□ **단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿**

25년 1학기 인터넷 보안 수업

인터넷 뱅킹 모의해킹

: 10억 대출 받기

2025년 5월 27일

학번 : 32231594
이름 : 박기쁨

<과정 설명>

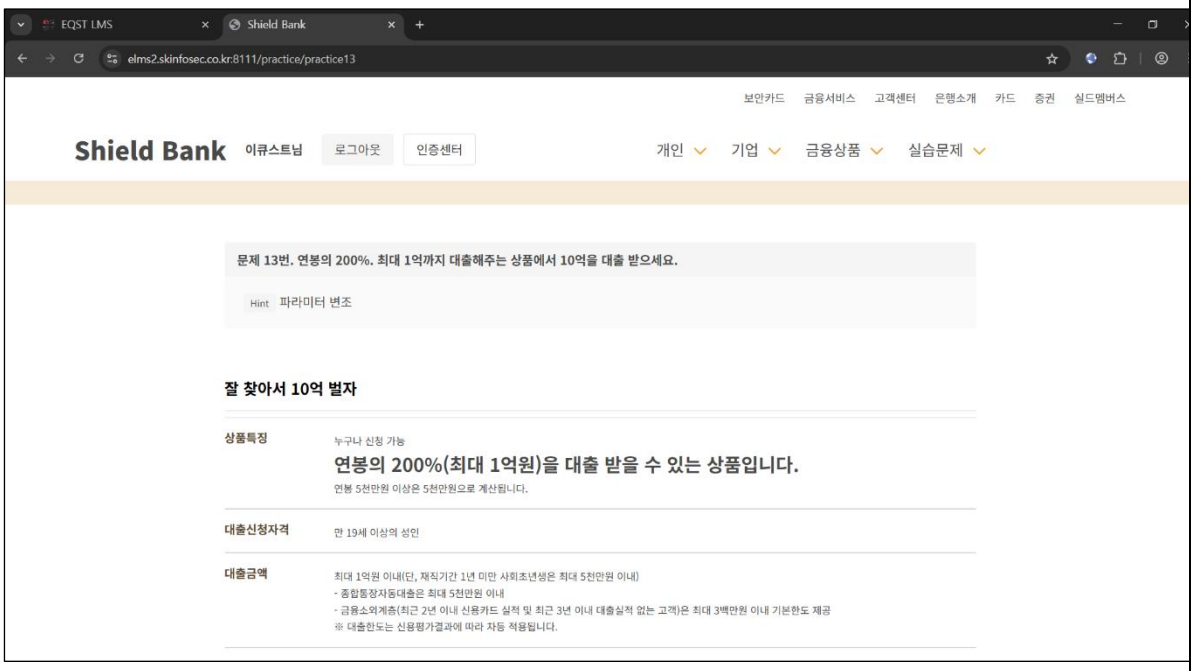
본 실습은 연봉의 200%, 최대 1 억까지 대출해주는 금융 상품 페이지를 해킹하여 10 억을 대출받는 과정을 다룬다.

Step 1. 페이지 동작 방식 확인

Step 1-1. 대출 과정 확인

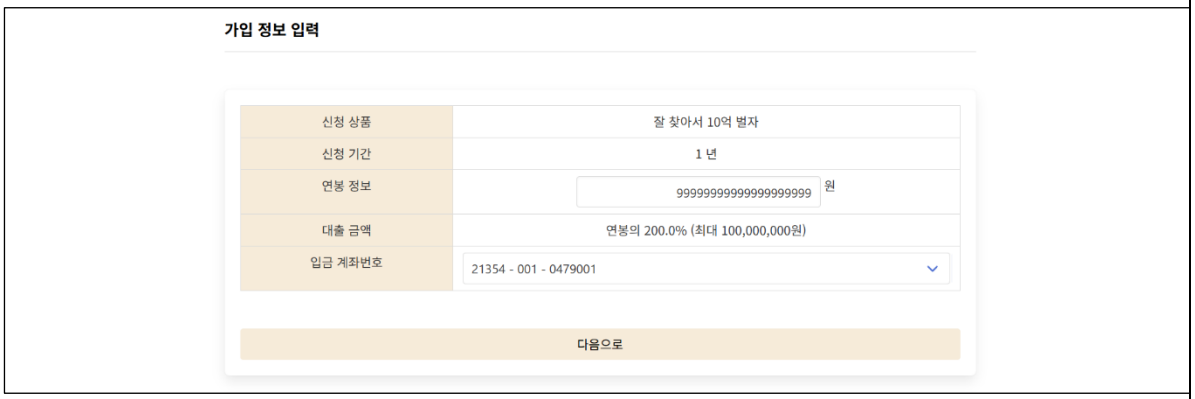
: 상품 페이지를 따라가며 대출 과정을 확인한다.

: 상품 설명에서 연봉 5 천만원 이상은 5 천만원으로 계산된다는 내용을 확인할 수 있다.



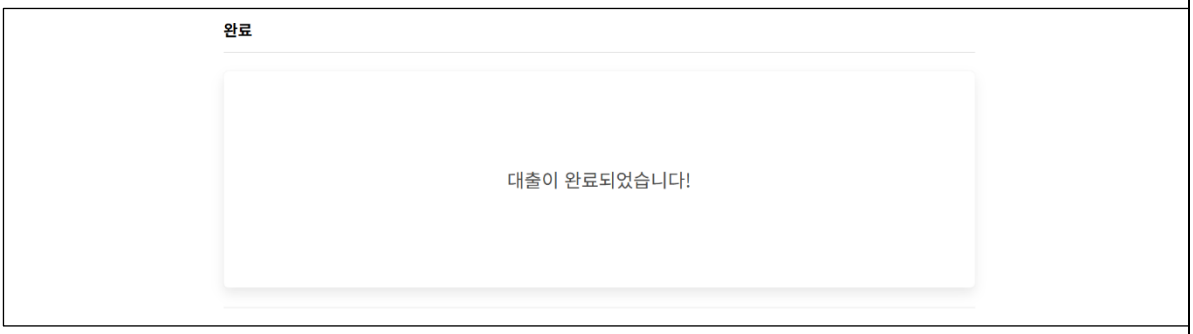
: 신청 버튼을 누르면, 연봉과 계좌번호를 입력하는 가입 정보 입력 페이지로 넘어간다.

: 연봉을 9999999999999999999 원으로 입력해본다.



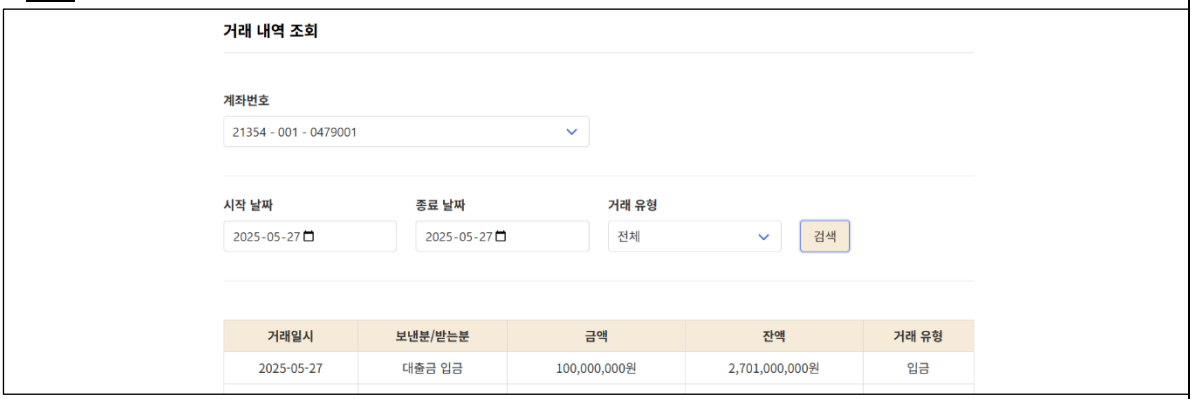
: 정보 입력 후 '다음으로' 버튼을 누르면, 계좌번호와 비밀번호, 보안카드 번호를 입력하는 사용자 인증 페이지로 넘어간다.

