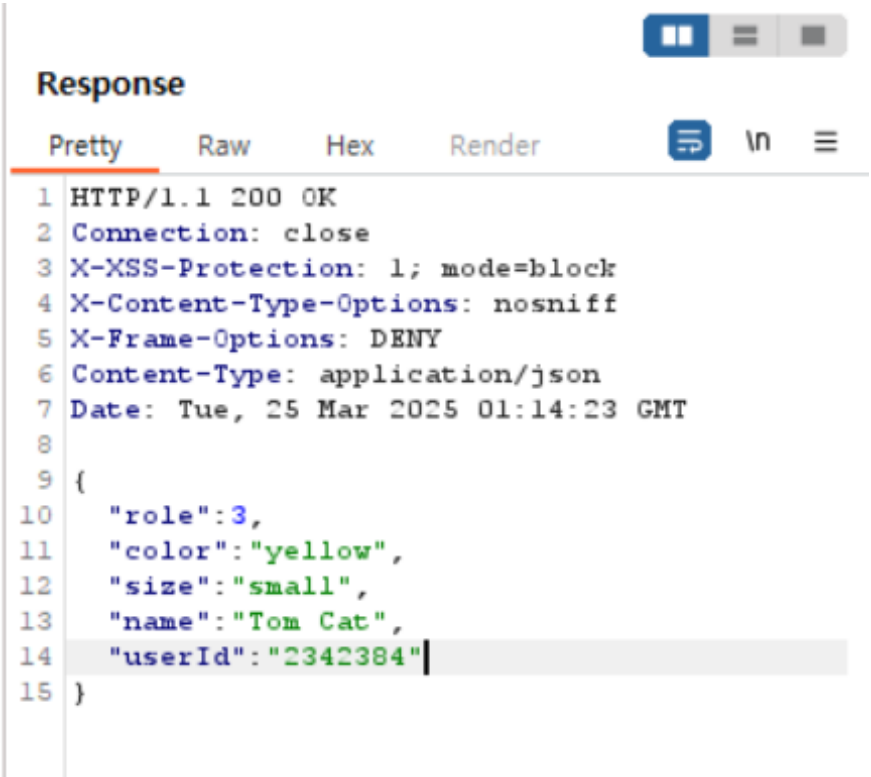
3번 문제. View Profile 버튼을 누른 뒤 GET /WebGoat/IDOR/profile 을 찾아 클릭



Response 탭의 내용을 보면 role, userId 항목이 있지만 보기에는 없기 때문에 role과 userId를 입력 해 준다.

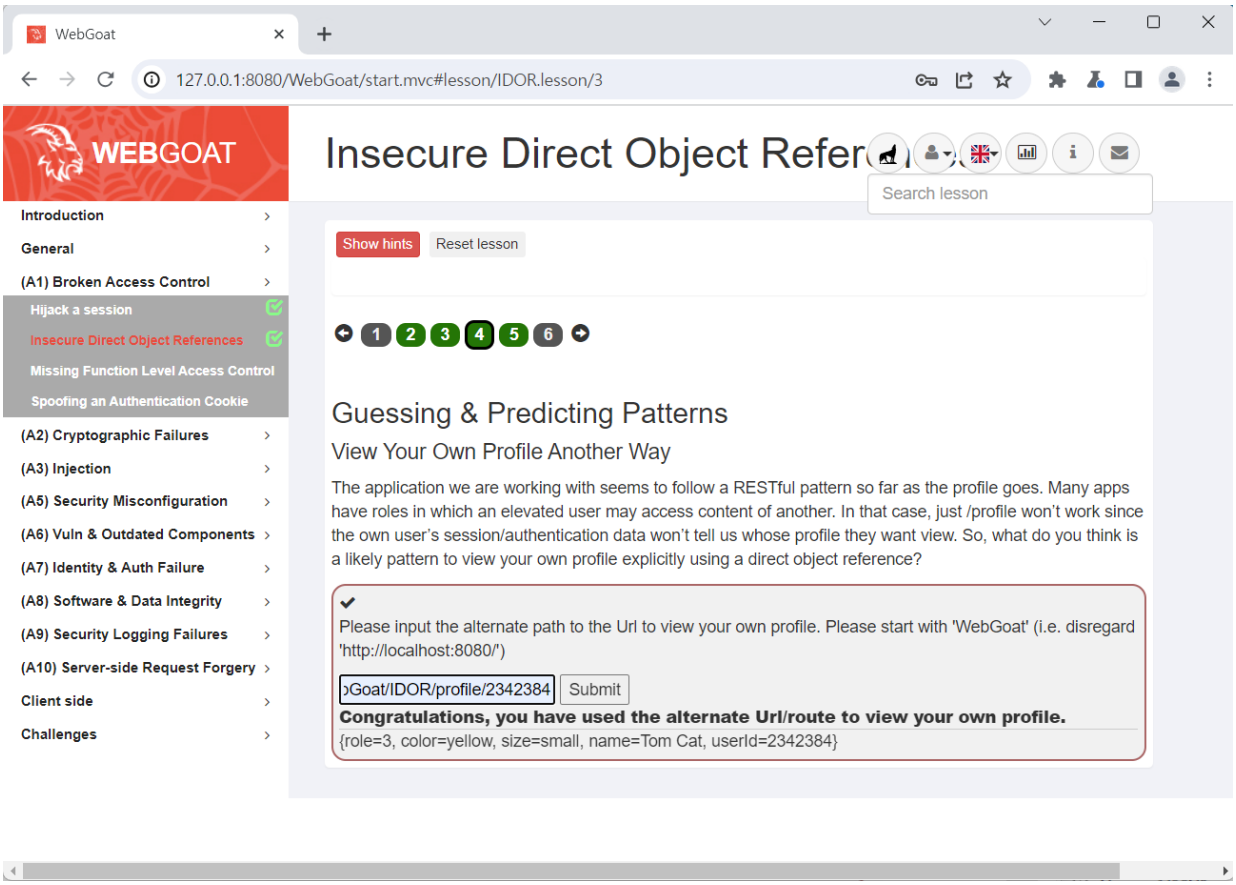


4번 문제. Response를 살펴보면 userId가 존재 → 2342384



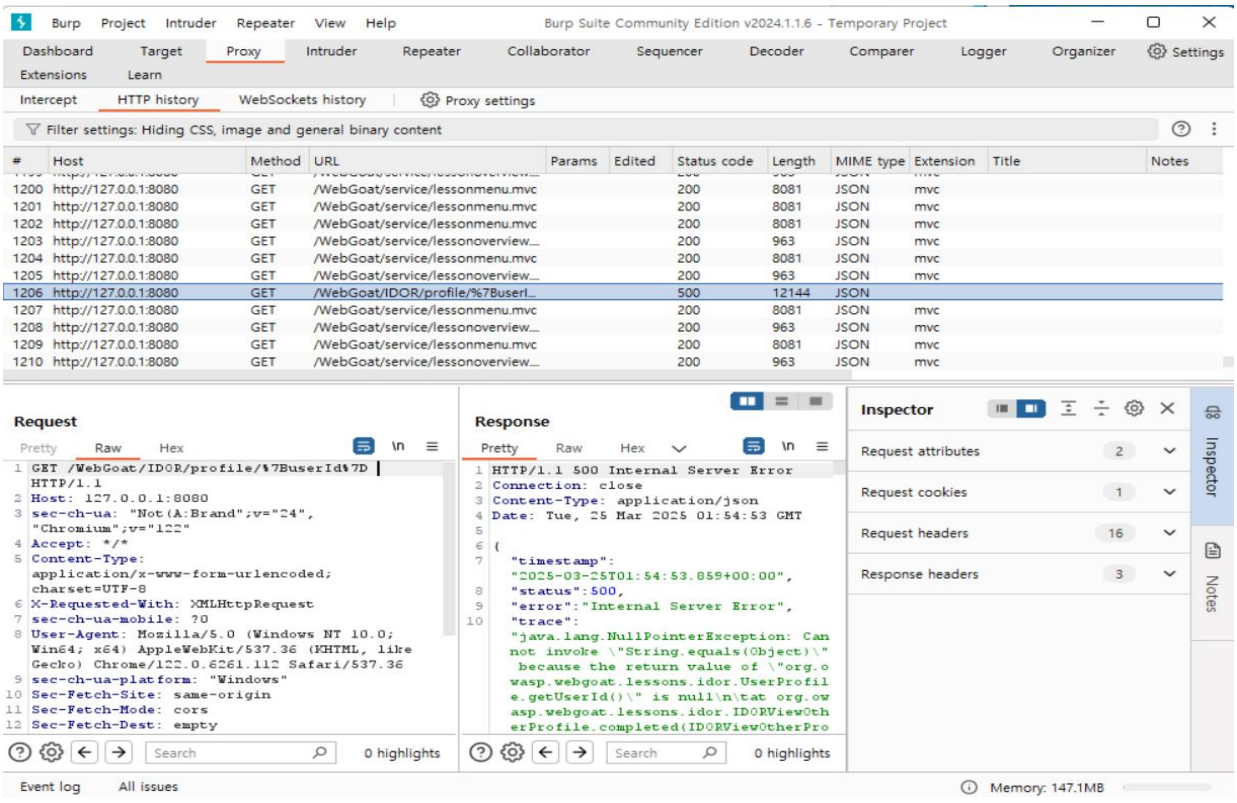
userId를 URI에 포함하여 WebGoat/IDOR/profile/2342384를 입력

