

7. Взлом паролей (pass)

50 очков

Компьютерная фирма ABCDEF-software создала веб-приложение. В приложении есть модуль управления пользователями, про который известно следующее:

- имя пользователя и пароль могут быть длиной 1 . . . 20 знаков, и состоять из латинских символов A . . . Z, a . . . z, или цифр 0 . . . 9;
- имена пользователей должны быть уникальными;
- имена пользователей и пароли чувствительны к регистру.

Вам доступны две функции данного модуля:

- показ списка всех имен пользователей;
- создание нового пользователя с заданным именем и паролем.

В модуль уже введены некоторые пользователи, а ваша задача – установить их пароли.

Оценивание. В качестве решения необходимо предоставить текстовый файл, в каждой строке которого даны имя пользователя и его пароль, разделенные пробелом. При оценивании учитывается количество правильно определенных паролей, а так же количество добавленных в систему новых пользователей:

1. Все решения, которые корректно определили хотя бы один пароль, упорядочиваются по количеству определенных паролей.
2. Если два решения корректно определили одинаковое количество паролей, лучшим считается решение, которое добавило в систему меньше новых пользователей.
3. Первое решение в полученном рейтинге получает 50 очков, последнее –5 очков; остальные решения получают очки пропорционально их расположению в списке.

Примечание. Суть данной задачи – определение паролей с помощью двух предоставленных функций, а не атака на сервер любым другим образом. Разрешено (и даже советуется) использовать программы, которые будут автоматически посылать необходимые запросы, но это необязательно. Стоит помнить, что при добавлении слишком большого количества пользователей работа модуля может стать слишком медленной или вообще прерваться.

Использование модуля управления пользователями

Модуль доступен по адресу <http://cms.eio.ut.ee/pass/>.

Для использования необходимо первым делом авторизоваться с помощью того же имени и пароля, которые вы использовали для логина на сайт соревнования <http://cms.eio.ut.ee/>. В результате модуль выдаст браузеру куки (*cookie*, https://ru.wikipedia.org/wiki/HTTP_cookie), которое действует в течение всего соревнования. (Если вы желаете решать задачу с помощью скриптов, не нужно программно реализовывать логин на модуль – достаточно добавить это куки к посылаемым запросам).

Вы можете использовать две версии модуля:

1. <http://cms.eio.ut.ee/pass/test.cgi>

Эта версия содержит дополнительную функцию сброса, которая удалит всех созданных вами пользователей и восстановит изначальное состояние модуля. Эту версию можно использовать для тестирования своего решения – пунктов за угадывания паролей в этой версии получить невозможно.

Изначальное содержание базы пользователей в данной версии таково:

```
'adam','eve'  
'joe','hacker1'  
'bill','1234'
```

2. <http://cms.eio.ut.ee/pass/live.cgi>

В данной версии нет функции сброса, и для каждого участника изначально сгенерирован уникальный набор пользователей и паролей. Оцениваются лишь угаданные пароли для этой версии модуля.

Модуль принимает следующие параметры в строке запроса:

- **q=list** — показывает список пользователей в базе; дополнительных параметров нет;
- **q=reset** — сбрасывает базу в начальное состояние; дополнительных параметров нет;
- **q=adduser** — добавляет нового пользователя; дополнительные параметры: **user=**, **pass1=**, **pass2=** (имя создаваемого пользователя и пароль, повторенный дважды, как принято у форм выбора паролей).

К модулю можно обращаться как **GET** так и **POST** запросами. Модуль отвечает только на авторизованные запросы (т.е. содержащие корректные куки).