: 정보 입력 후 공동인증서 인증을 마치면, 마지막 페이지로 넘어가며 대출이 완료된다.



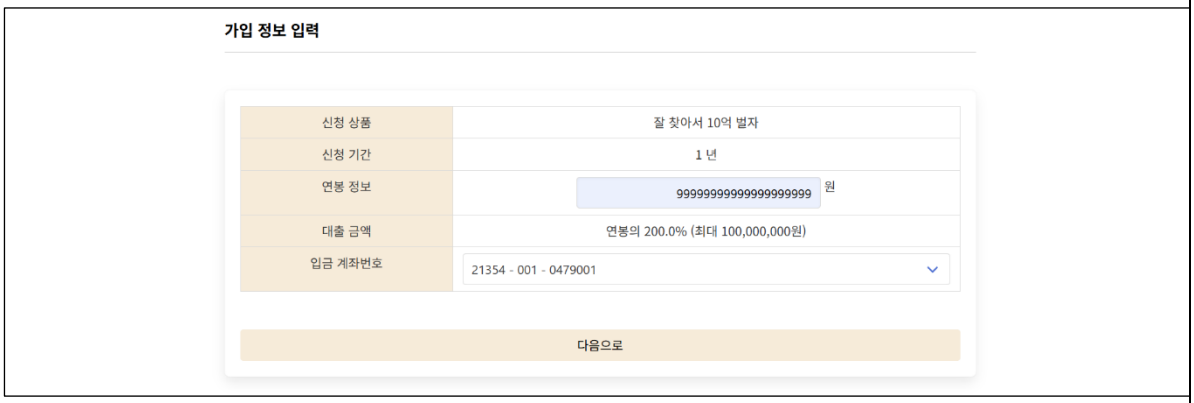
: 거래 내역 조회 페이지에서 대출이 성공적으로 이루어졌음을 알 수 있다.

: 연봉을 9999999999999999999 원으로 입력하였지만 5 천만원으로 계산되어, 연봉의 200%인 1 억이 대출되었음을 알 수 있다.

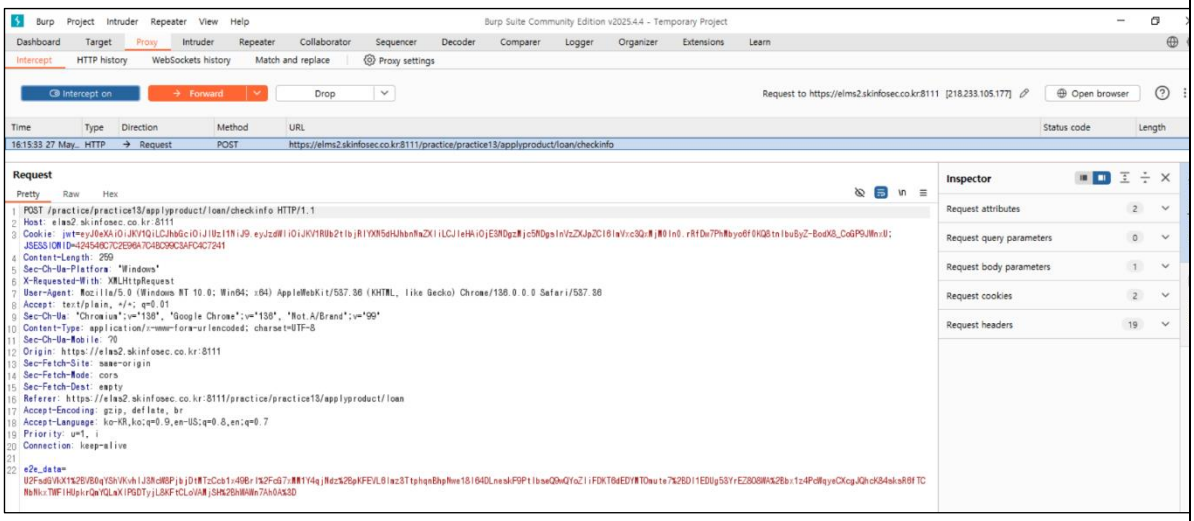


Step 1-2. 패킷 확인

: 가입 정보 입력 페이지에서 연봉 정보가 패킷에서 어떻게 전달되는지 확인한다.



: Burp 를 이용하여 패킷을 intercept 해보면, 파라미터와 파라미터 값들이 암호화되어 전달되고 있음을 알 수 있다.



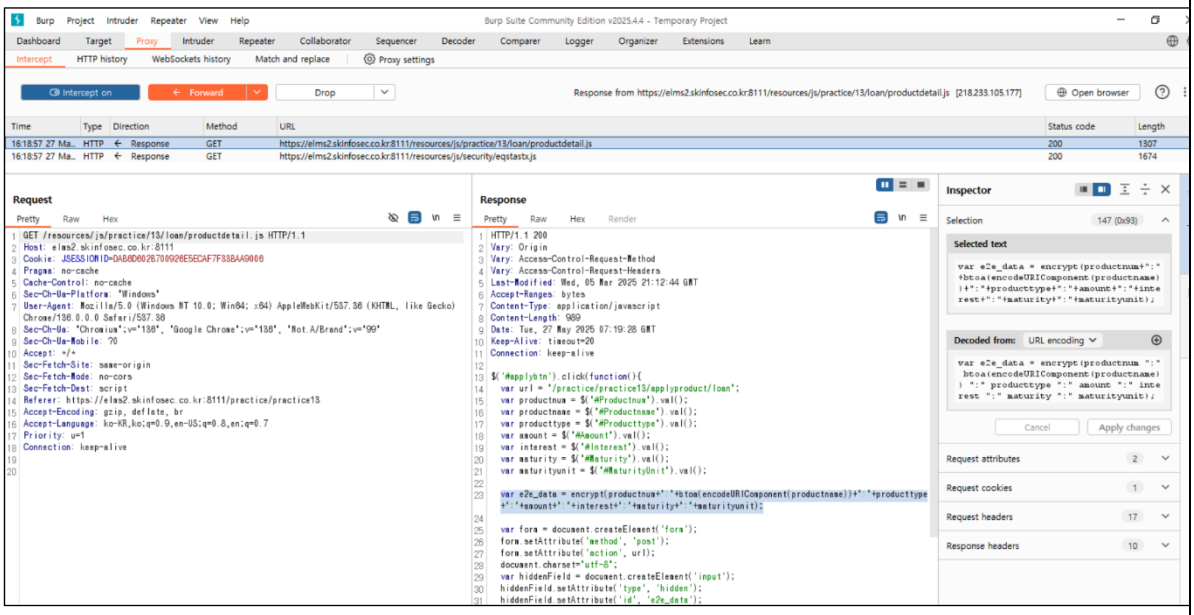
Step 2. prompt 를 이용한 파라미터 변조

Step 2-1. prompt 문 삽입

: 패킷의 파라미터 값들이 암호화되어 전달되고 있으므로, 패킷을 intercept 하여 실시간으로 변조하는 것은 불가능하다.