Submit 버튼을 누르면 성공

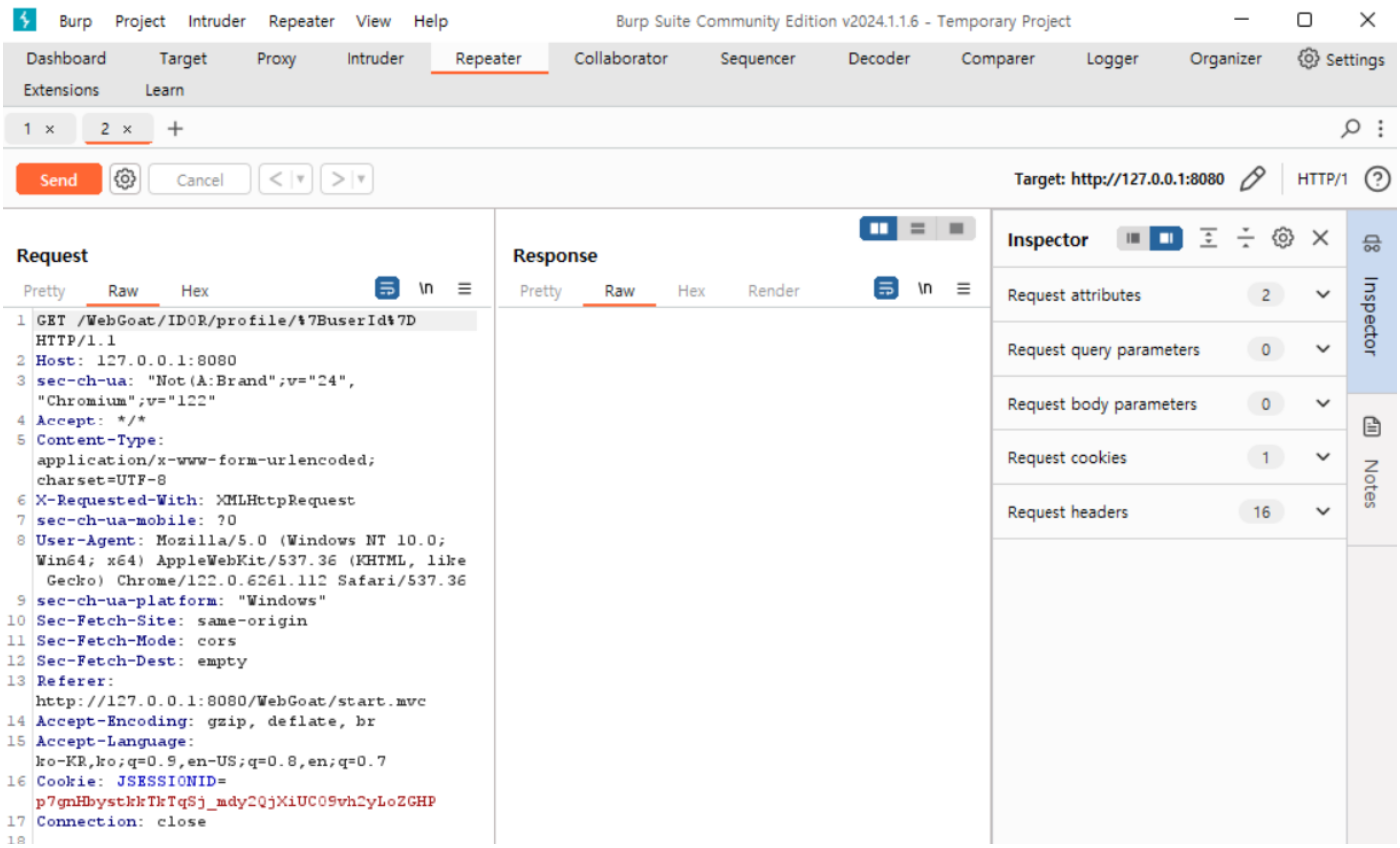


5 - 1번 문제. ViewProfile 버튼을 누르고 HTTP history를 본다

GET /WebGoat/IDOR/profile/%7BuserId%7D를 찾아 클릭

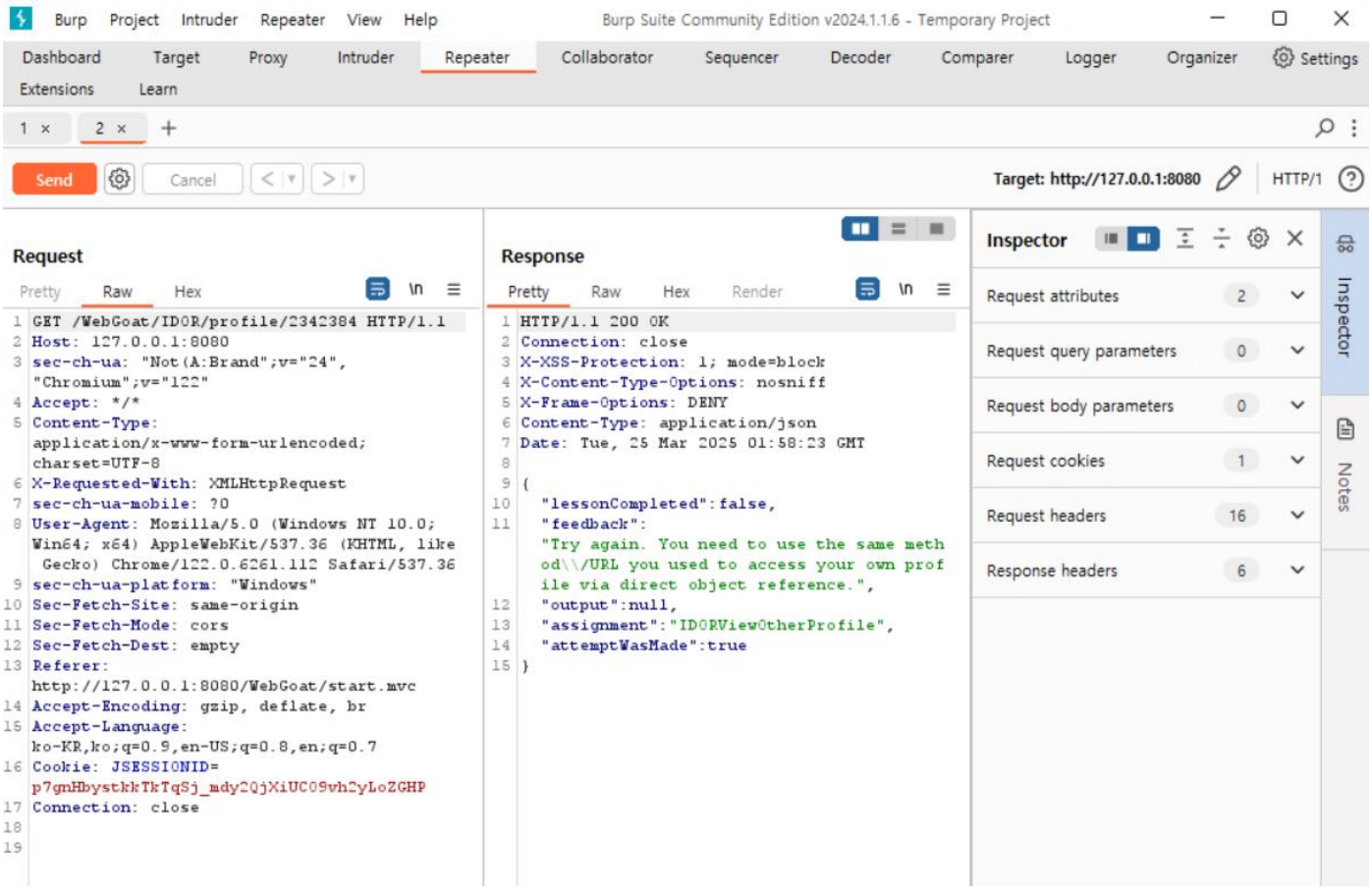


Send to Repeater 클릭 후, Repeater 탭으로 이동



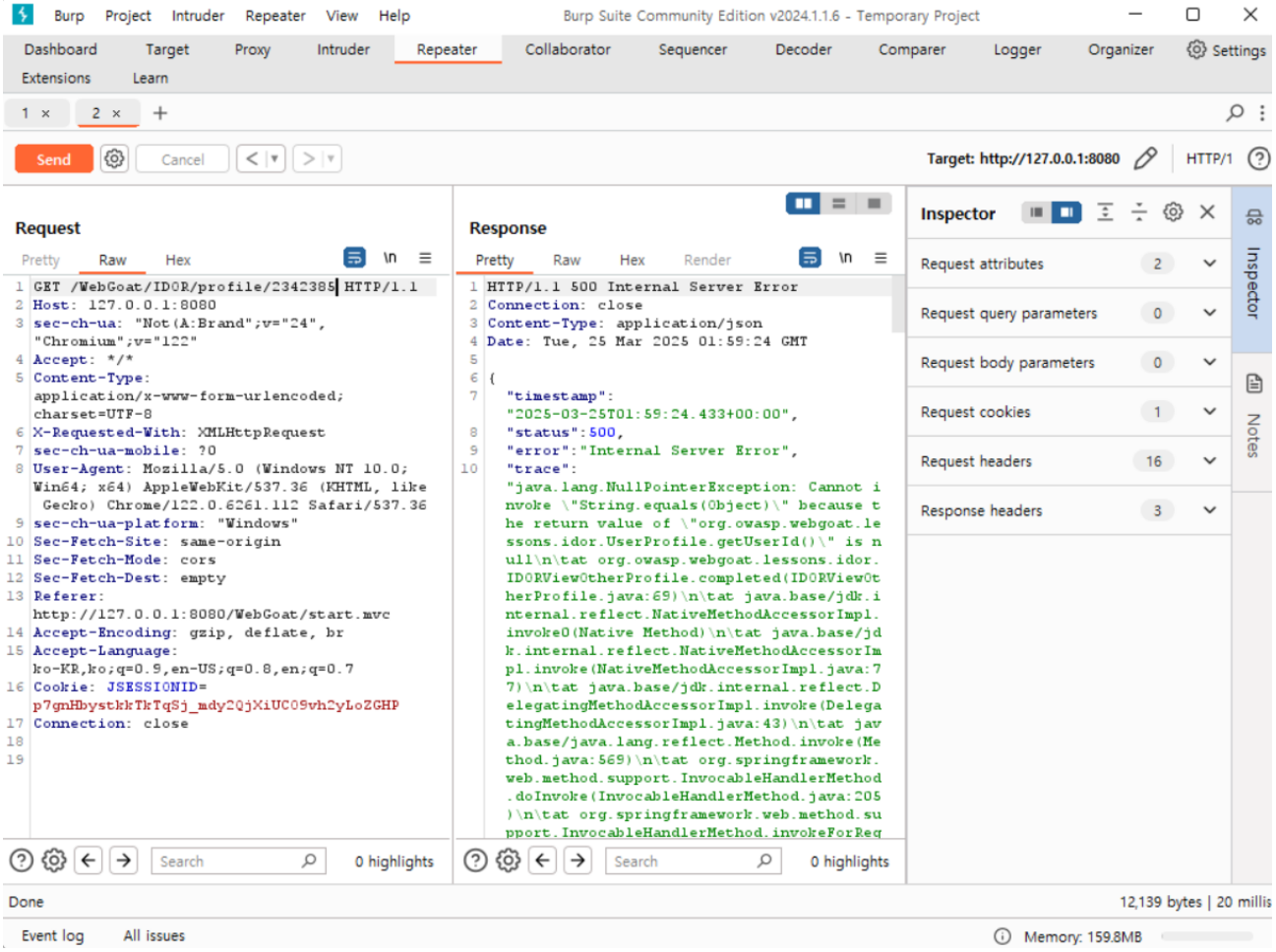
%7BuserId%7D 부분을 Tom의 userId인 2342384로 바꾸고 Send 버튼 클릭

Response 화면에 다시 시도하라는 메시지가 뜬다.

