Secure Password Storage in PostgreSQL

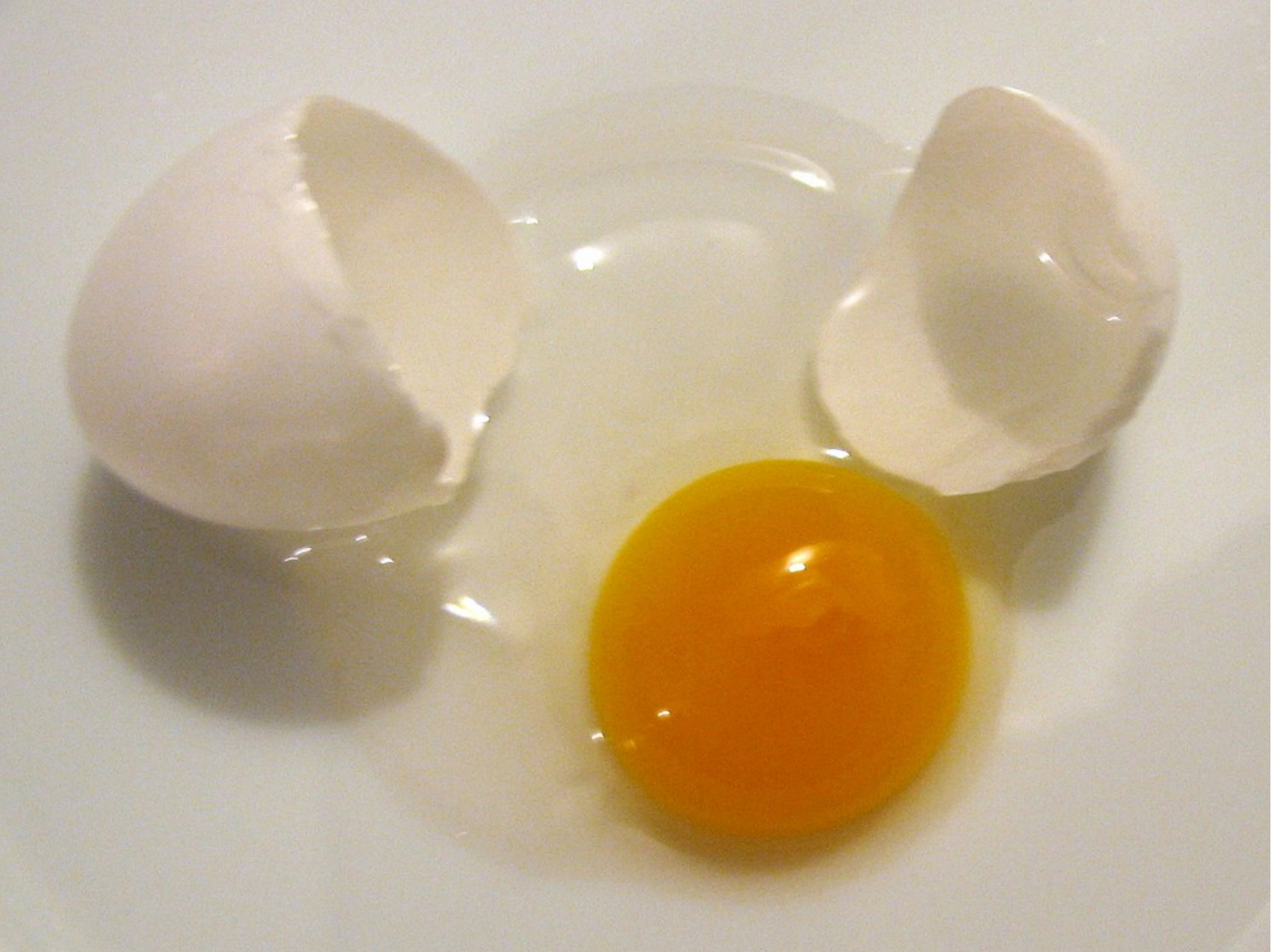
PGDay.IT 2011

Prato, Italy

Magnus Hagander
magnus@hagander.net
@magnushagander

Whats is this about

- Building (web) applications
- That deal with users



The Top 50 Gawker Media Passwords

Article | Video | Comments (152)

Email | Print | Like | Send | + More | Text

By Zachary M. Seward and Albert Sun

Readers of Gizmodo, Lifehacker and other Gawker Media sites may be among the sawiest on the Web, but the most common password for logging into those sites is embarrassingly easy to guess: "123456." So is the runner-up: "password."