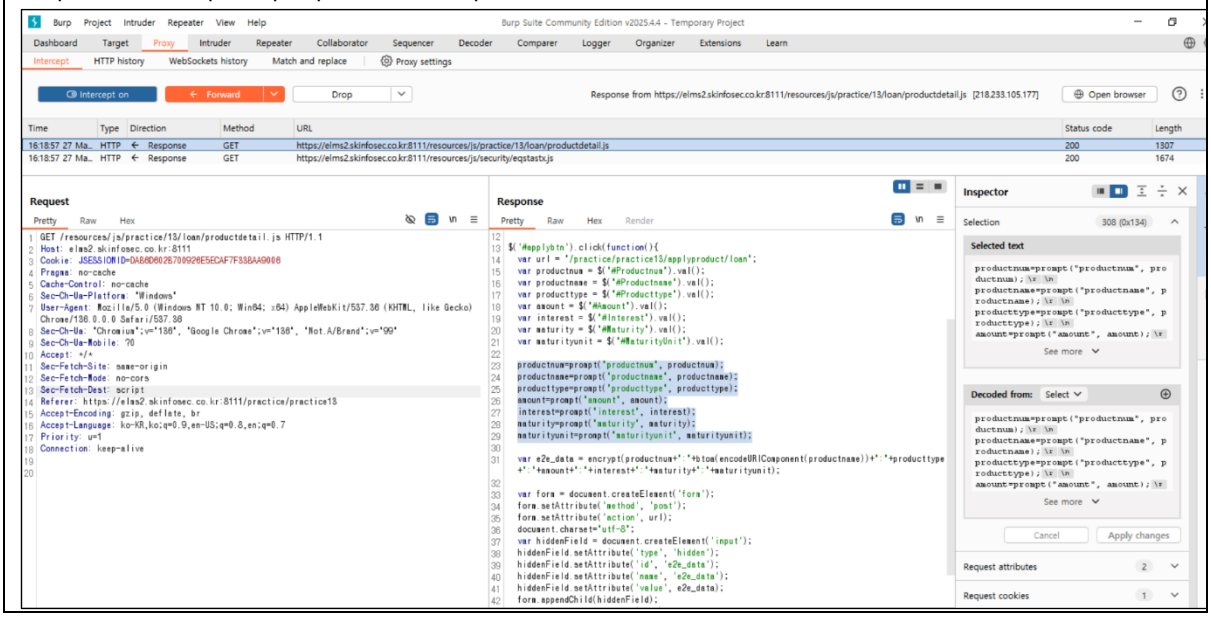
: 페이지의 소스코드에 prompt 문을 삽입하고, 띄워진 prompt 를 이용하여 파라미터 값을 변조한다.

: 페이지 최초 로드 시 전달되는 productdetail.js 파일을 intercept 하여 소스 코드를 확인해보면, E2E 암호화가 실행되는 부분을 확인할 수 있다.

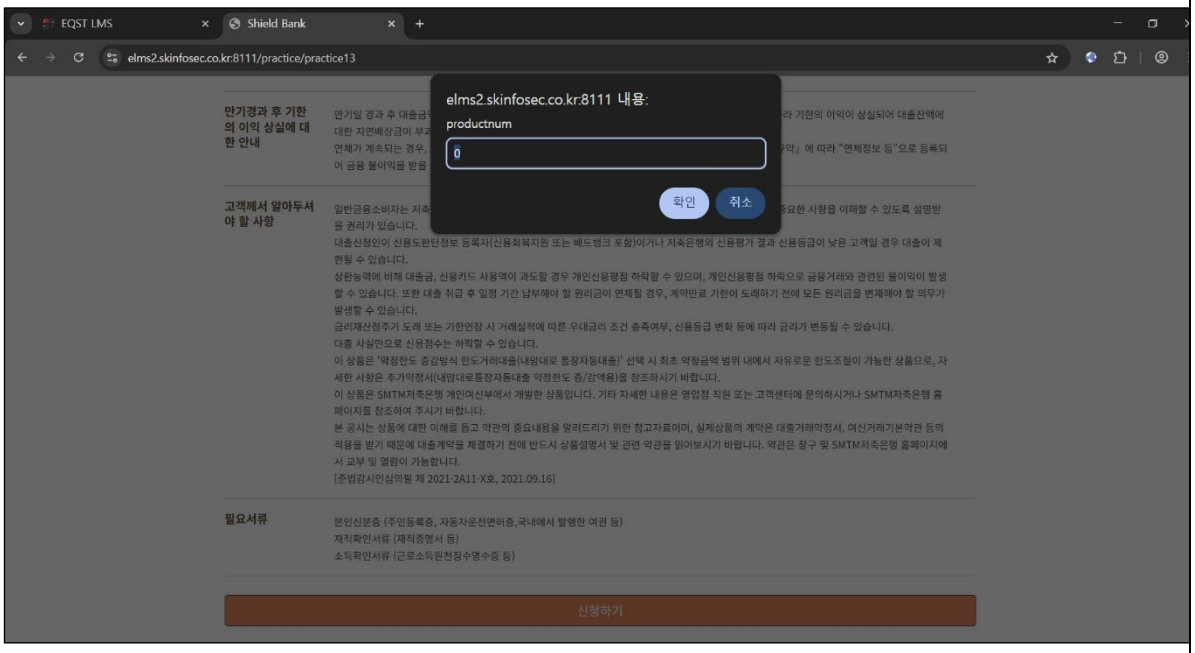


: E2E 암호화 코드 바로 앞에, 모든 파라미터에 대한 prompt 문을 작성하여 삽입한다.

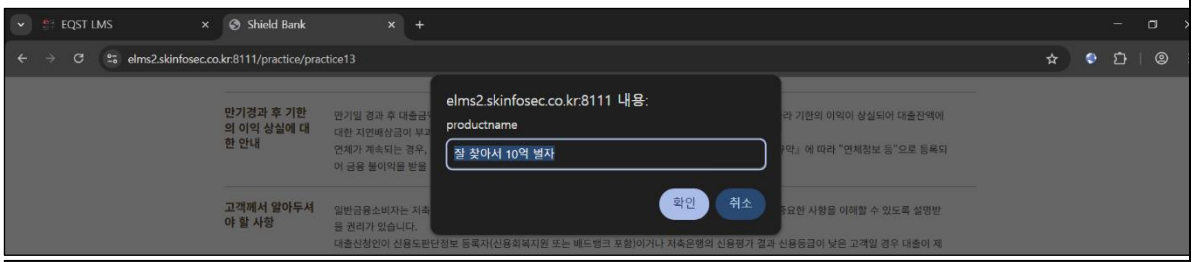
({parameter}=prompt("parameter", {parameter}))

