Passwörter sicher speichern

oder die Geschichte von den drei kleinen Schweinchen

Inhaltsverzeichnis

- Wer bin ich? - Der Erzähler
  - Warum der Vortrag? eHarmony, LinkedIn, last.fm, Sony, ...
- Geschichte vom Speichern der Passwörter
  - vom Strohaus: Klartext-Passwörter
  - über das Holzhaus (Hash, ungesalzen, eine Runde)
  - und das Ziegelhaus: KDF (Key derivation functions)

Der Erzähler

- Fabian Blechschmidt
- PHP seit 2004
- Freelancer seit 2008
- Magento seit 2011
- Certified Magento Developer
- spielt gerne, aktuell mit
  - Magento und Symfony2
  - Passwörter, Hashing, etc.

Warum der Vortrag?

eHarmony, LinkedIn, last.fm, Sony, ...

- LinkedIn, eHarmony (Dating-Portal) und last.fm (Streaming-Seite) gehackt
  - Beute: 8 Millionen Accounts
- „*I left a bunch of stuff running over night, and have about 50% of all the passwords cracked.*“ (LinkedIn: 2,9 Mio Acc.)
- http://erratasec.blogspot.de/2012/06/linkedin-vs-password-cracking.html

Ausgangspunkt:
Du wirst gehackt - früher oder später

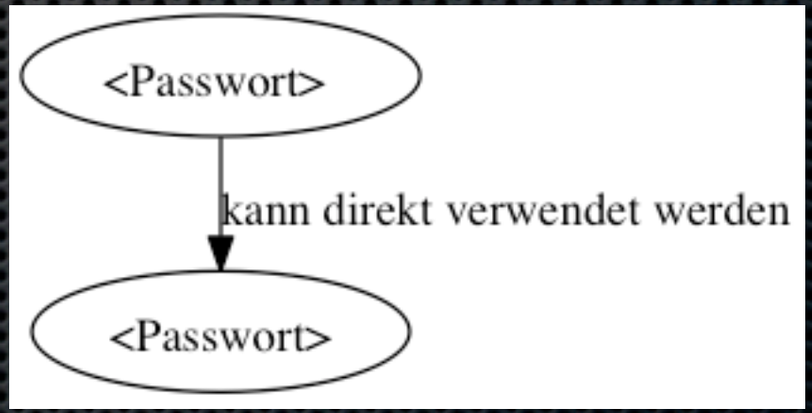
- Frage ist NICHT: Hat deine Anwendung Sicherheitslücken?
- SONDERN: Wann werden sie gefunden?
- Und durch wen?

Strohhaus aka **Klartextpasswörter**

- Wie? Passwort direkt in die Datenbank
- Vorteil:
  - Benutzer kriegt SEIN Passwort wieder
- Nachteil:
  - Datenbank weg, ALLE Passwörter weg.

"Ich werde strampeln und trampeln,
ich werde husten und prusten
und dir dein Haus zusammenpusten."

- Problem(e):
  - Zeit zum Cracken (Passwörter berechnen):
    - nicht nötig ⇒ so schnell wie die Platte lesen kann.