Find Out if Your Passwords Were Leaked by LulzSec Right Here

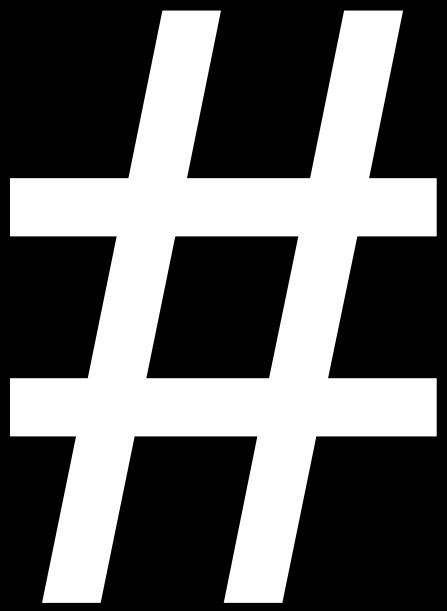
Another day, another giant LulzSec data dump. This time, the target's not the US government or a big company, but a sprawling list of 62,000 internet strangers (and their login data). Are you one of them? Find out.

Home » articles, news

Statistics from 10,000 leaked Hotmail passwords

Submitted by Bogdan Calin on October 6, 2009 – 7:54 pm **196 Comments**

An anonymous user posted usernames and passwords of over 10,000 Windows Live Hotmail accounts to a web site called PasteBin. PasteBin is currently down for maintenance but I managed to get a copy of the list, and quickly generated some statistics from these passwords.



```
postgres=# CREATE EXTENSION pgcrypto;
CREATE EXTENSION
```

Generating a hash

```
postgres=# CREATE EXTENSION pgcrypto;
CREATE EXTENSION

postgres=# SELECT crypt('topsecret', gen_salt('bf'));
                             crypt
--------------------------------------------------------------
 $2a$06$gtwIVMvGNoClLvD4vqVwAus4OF47mLv0J6XyYylzpAKaf.
(1 row)
```

Generating a hash

```
postgres=# CREATE EXTENSION pgcrypto;
CREATE EXTENSION

postgres=# SELECT crypt('topsecret', gen_salt('bf'));
                             crypt
--------------------------------------------------------------
 $2a$06$gtwIVMvGNoClLvD4vqVwAus4OF47mLv0J6XyYylzpAKaf.
(1 row)
```

Verifying the password

```
postgres=# SELECT name, email FROM users WHERE
  users.userid='mha' AND
  users.pwdhash =
     crypt('topsecret', users.pwdhash);
```

Awesome, we're done?

26,000 email addresses and passwords leaked. Check this list to see if you're included.

By Stephen Chapman | June 12, 2011, 10:03pm PDT

Summary: *Take a few minutes to see if your email address and/or password is included on this list. It may save you a headache or two*

Find if your Email Address Got Leaked through Gawker's Database

oy@hotmail.com
on@google.com

Did the latest Sony hack leak my info?

Enter your email address to check:

check your email / hash

Wrap check in a function

```
CREATE OR REPLACE FUNCTION login(_userid text,
        _pwd text, OUT _email text)
 RETURNS text
 LANGUAGE plpgsql
AS $$
BEGIN
  SELECT email INTO _email FROM users
    WHERE users.userid=lower(_userid)
    AND pwdhash = crypt(_pwd, users.pwdhash);
END;
$$
```

And use that

```
postgres=# select login('mha', 'somethingsilly');
 login
-------

(1 row)


postgres=# select login('mha', 'topsecret');
        login
---------------------
 magnus@hagander.net
(1 row)
```

Just one small problem...

```
postgres=# SELECT * FROM users;
 userid |                             pwdhash
                  |        email
--------
+-----------------------------------------------
-----------+-----------------------
 mha    |
$2a$06$JuAuqsbSvocROU49v4uEkOMVOCtc57gT6fHCAB.L7GDbC
uSHz7.gS | magnus@hagander.net
…
…
…
(11242 rows)
```

Prevent direct access!

