Summer University, Web Security Lab 1, July 2015 Name: Jorge Gallegos, Will Simons, Bastian Gardel, Raphael Mas

Group: Asterix

These exercises are designed to give you a taste of how an attacker might attempt to compromise a site's security. The site we will work with is http://cs31.cs.sjsu.edu/⟨**group**⟩, where ⟨**group**⟩ is the name given to your group. It is designed as a resource for superheros; we'll play the role of the supervillains and try to attack the site.

1. (10 points) Go to http://cs31.cs.sjsu.edu/⟨**group**⟩/login1.php and try to log in to the site. Review some common passwords from
   `http://www.zdnet.com/article/25-most-used-passwords-revealed-is-yours-one-of-them/`
   Find a username and password and use it to log in to the website. (Note that the usernames are all based on the names of superheroes).
   What username did you discover? _____
   What is the password for that username? _____
   What steps did you take to find this password?

2. (10 points) Using SQL injection, get the full password list, stored in the `user1` table, Note that the page http://cs31.cs.sjsu.edu/⟨**group**⟩/thanks.php does not properly sanitize its input. Describe what you did and list all username/password combinations in the table.

3. (10 points) Add a new account to the `user1` table. Verify that you are able to log in. Describe how you did it.

4. (15 points) To break into a site might require a little detective work.
The page http://cs31.cs.sjsu.edu/⟨**group**⟩/villains.php shows a list of Batman's allies and enemies.
For this question, you will need to deduce table names and other details about the site's design.

   (a) Change the status of the Joker to "Reformed". Describe how you did it.

   (b) Add Commissioner Gordon to the list of villains, Describe how you did it.

   (c) Delete the record for Talia al Ghul altogether. Describe how you did it.

5. (15 points) After realizing that the site has been compromised, the site developers have started to hash their passwords. The new login page is http://cs31.cs.sjsu.edu/⟨**group**⟩/login2.php and the new table is `user2`. Through experimentation, you have discovered that the passwords are hashed with MD5 (https://en.wikipedia.org/wiki/MD5).

   (a) Determine as many passwords as you can. List the username/password combinations.
   You may find this url helpful: `http://md5.gromweb.com/`.

   (b) Discuss the choice of MD5 for the hashing function. Why is it a good or not-so-good choice? Would another hashing function been better? Why or why not?

6. (10 points) The site designers attempt to foil your attack by the use of salt values:

```
md5(salt + password)
```

For this exercise, the page is http://cs31.cs.sjsu.edu/⟨**group**⟩/login3.php and the table name is `user3`.

Write a program in your language of choice to crack as many of the passwords in the `user3` table as possible. Use the list of common passwords from http://cs31.cs.sjsu.edu/passwords.txt. (copied from `http://dazzlepod.com/site_media/txt/passwords.txt`.) Write the cracked username/password combinations.

7. (10 points) The site developers improve their site again to include an unknown pepper value. You have learned that the pepper value is a number between '0' and '9'. The hashing function is:

```
md5(salt + pepper + password)
```

The new login page is http://cs31.cs.sjsu.edu/⟨**group**⟩/login4.php and the table name is `user4`.

(a) Update your code from the previous section to determine this pepper value.

(b) What username/passwords can you determine from the `user4` table?

(c) How much longer did your program take to run?

(d) How much slower would your code have run if the pepper were between 0 and 999,999?

8. (10 points) The site contains http://cs31.cs.sjsu.edu/⟨**group**⟩/secret-identities.php, which is only visible to Batman. Determine the secret identities of the following characters.

Darkwing Duck: _____
Stupendous Man: _____

(Note: There may be multiple ways of determining these identities.)
(Note: Using Google to find the secret identities is cheating.)