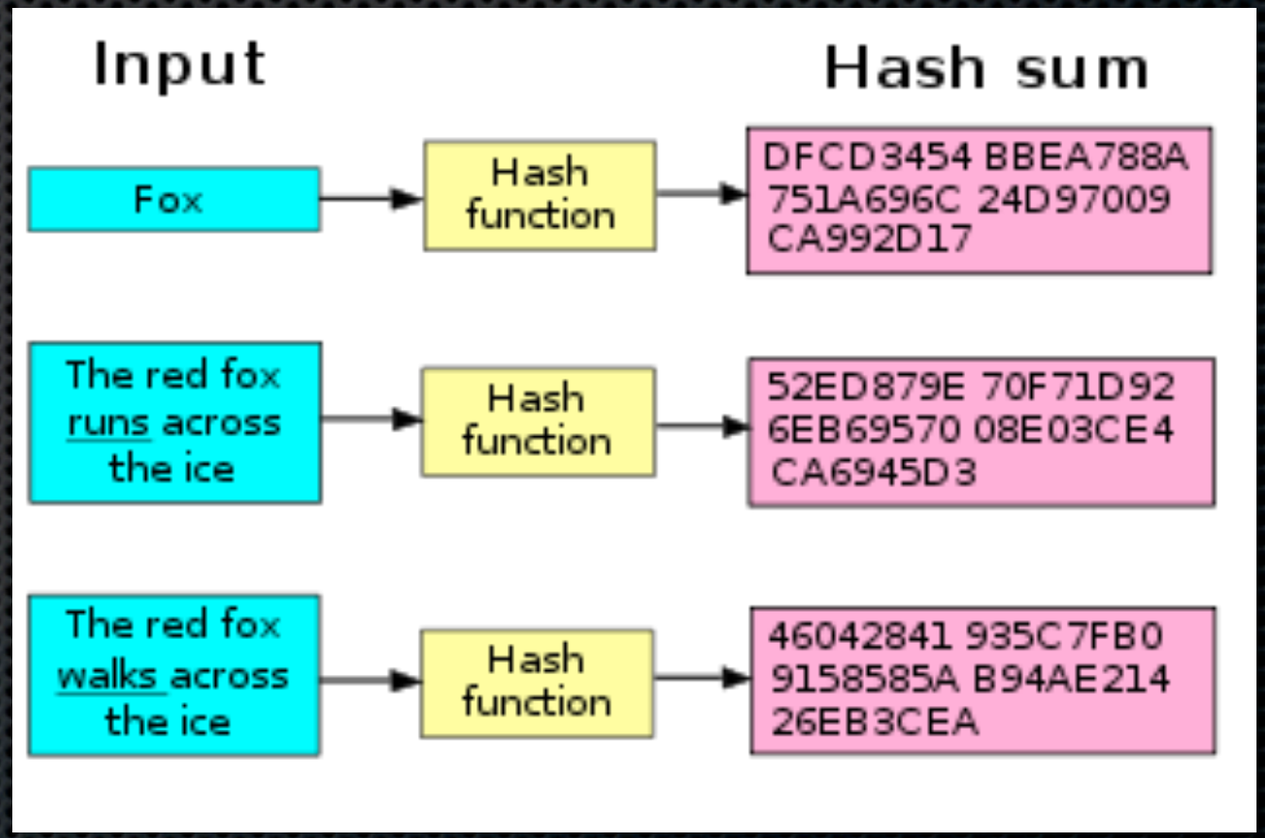


Holzhaus
aka **Passwort (gehasht)**

- Passwörter gehasht speichern
- Vorteil:
  - Passwort nicht im Klartext
- Nachteil:
  - heute leicht zu knacken