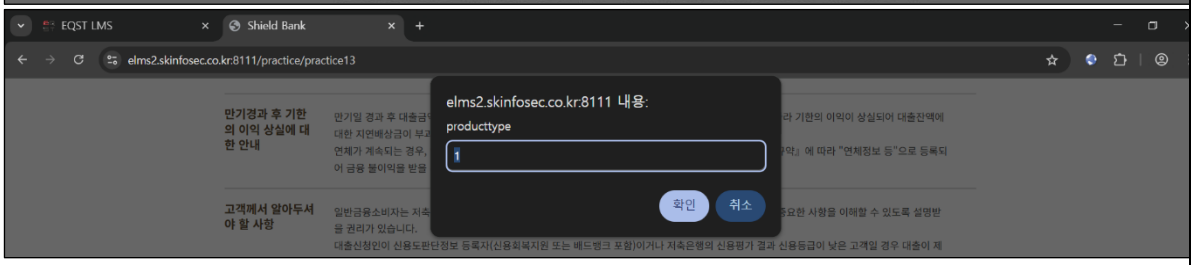


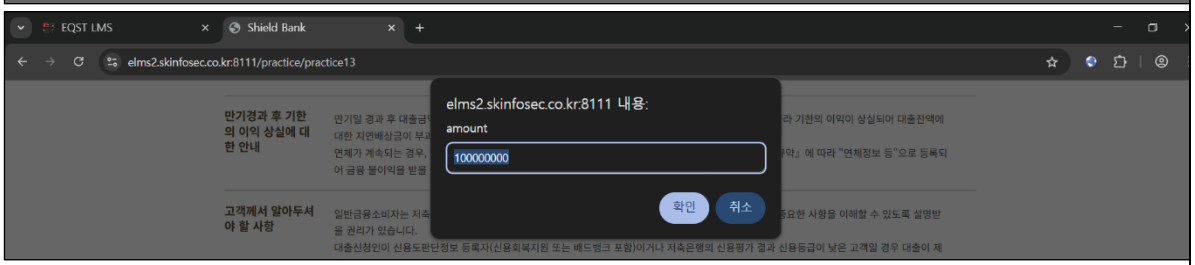
: intercept 를 해제한 후 페이지로 돌아가 신청하기 버튼을 누르면 prompt 창이 띄워지며, 파라미터와 파라미터 값에 접근할 수 있게 된다.

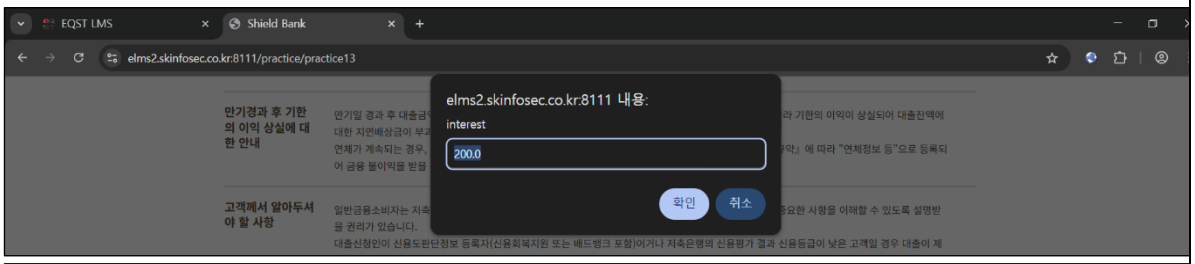


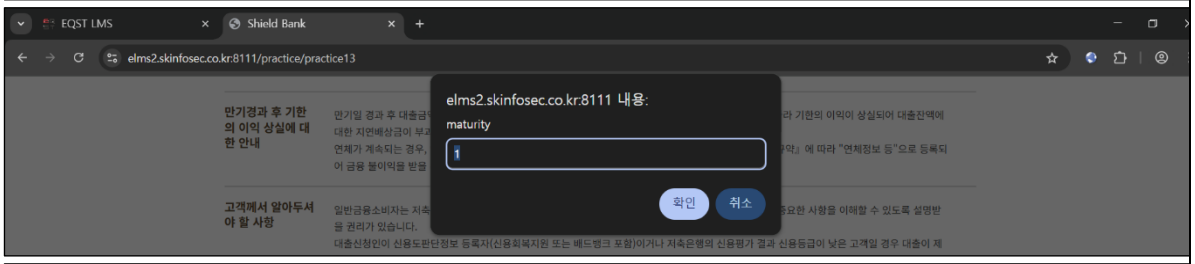
(모든 파라미터와 파라미터 값이 prompt 로 띄워진다.)

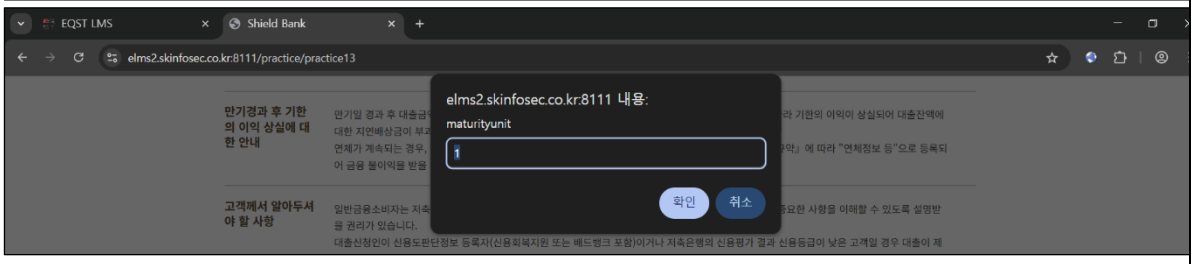






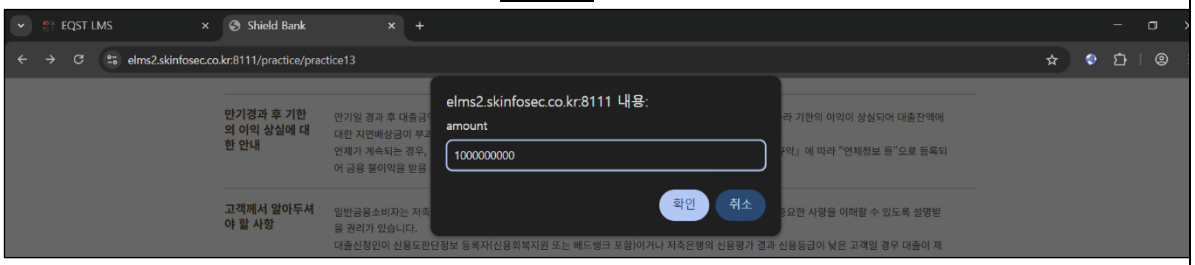






Step 2-2. prompt 를 이용한 파라미터 변조 시도 (amount)

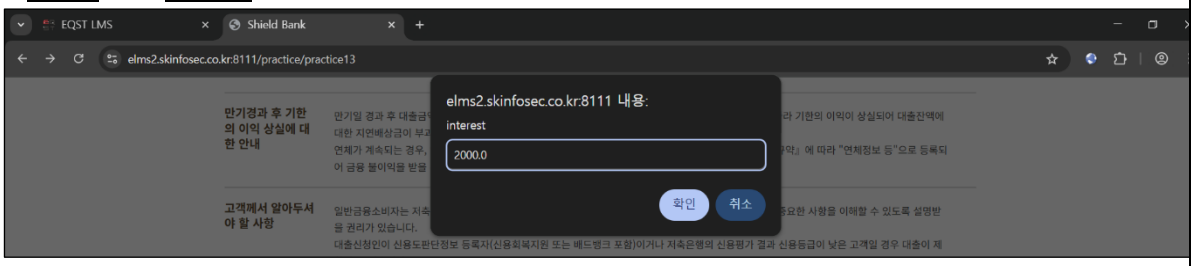
: 최대 대출 금액 파라미터로 추정되는 amount 값을 1 억에서 10 억으로 변조해본다.