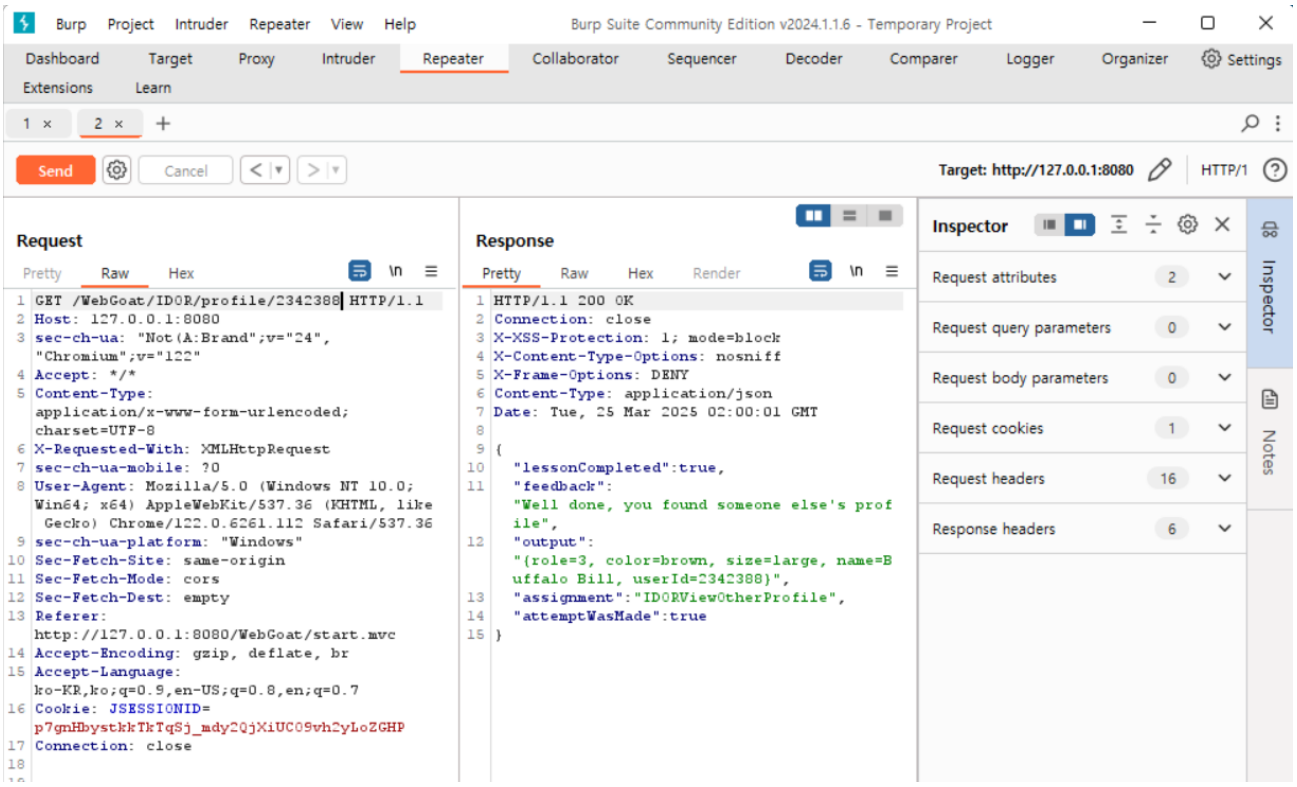


userId부분을 1씩 증가하며 Response를 살펴본다

해당 ID가 없으면 Internal Server Error 발생

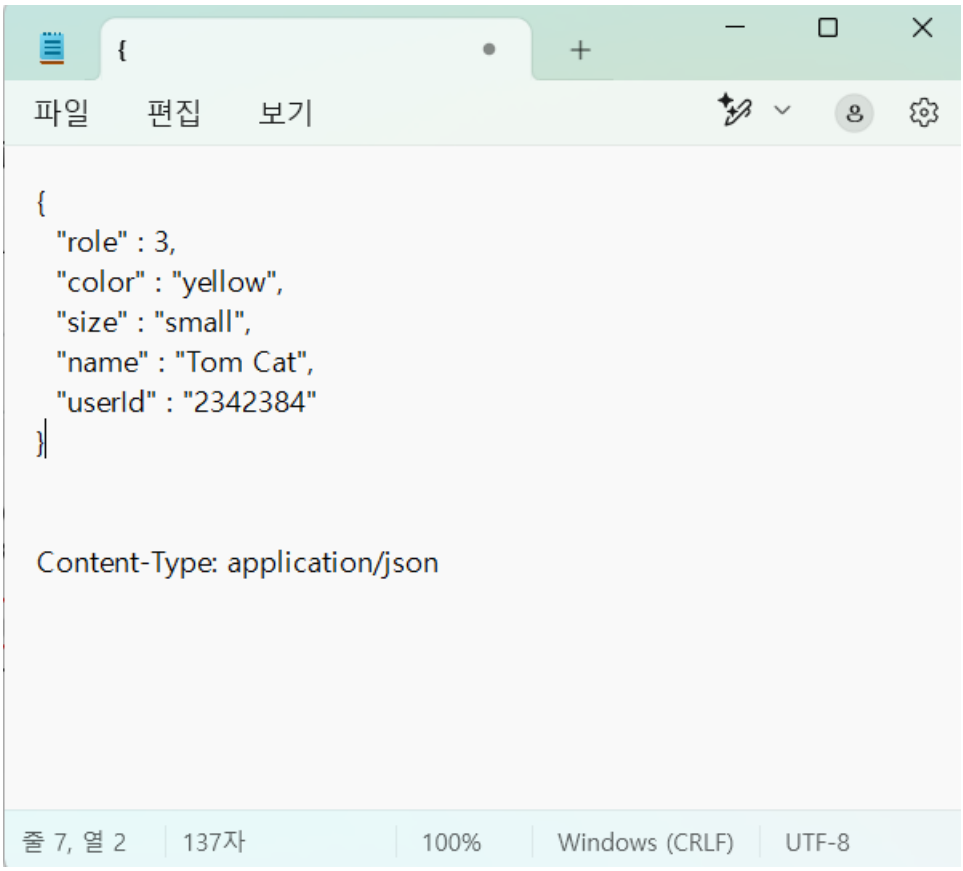


계속 1씩 증가하다 보면 userId가 매칭된다 → 성공 (userId : 2342388)