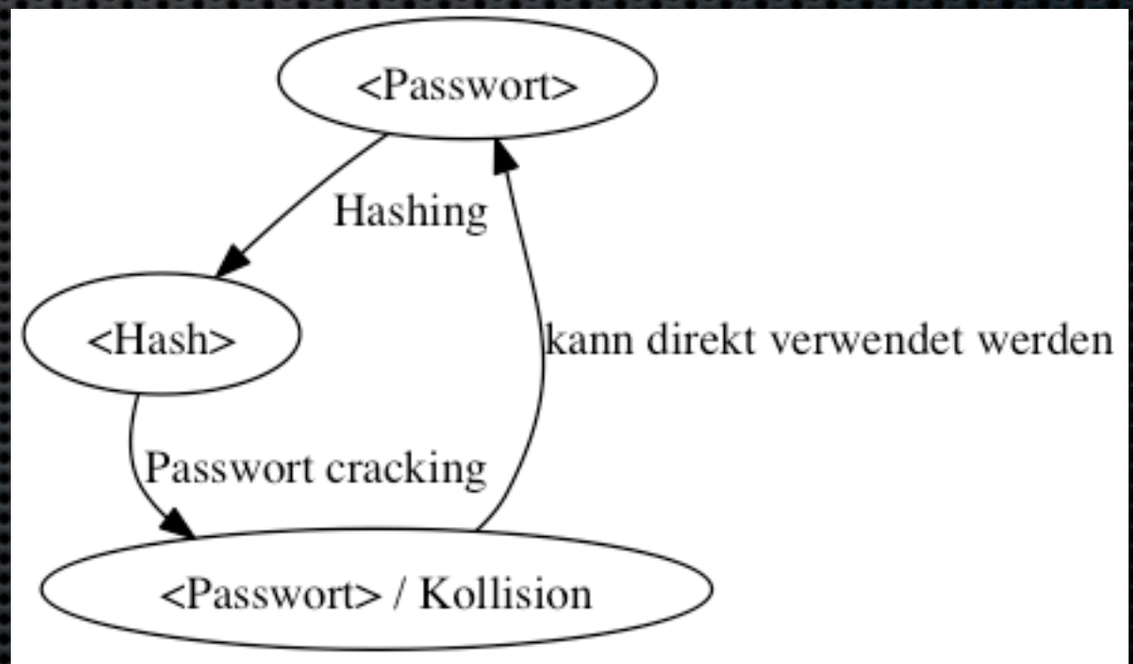
Hashing

- Einweg-Funktion
- leicht in eine Richung, schwer in die andere
- z.B. Primfaktorzerlegung vs. Multiplikation oder Modulo-Berechnungen
- z.B. MD5, SHA2, SHA512



"Ich werde strampeln und trampeln,
ich werde husten und prusten
und dir dein Haus zusammenpusten."

- Klartext zum Hash finden ist schwer, ABER: „Problem“ ist vorhersagbar
  - d.h. man kann Passwörter/Kollisionen im Voraus berechnen
- Kollision:
  - H(abcde) == H(12345)



Problem 1: Vorhersagbar/Kollisionen
Lösung: Salting

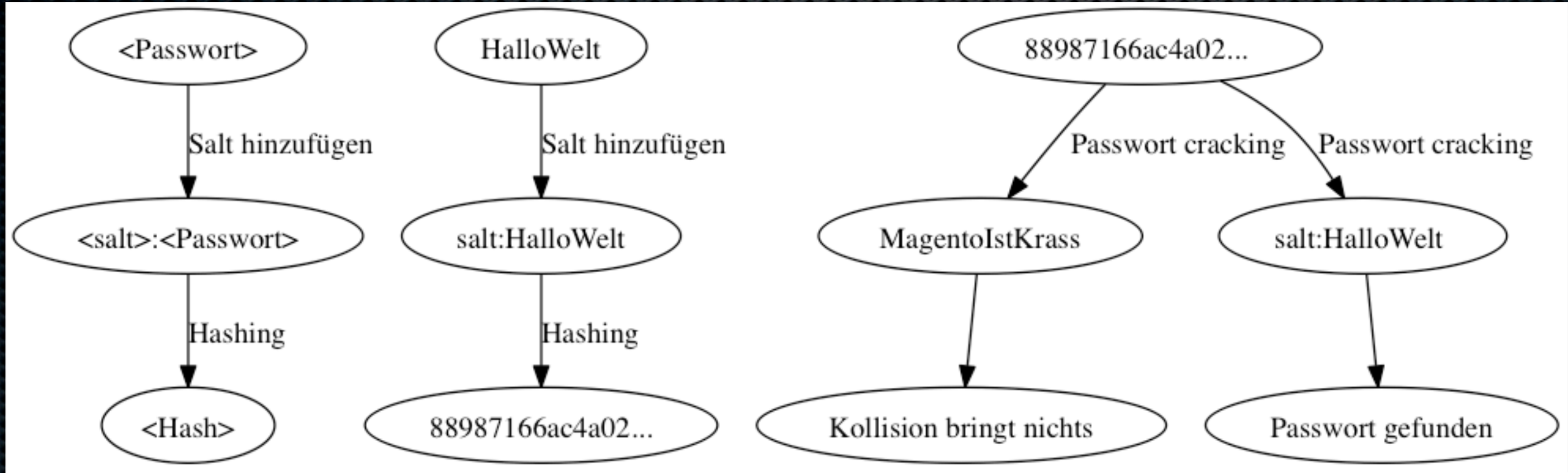
- Benutzer sucht Passwort aus: sexandgod
- Programm generiert ZUFÄLLIGEN Salt: 4R6/4§
- Beides verbinden: sexandgod:4R6/4§
- und hashen: MD5 ("sexandgod:4R6/4§") = c1789276afc4651ce074864eb1115b8a
- Salt und Hash in die Datenbank schreiben: c1789276afc4651ce074864eb1115b8a:4R6/4§

Lösung: Salting Part 2

- Cracker erzeugt Kollision für Hash
- MD5(„SpielplatzFürKinder“) = c1789276afc4651ce074864eb1115b8a
- Passwort wird eingegeben und mit Salt gehasht:

  SpielPlatzFürKinder:4R6/4§
- MD5(SpielPlatzFürKinder:4R6/4§) = 3ff5c494f24fa3660b11b03611adb1ad **!=** c1789276afc4651ce074864eb1115b8a