: 잘못된 접근이라는 문구가 있는 에러 페이지로 이어진다.

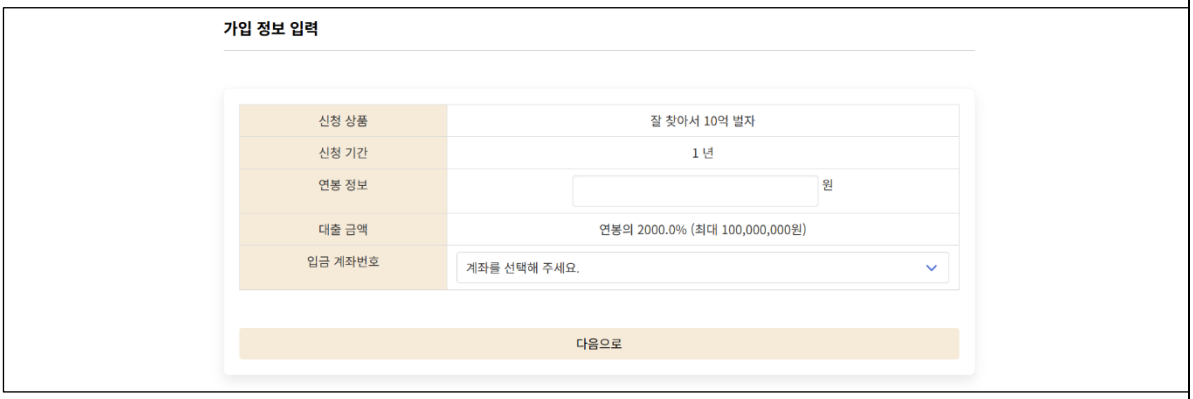
Step 2-3. prompt 를 이용한 파라미터 변조 시도 (interest)

: amount 대신, 최대 대출 금액의 연봉 대비 비율 파라미터로 추정되는 interest 값을 200.0 에서 2000.0 으로 변조해본다.

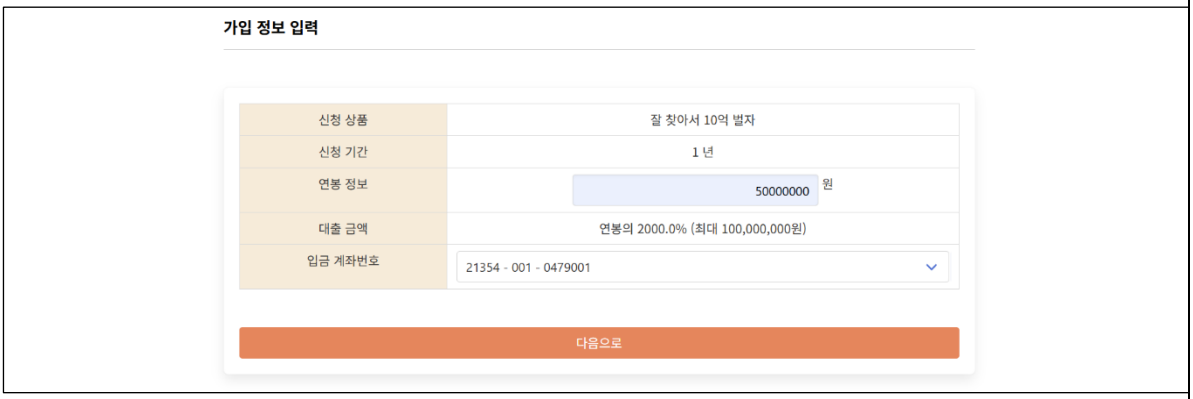


: 가입 정보 입력 페이지로 무사히 이어진다. (타 파라미터들의 값을 변조하면, amount 파라미터 변조 시와 마찬가지로 에러 페이지로 이어진다.)

: 최대 대출 금액의 연봉 대비 비율이 200.0%에서 2000.0%로 변조되었음을 확인할 수 있다.



: 기타 정보들을 입력한 후 '다음으로' 버튼을 누른다.



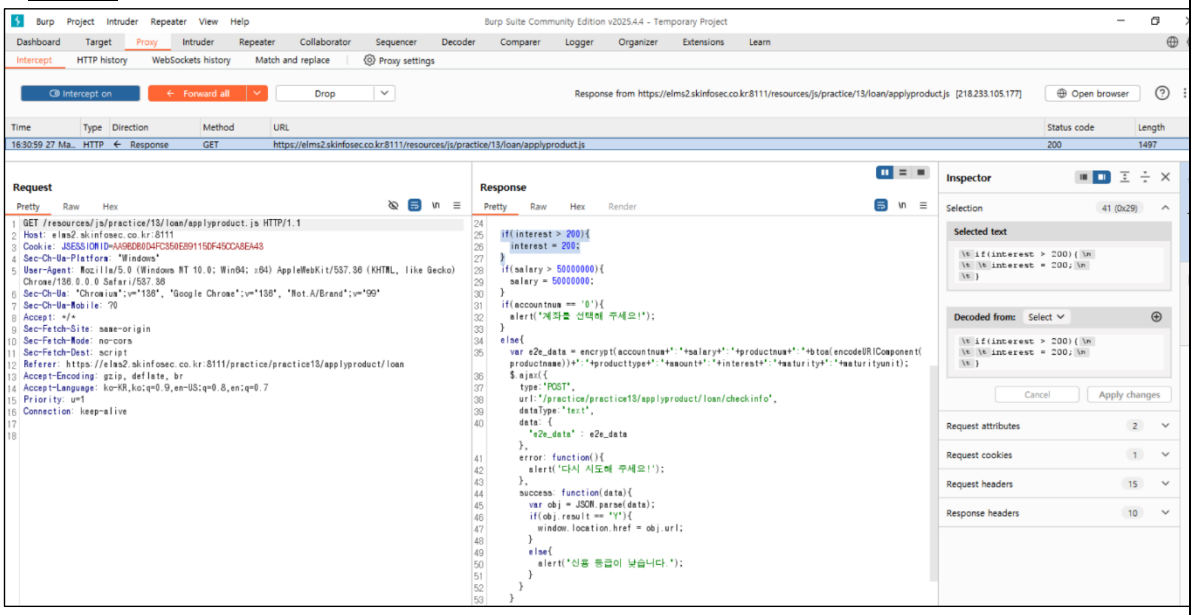
: "신용 등급이 낮습니다."라는 문구의 알림창이 띄워진다.