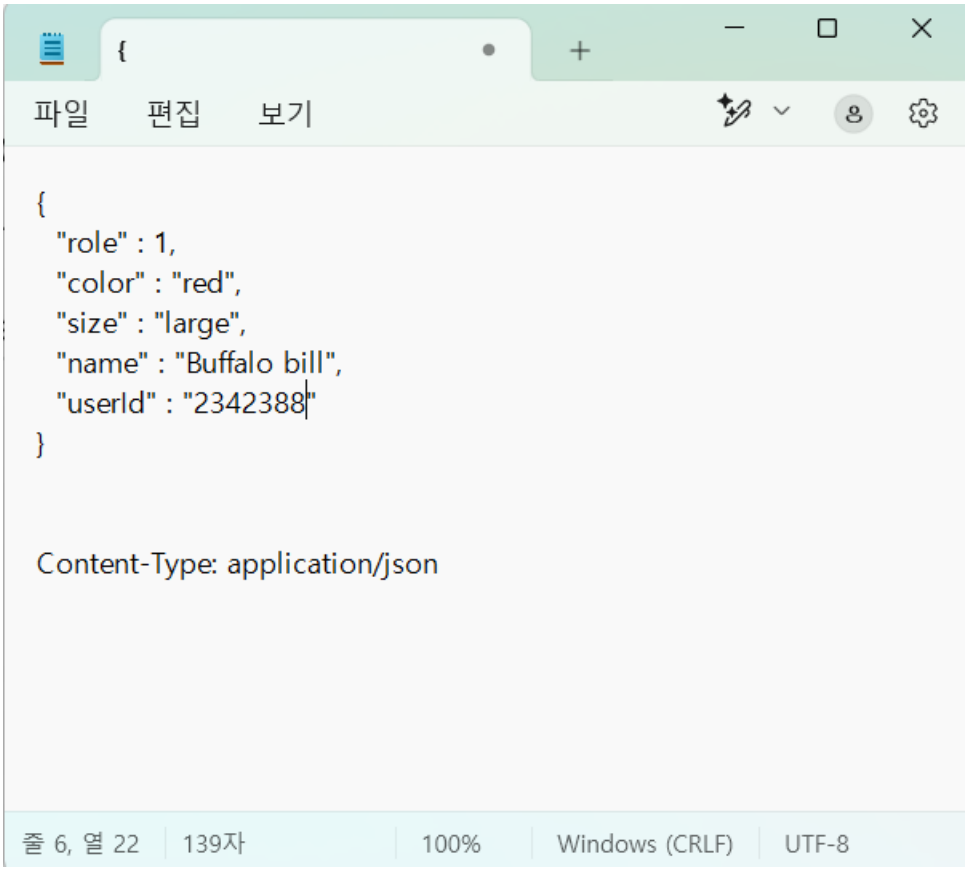


5 - 2번 문제. Tom의 프로필 데이터 Response를 살펴보면 json 포맷인 것을 확인 가능

Tom의 프로필 데이터와 Content-Type 복사

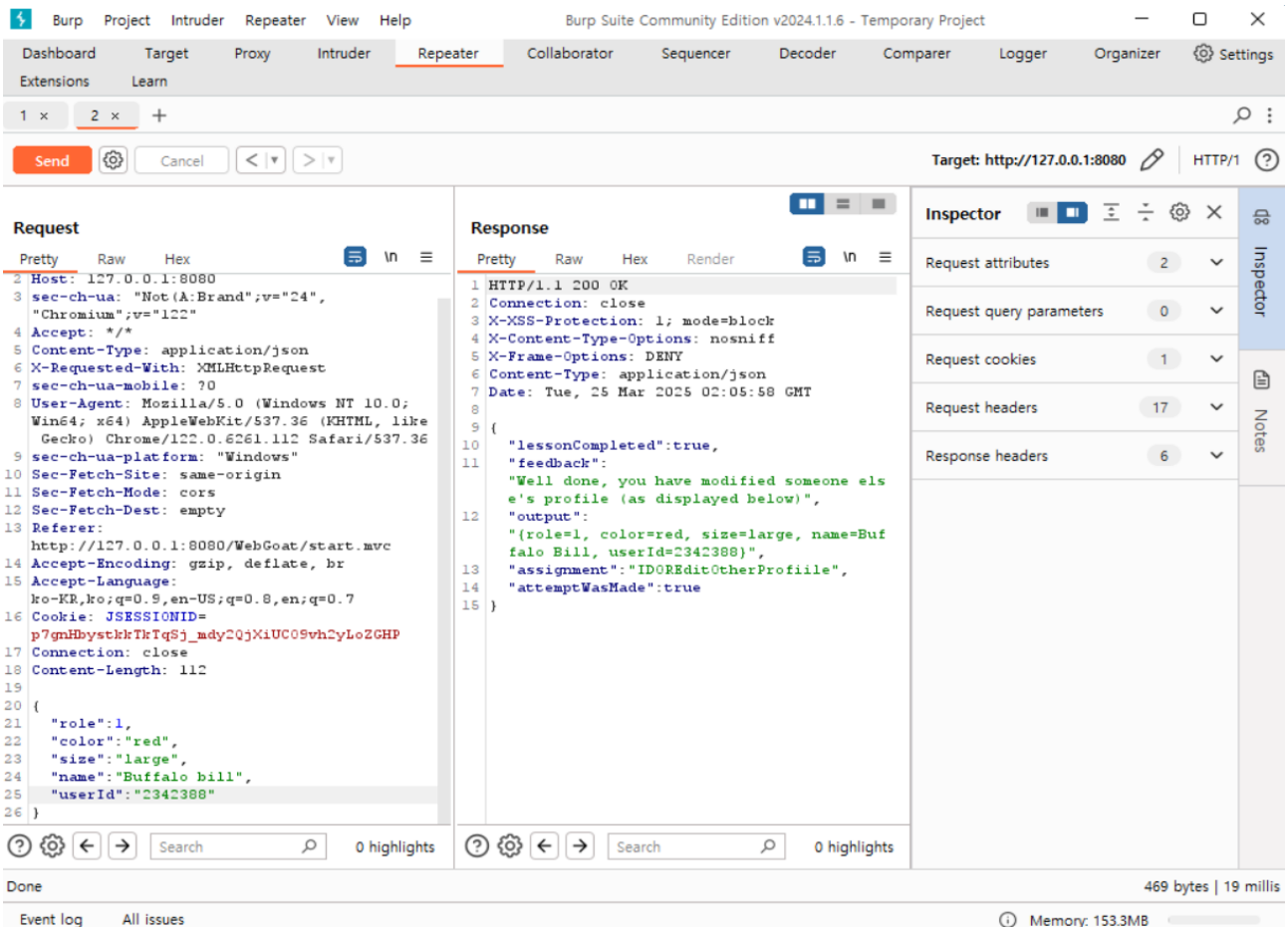


복사해 놓은 Tom의 프로필 데이터 수정