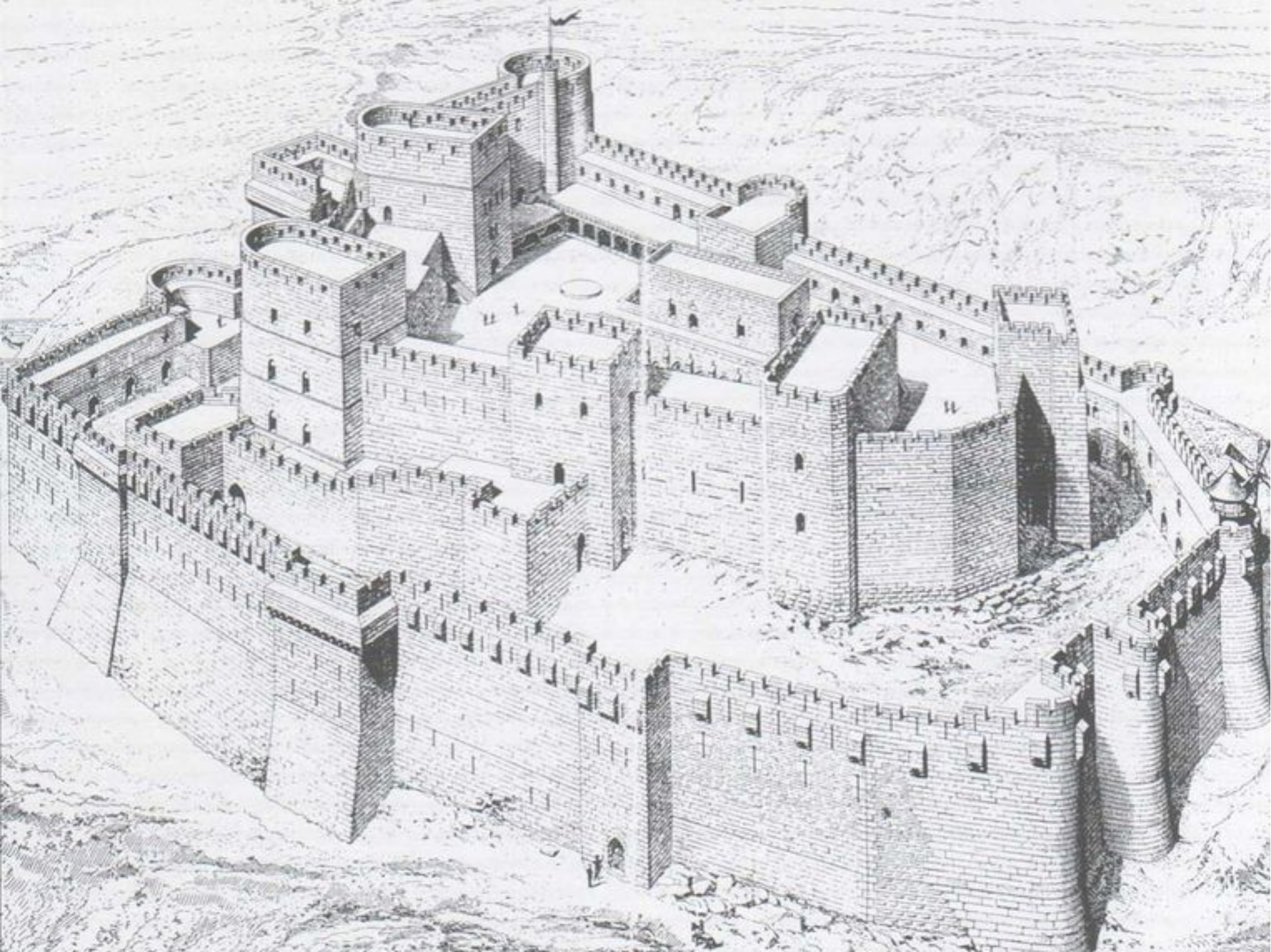
```
CREATE OR REPLACE FUNCTION login(_userid text,
        _pwd text, OUT _email text)
 RETURNS text
 LANGUAGE plpgsql
 SECURITY DEFINER
AS $$
BEGIN
  SELECT email INTO _email FROM users
    WHERE users.userid=lower(_userid)
    AND pwdhash = crypt(_pwd, users.pwdhash);
END;
$$

REVOKE ALL ON users FROM public;
```

Prevent direct access!

```
postgres=> select * from users;
ERROR:  permission denied for relation users


postgres=> select login('mha', 'topsecret');
        login
---------------------
 magnus@hagander.net
(1 row)
```



Thank you!

Twitter: @magnushagander
http://blog.hagander.net/
magnus@hagander.net

http://www.flickr.com/photos/osi/122937793/
http://www.flickr.com/photos/litlnemo/5304381201/in/photostream/
http://www.flickr.com/photos/86608983@N00/375048613/in/photostream/