Step 3. 두 번째 페이지 소스코드 변조

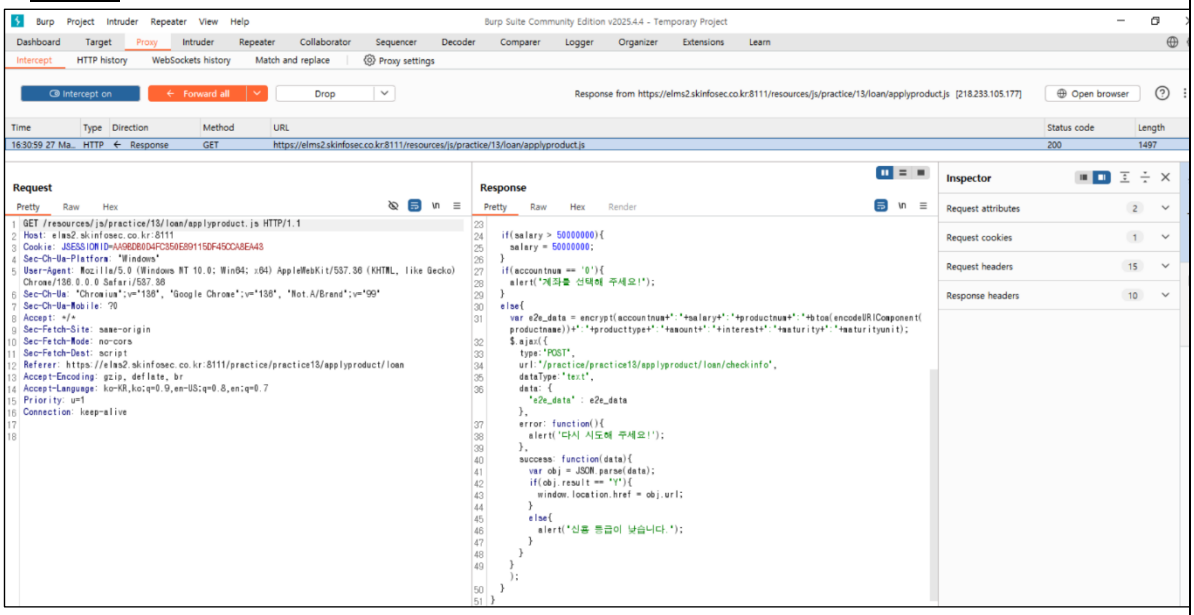
Step 3-1. 두 번째 페이지 소스코드 확인

: applyproduct.js 파일을 intercept 하여 소스 코드를 확인해보면, 모종의 이유로 obj.result 값이 Y가 아닌 다른 값으로 설정되어 "신용 등급이 낮습니다" 문구가 띄워졌음을 알 수 있다.

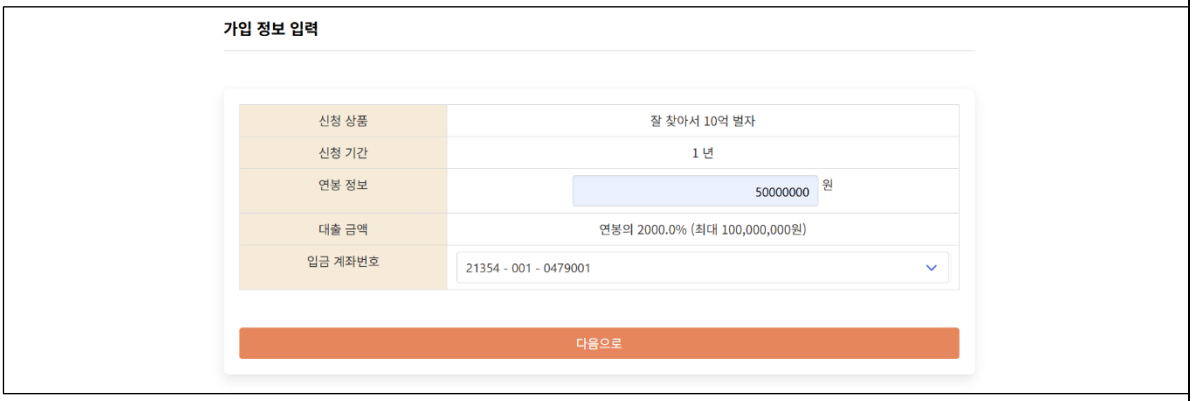
: 이전 페이지에서, prompt 를 이용하여 유일하게 interest 파라미터 값만 변조하였으므로, interest 파라미터 관련 코드에서 오류가 발생했을 가능성이 가장 높다.



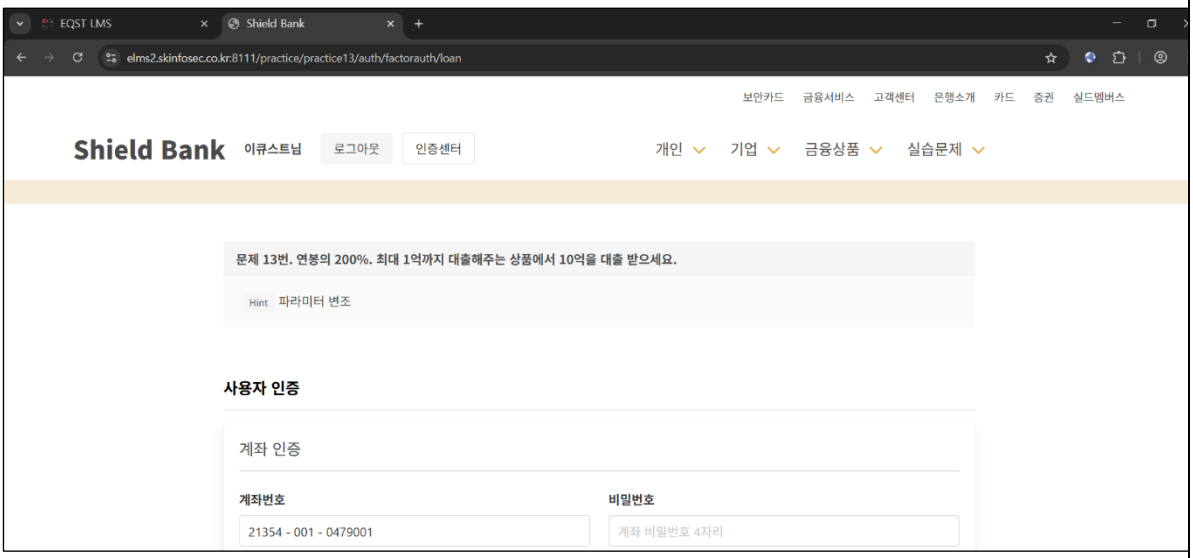
: interest 값을 200 이하로 제한하는 코드를 삭제해본다.



: 코드 변조 후 intercept 를 해제하고, 기타 정보들을 입력한 후 '다음으로' 버튼을 눌러본다.

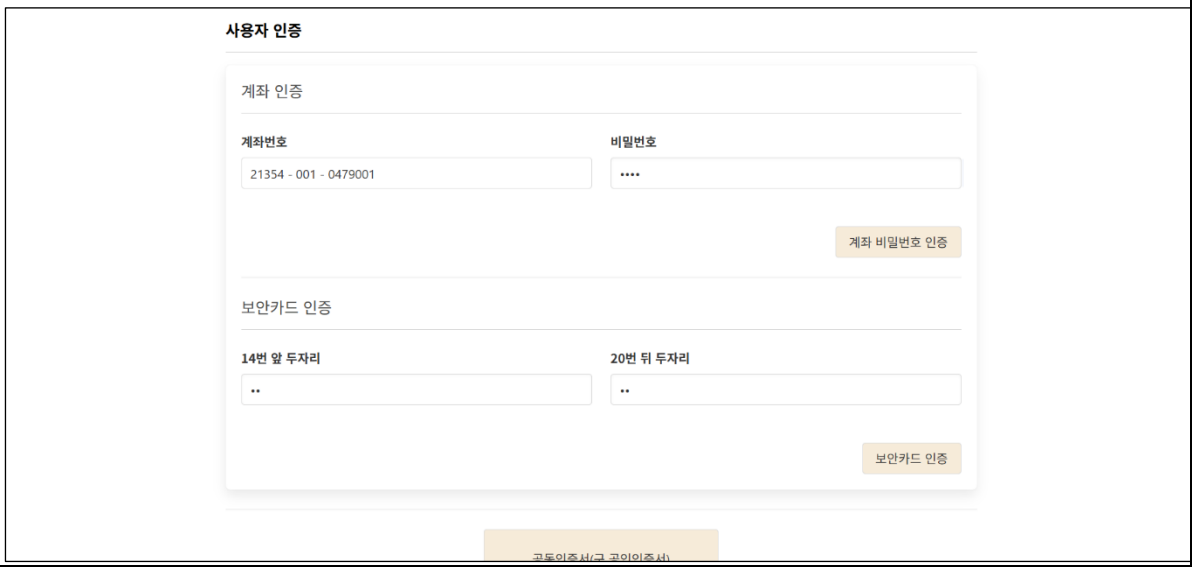


: 사용자 인증 페이지로 무사히 이어진다.