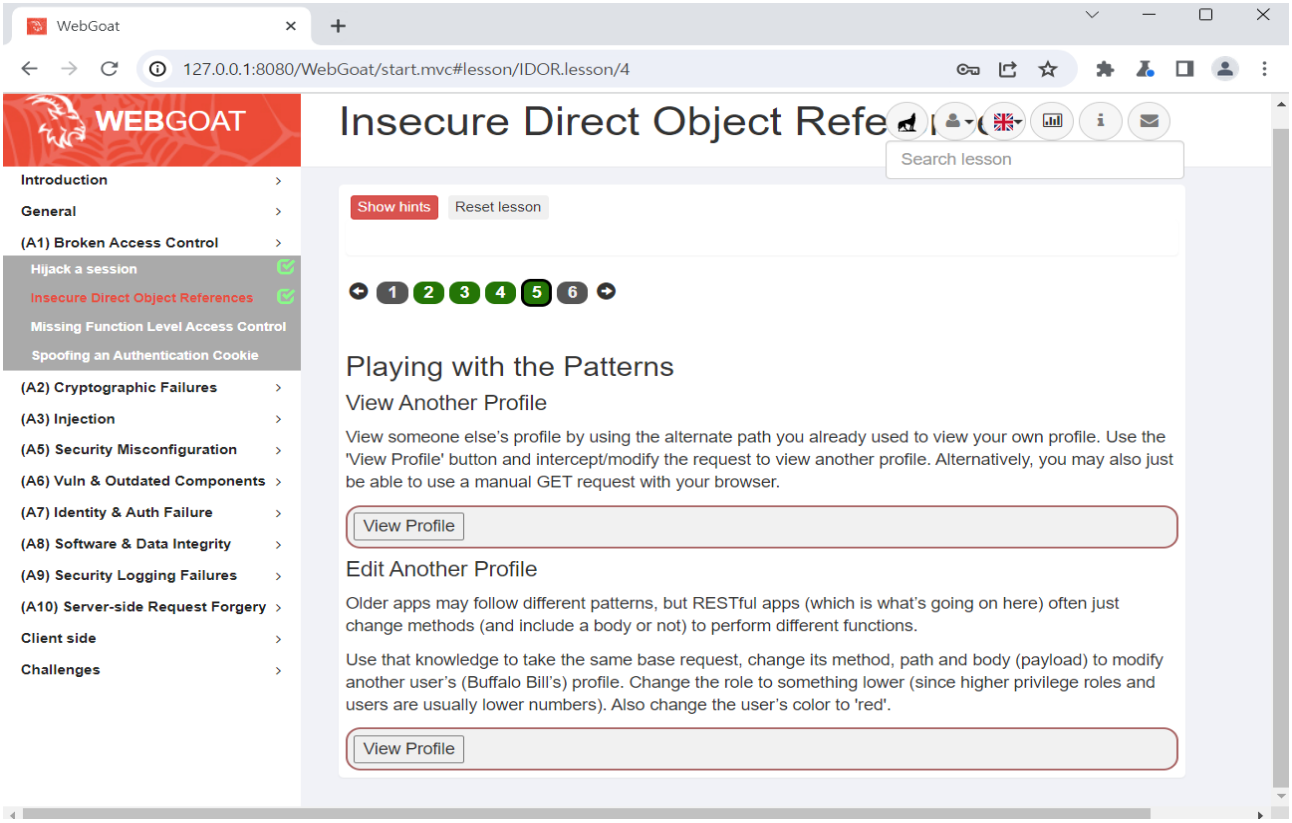


Repeater에서 PUT 명령으로 수정하고 Content-Type: application/json 으로 수정

수정된 Tom의 프로필 데이터 붙어넣기



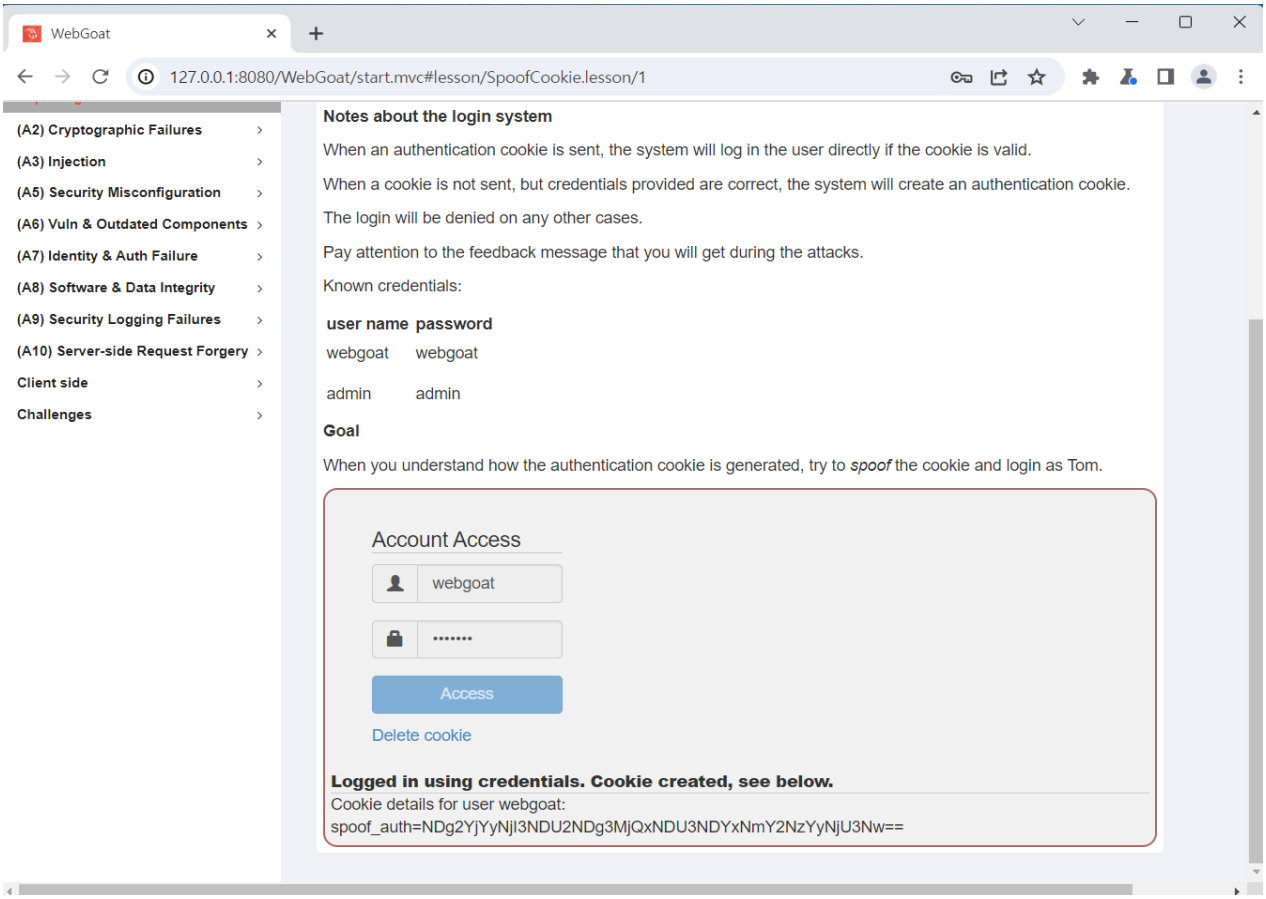
Insecure Direct Object References 모든 문제 성공!



