Etap 2

Wstęp

W drugim etapie kluczowa podatność została poprawiona. Administrator postanowił wymusić na użytkownikach podporządkowanie się konkretnym zasadom tworzenia hasła, jednak z łatwością jesteśmy w stanie stwierdzić, że nie zapewniają one odpowiedniego poziomu bezpieczeństwa. Te zasady to:

- Hasło musi być 5 znakowe
- Może składać się ze znaków z tej listy: agresoy!@#$%

Crunch

Przykładowe polecenie:

```
crunch 1 3 PIKACHU -o plik.txt
```

W tym poleceniu cyfry oznaczają zakres długości haseł, PIKACHU oznacza litery, których program użyje do wygenerowania haseł, parametr -o mówi do jakiego pliku crunch tą listę wypisze. W tym konkretnym wypadku wygenerowana zostanie lista z 1,2 i 3 znakowymi hasłami, które zawierają znaki ze słowa PIKACHU. **Bardzo ważne: wielkość liter ma znaczenie!**

Zadanie

Sprawdź w bazie danych, jaki użytkownik w niej widnieje (tabela users), a następnie złam jego hasło. Aby wygenerować listę wszystkich możliwych haseł posłużymy się programem Crunch.