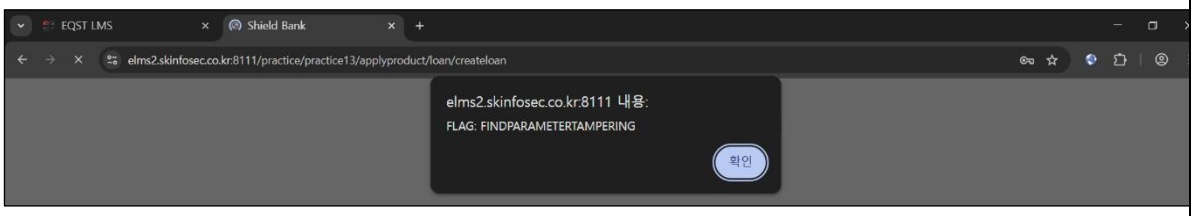


Step 3-2. 정보 입력 및 10 억 대출

: 계좌번호와 비밀번호, 보안카드 번호를 입력한 후 공동인증서 인증을 마친다.



: 10 억 대출에 성공하여 FLAG 를 획득할 수 있다. **(FLAG: FINDPARAMETERTAMPERING)**

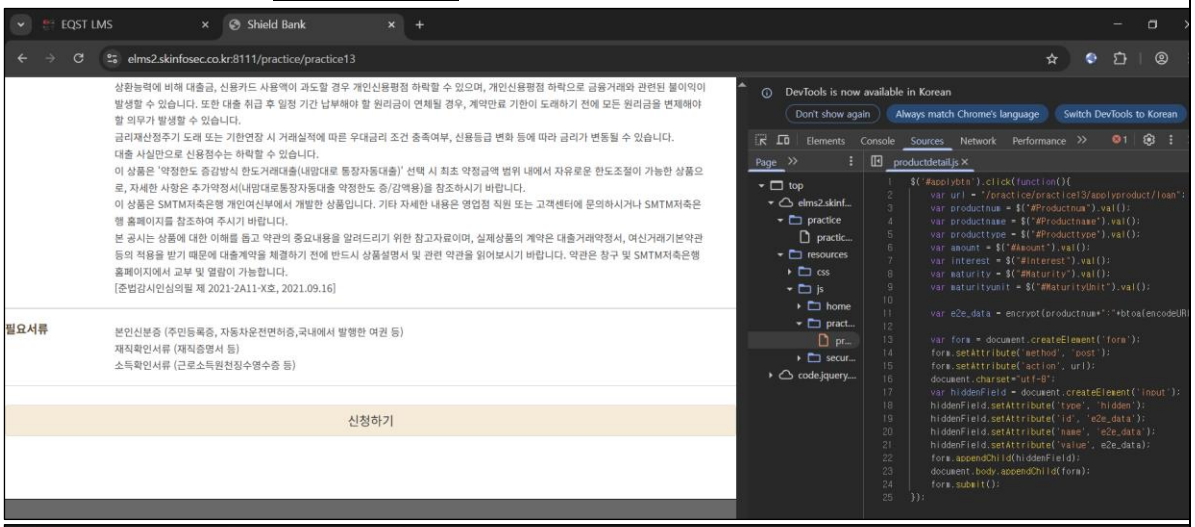


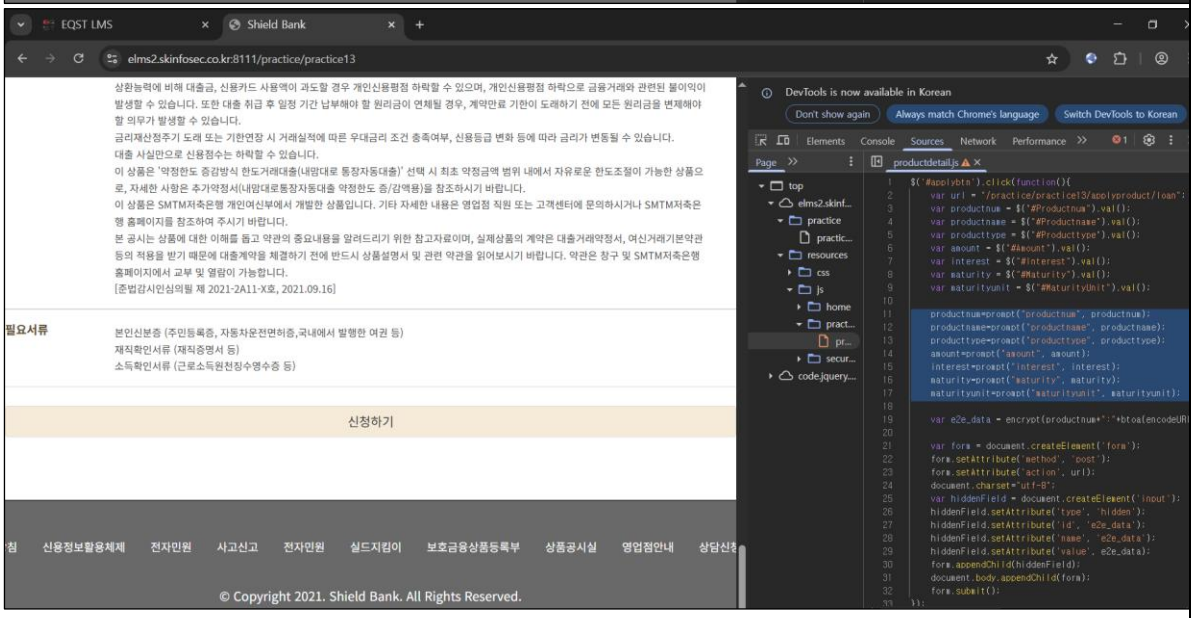
: 거래 내역 조회 페이지에서도 10 억 대출 내역을 확인할 수 있다.