Spoofing an Authentication Cookie

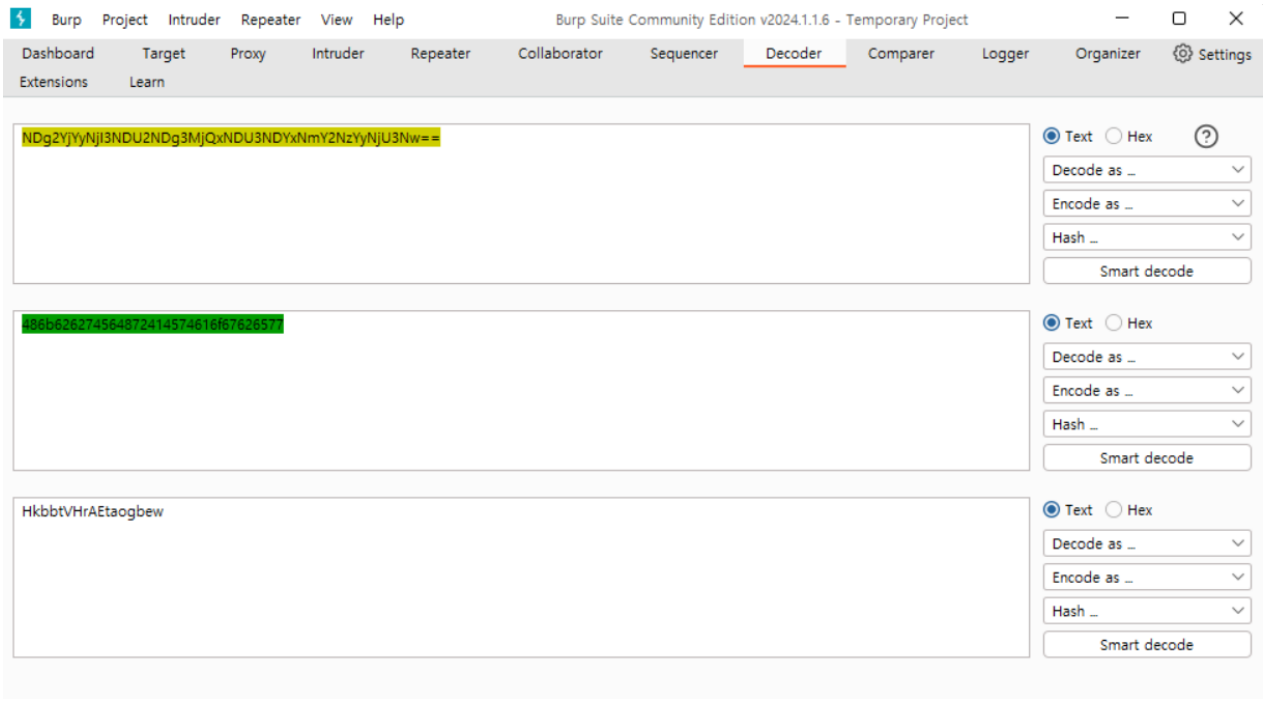
2번 문제. webgoat 계정으로 로그인

밑에 뜨는 쿠키 값으 복사, Decoder 탭으로 이동

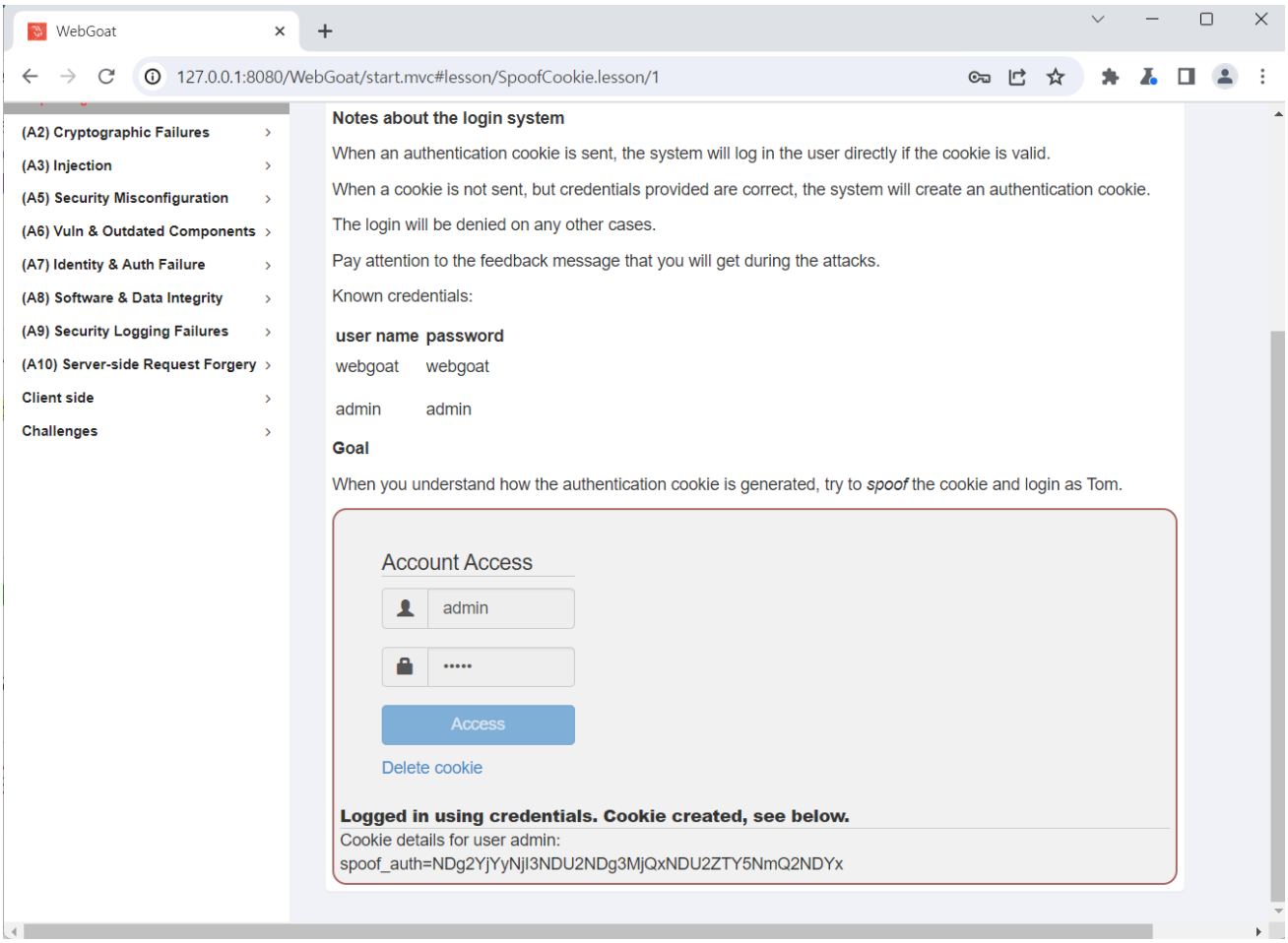


첫 번째에 있는 값을 Base64로 디코딩, 두 번째에 있는 값을 ASCII hex로 디코딩

세 번째에 있는 값 끝 부분이 webgoat를 거꾸로 쓴 것이다 (taogbew)