Salting: Überblick

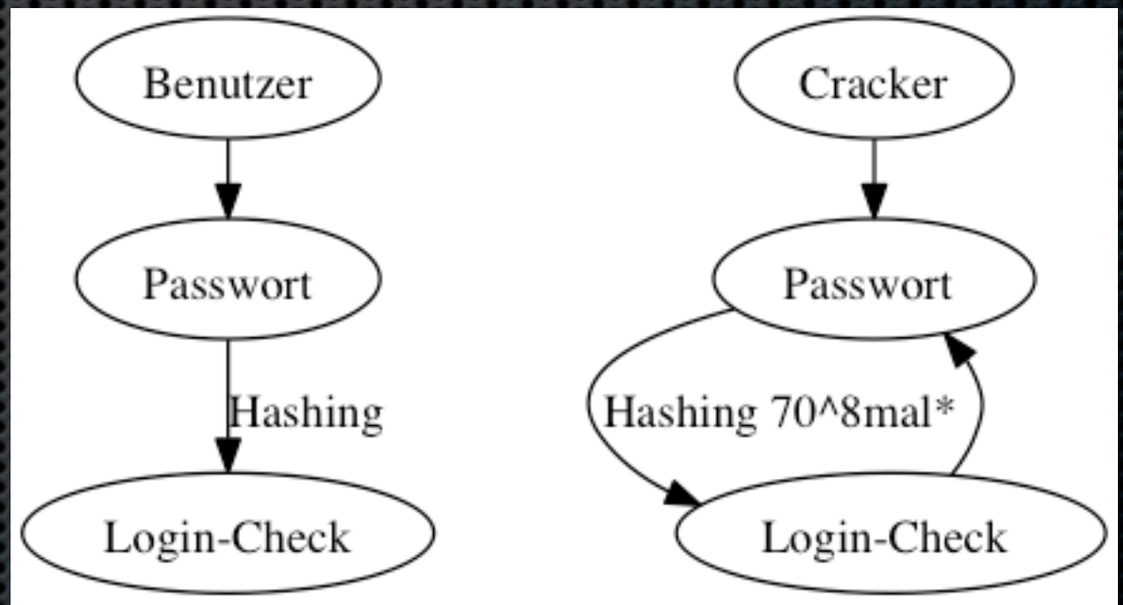


- Hash mit Salt braucht **bestimmte** Kollision

Problem: Hashes lassen sich „leicht“ berechnen
Lösung: KDF: **k**ey **d**erivation **f**unction

- pro Login einmal Hashen
- pro Passwort cracken:

  576.480.100.000.000
  ≈5,8*10^13 mal hashen



*70^8 [A-Za-z0-9#+-_.,;:]{8}

KDF - mehr Aufwand für alle

- SHA2(„Beliebige Zeichenkette“) ist unbekannt, bis berechnet.
- SHA2(SHA2(„Beliebige Zeichenkette“)) mind. doppelt so aufwendig wie SHA2(„Beliebige Zeichenkette“)

```
$n = 10^7; $res = „Beliebige Zeichenkette“;
for($i = 0;$i<=$n;$i++){
    $res = sha2($res);
}
```

Ziegelhaus aka KDF (abstrakt)

- **Hash**funktion

sehr oft auf ein

Eingabestring und ein

Salt angewendet.

Quellen

- http://www.maerchenstern.de/maerchen/die-drei-kleinen-schweinchen.php5
- http://mashable.com/2012/06/15/hard-to-hack-password/
- http://erratasec.blogspot.de/2012/06/linkedin-vs-password-cracking.html
- http://blog.zoller.lu/2012/06/storing-password-securely-hashses-salts.html
- http://de.wikipedia.org/wiki/Rainbow_Table
- http://en.wikipedia.org/wiki/PBKDF2
- http://www.openwall.com/presentations/PHDays2012-Password-Security/

Bilder

- Strohhaus:
- http://www.flickr.com/photos/kahtava/107922486/sizes/l/in/photostream/
- http://www.flickr.com/photos/kahtava/
- Holzhaus:
- http://www.flickr.com/photos/29214188@N05/7235311244/sizes/l/in/photostream/
- http://www.flickr.com/photos/29214188@N05/
- Ziegelhaus:
- http://www.flickr.com/photos/54359823@N03/6798308864/sizes/l/in/photostream/
- http://www.flickr.com/photos/54359823@N03/