Step X. 기타 방법 (개발자도구 이용)

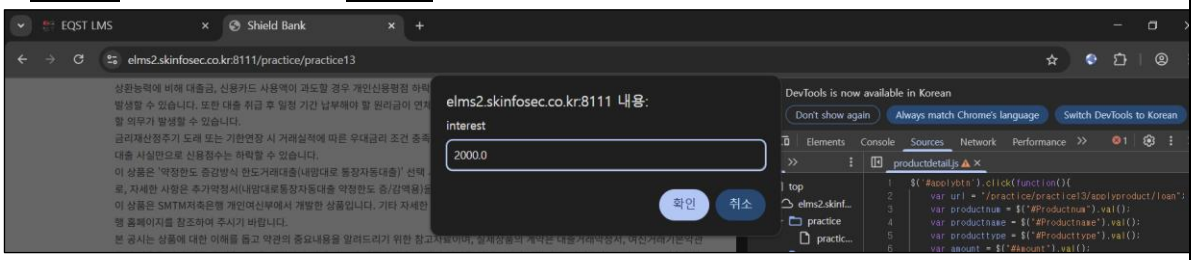
금융권 실무에서는 개발자도구 사용이 막혀 있는 경우가 많아 본 실습에서도 개발자도구를 사용하지 않았지만, 개발자도구를 사용하여 보다 간편하게 실습을 진행할 수 있다.

: 개발자도구를 통해 productdetail.js 파일의 소스코드를 확인하고 prompt 문을 삽입한다.

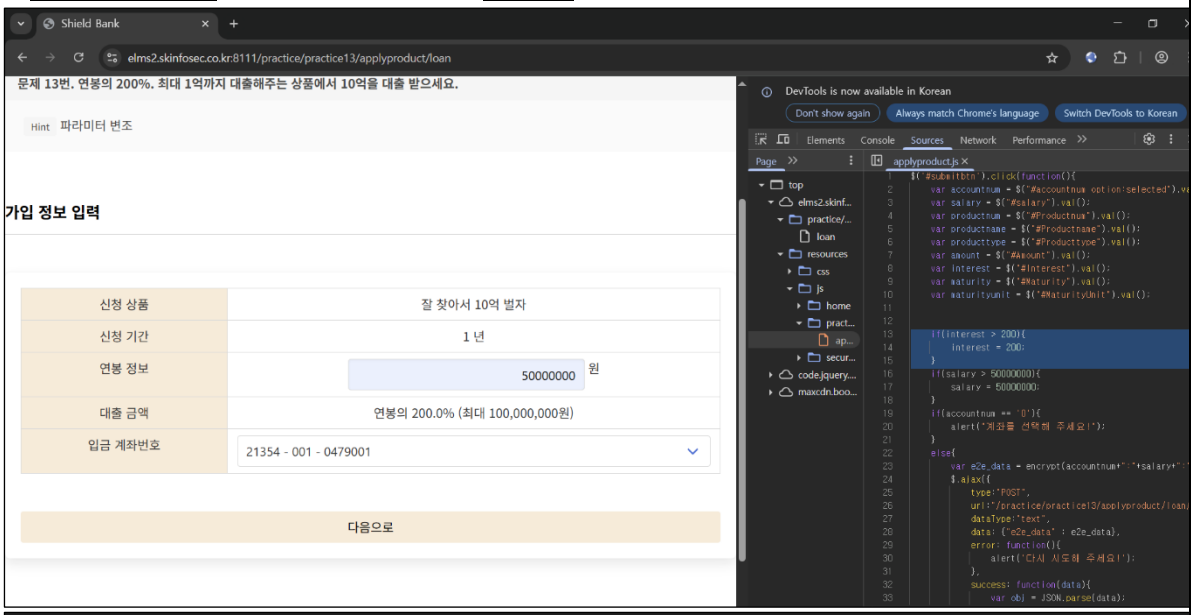


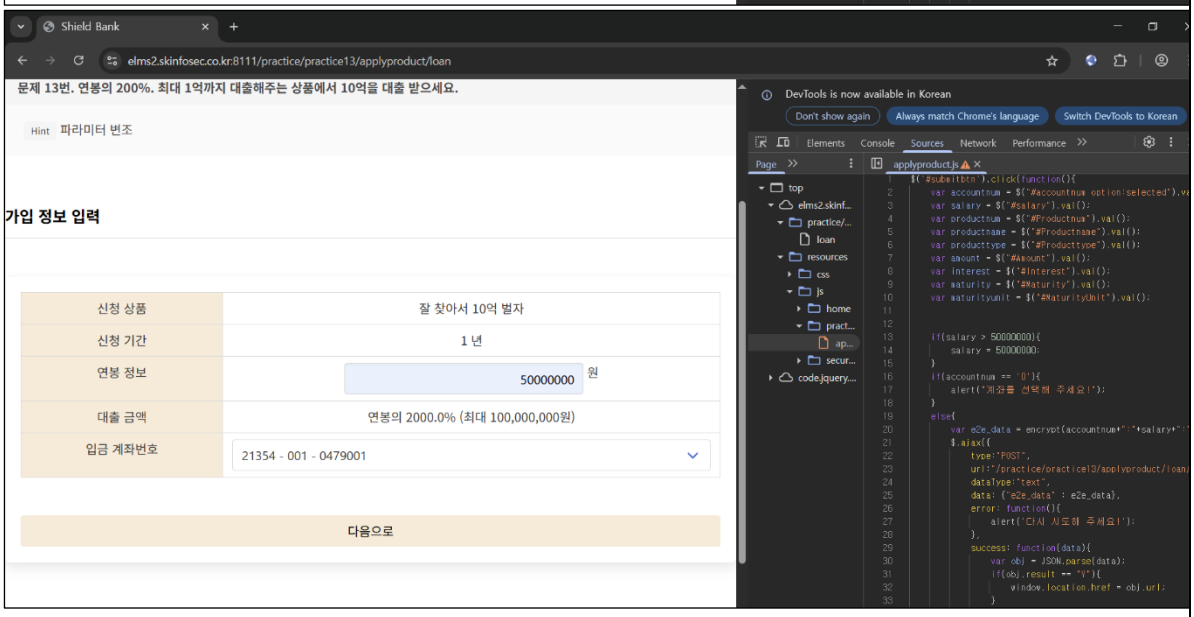


: interest 파라미터의 값을 2000.0 으로 변조한다.

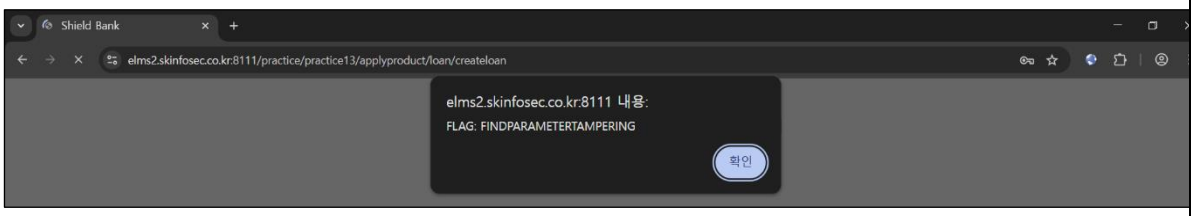


: applyprodunt.js 파일의 소스코드 중 interest 값을 제한하는 코드를 삭제한다.





: 마찬가지로 10 억 대출에 성공하여 플래그를 획득한다.



성명	프로젝트 후 소감
박기쁨	지금까지의 실습은 그날 배운 내용을 적용해볼 수 있는 단순한 페이지에서의 실습이었다면, 이번 실습은 실제 금융 사이트와 흡사한 사이트에서 진행되어 더욱 재밌고 특별한 실습이었던 것 같다. 파라미터를 변조하는 방법 중 프롬프트를 이용하는 방법을 처음 배웠는데, 패킷을 intercept 하여 실시간으로 변조하는 방법을 사용할 수 없을 때, 소스코드를 변조하는 방법도 시도해볼 수 있다는 사실을 알게 되었다.