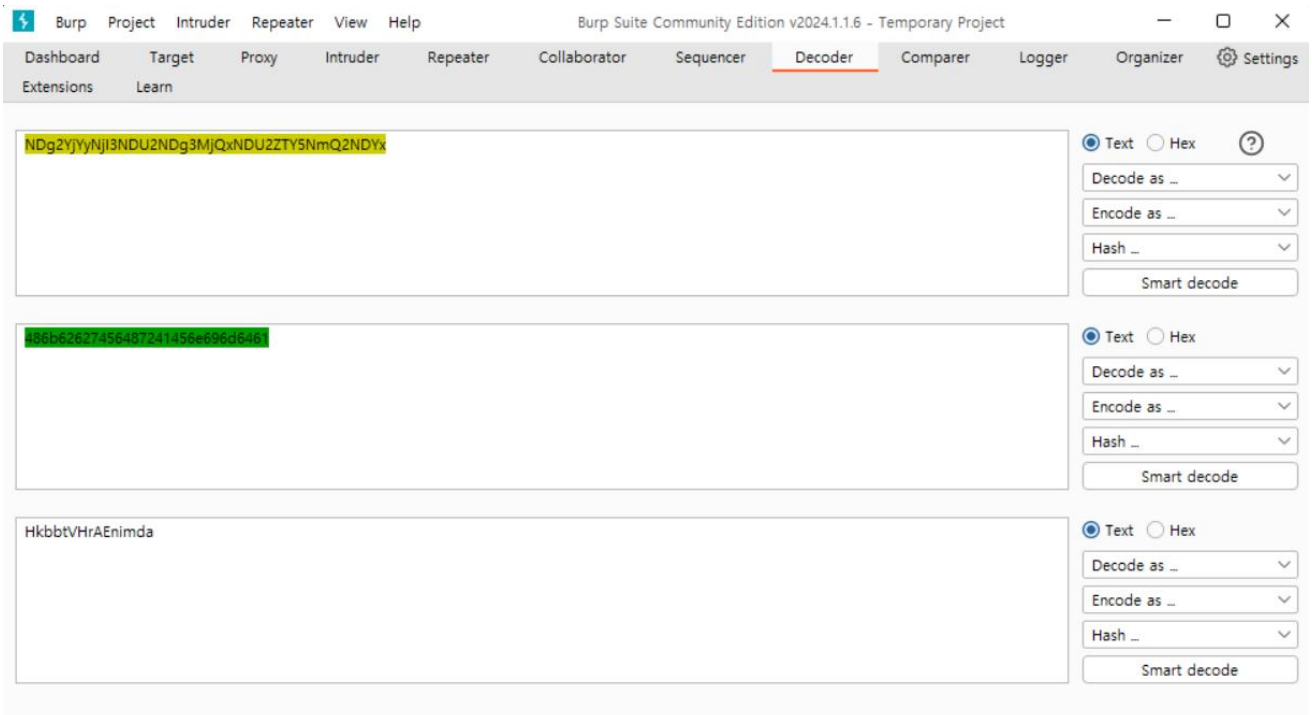
쿠키를 지운 뒤 admin 계정으로 로그인



첫 번째에 있는 값을 Base64로 디코딩, 두 번째에 있는 값을 ASCII hex로 디코딩

세 번째에 있는 값 끝 부분이 admin을 거꾸로 쓴 것이다 (nimda) → 앞 부분은 webgoat와 동일

쿠키 값 : 변경되는 난수값 + 거꾸로된 계정명

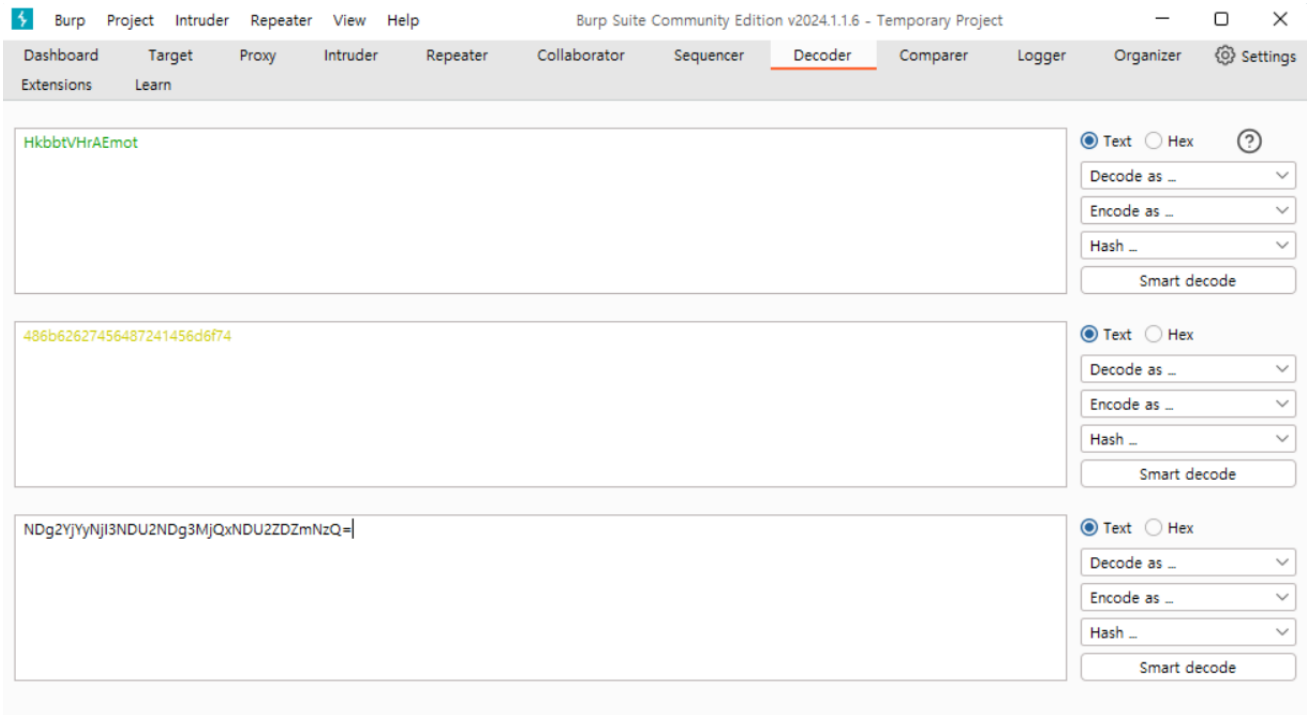


Tom으로 로그인 하기 위해 위의 난수값에서 거꾸로된 계정명(mot)를 추가하여 쿠키 값 만들기

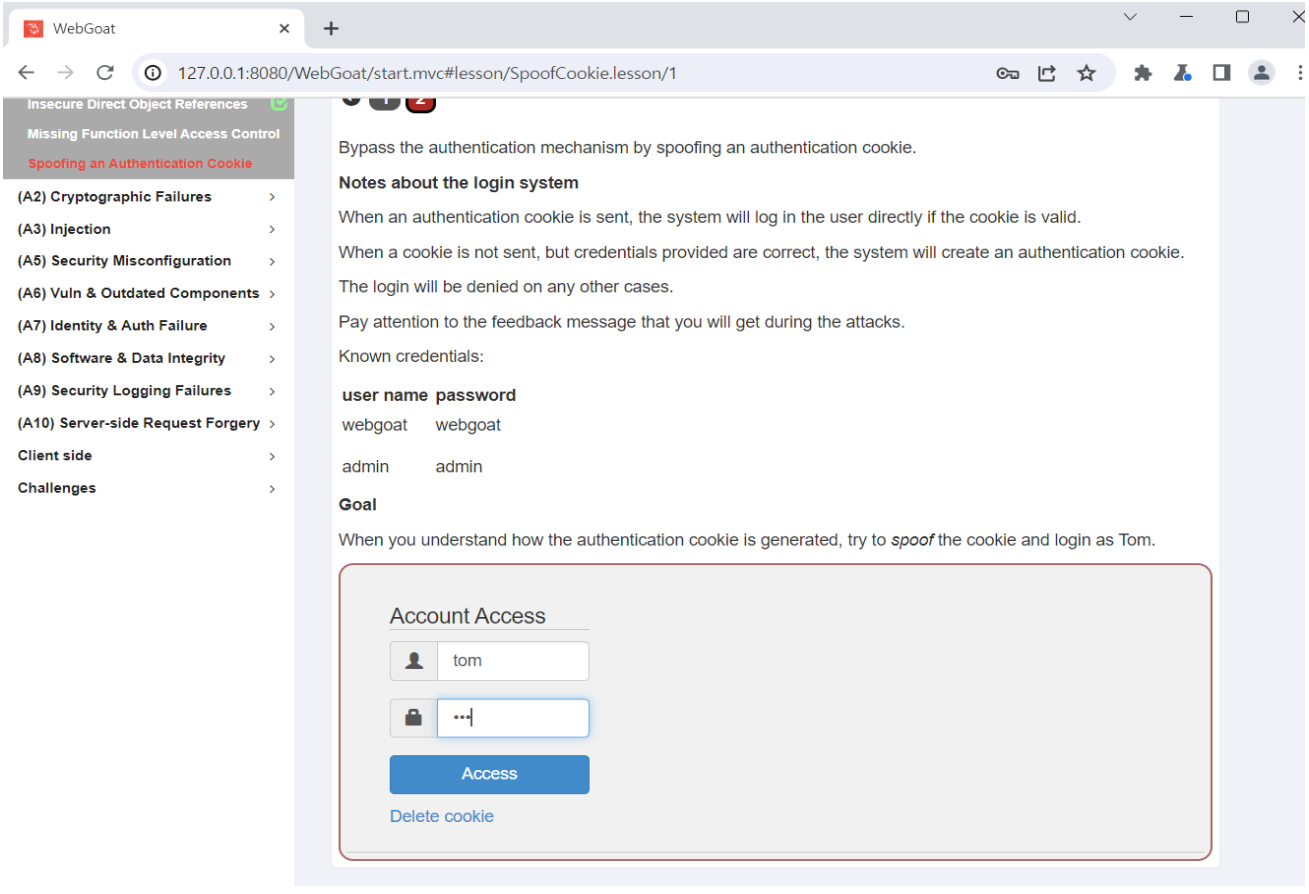
첫 번째 칸에 만든 쿠키 값 삽입

첫 번째에 있는 값을 ASCII hex로 인코딩, 두 번째에 있는 값을 Base64로 인코딩

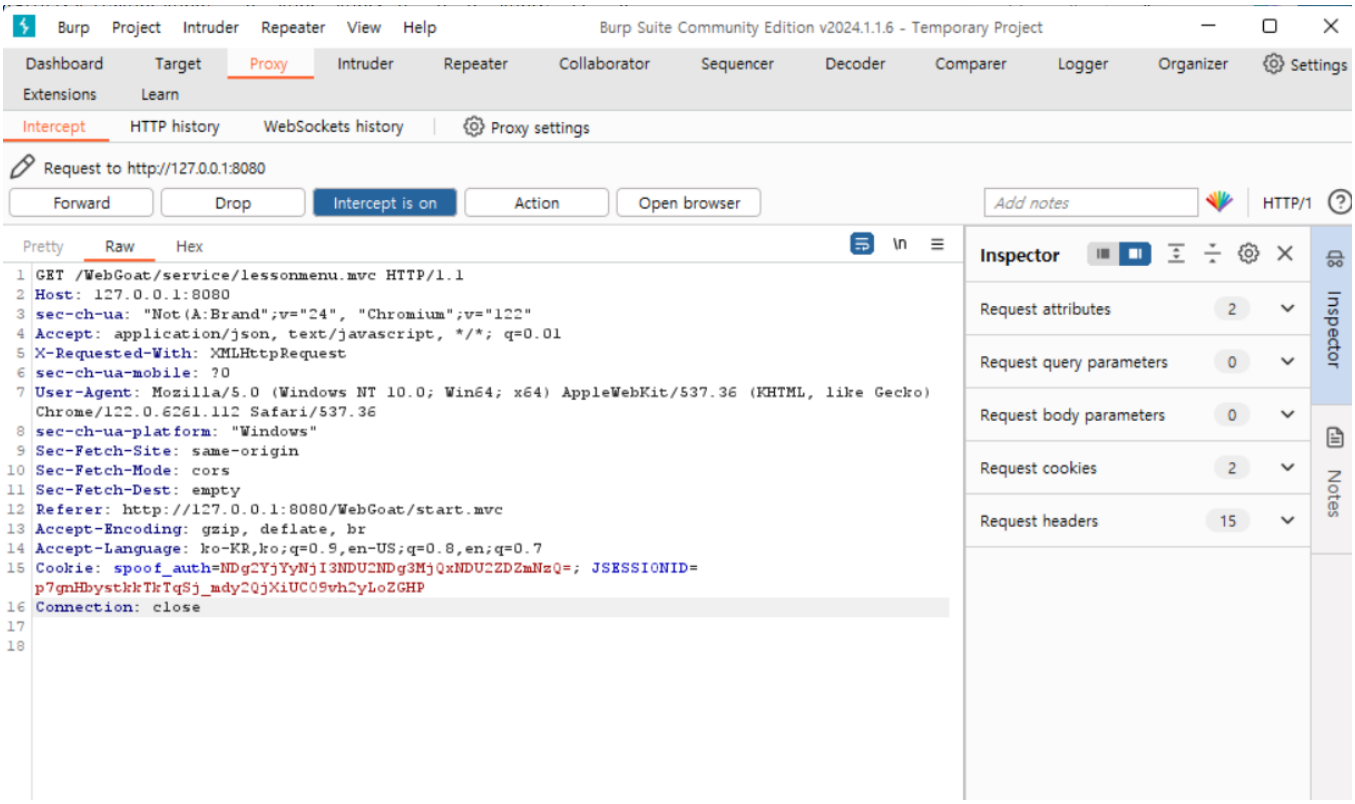
인코딩 된 쿠키 값을 복사



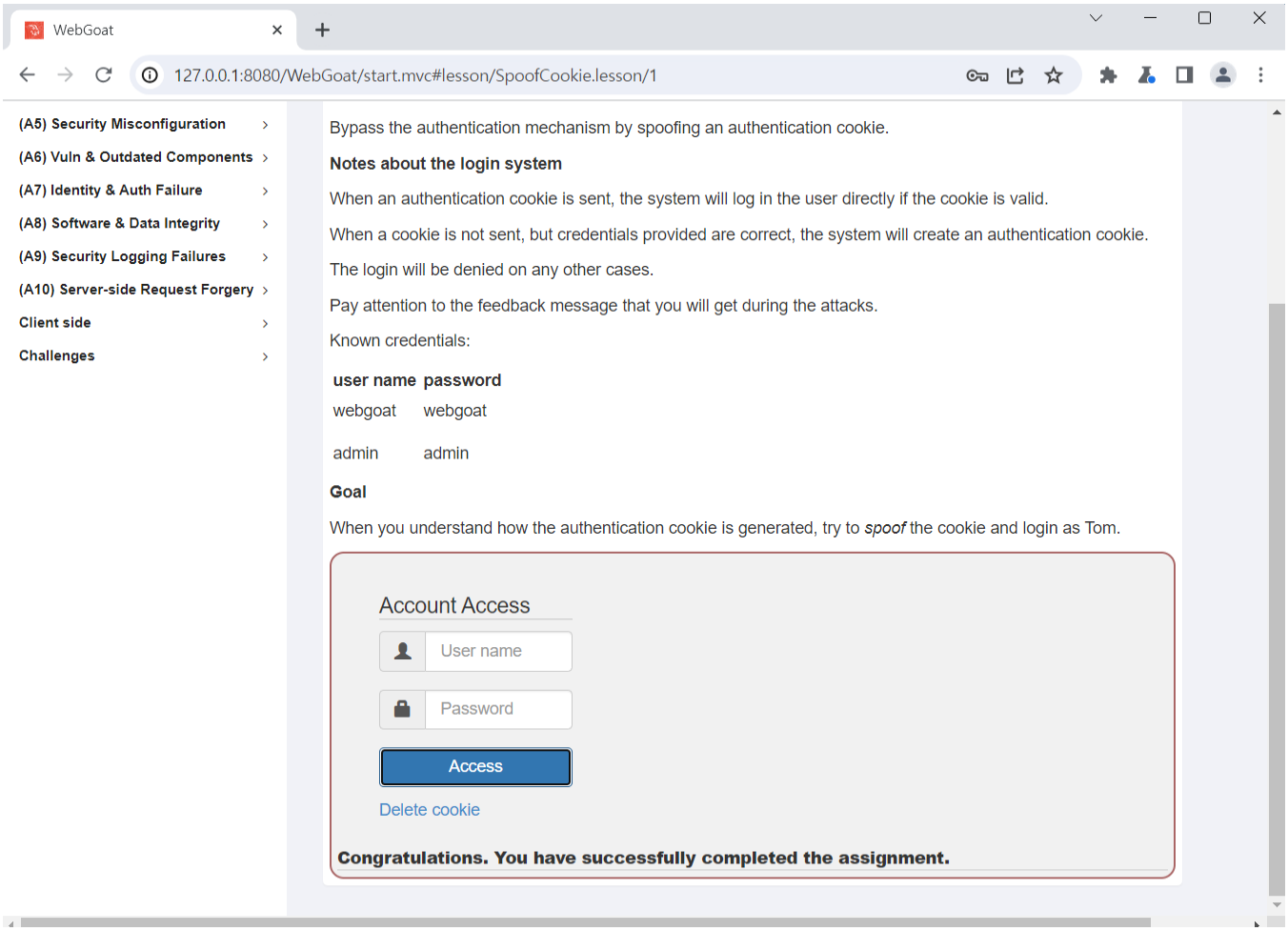
로그인 창으로 가서 tom 계정을 입력, Intercept is on으로 켠 뒤 로그인



복사해 둔 쿠키 값을 'spoof_auth=' 입력후 붙여 넣기 (세미콜론 꼭 붙어야함!)



Intercept is off로 바꾼 뒤 로그인 창으로 가면 성공한 메시지가 뜬다



Spoofing an Authentication Cookie 문제 성공!