

# WORDPRESS SICHERHEIT

## Wie sicher ist mein Passwort?

*Marc Nilius - @marcnilius - @WPSicherheit  
Barcamp Bonn 2016*

**Wie sicher ist dein Passwort?**

**Wieviele Zeichen?**

**Welche Zeichen?**

**Kleinbuchstaben? Großbuchstaben?**

**Sonderzeichen?**

# Was ist ein Brute-Force-Angriff?

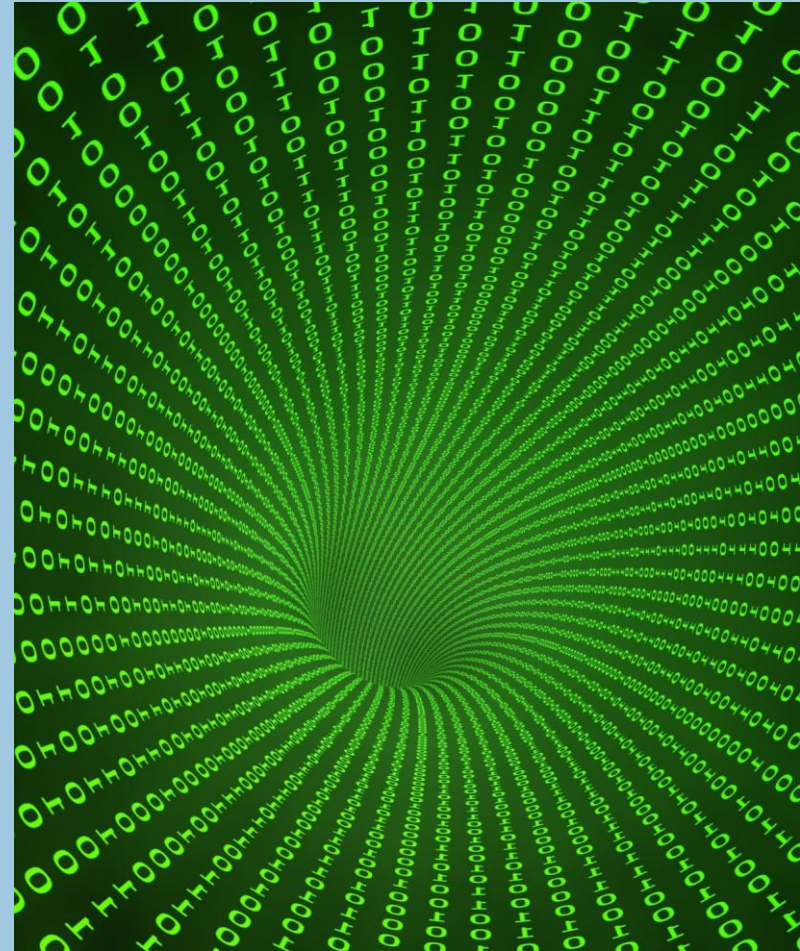
**Brute-Force-Angriff:**  
Zugriff durch Ausprobieren aller  
Möglichkeiten mit „roher Gewalt“

**Online:**

z.B. WordPress-Login, Zugriff über das  
Internet (langsam)

**Offline:**

Durch vorangegangenen Hack/Diebstahl  
Zugriff auf die Datenbank.  
Dann Durchprobieren der Passwörter auf  
lokalem Computer (schnell)



# Wie lange dauert es, bis ein Passwort geknackt ist?

Passwort, 8 Zeichen lang, bestehend aus:

Großbuchstaben A-Z, Kleinbuchstaben a-z, Zahlen 0-9

HDMuMp9Y

Online (1000 Versuche/Sekunde): 7000 Jahre

Offline (großes Array): 2,22 Sekunden

Mit Sonderzeichen:

rJl=32aY

Online (1000 Versuche/Sekunde): 213.000 Jahre

Offline (großes Array): 1,12 Minuten

# Wie lange dauert es, bis ein Passwort geknackt ist?

Demo: <https://www.grc.com/haystack.htm>

Wie lange dauert es, bis ein Passwort geknackt ist?



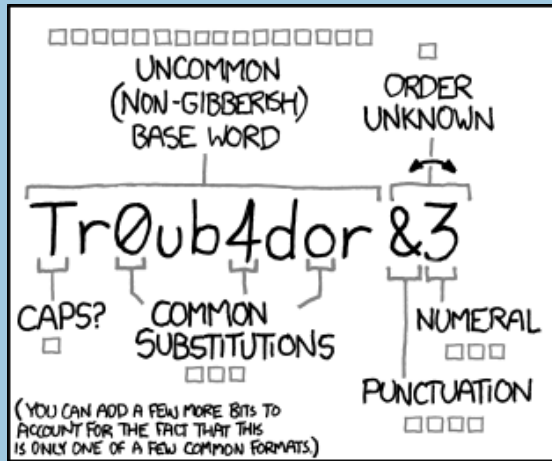
# Wie sieht ein sicheres Passwort aus?

RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘
11	welcome	NEW

12	1234567890	NEW
13	abc123	1 ↗
14	111111	1 ↗
15	1qaz2wsx	NEW
16	dragon	7 ↘
17	master	2 ↗
18	monkey	6 ↘
19	letmein	6 ↘
20	login	NEW
21	princess	NEW
22	qwertyuiop	NEW
23	solo	NEW
24	password	NEW
25	starwars	NEW



# Wie sieht ein sicheres Passwort aus?



~28 BITS OF ENTROPY

□□□□□□□□      □  
□□□□□□□□      □□□  
□□□      □□□  
□□□□      □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

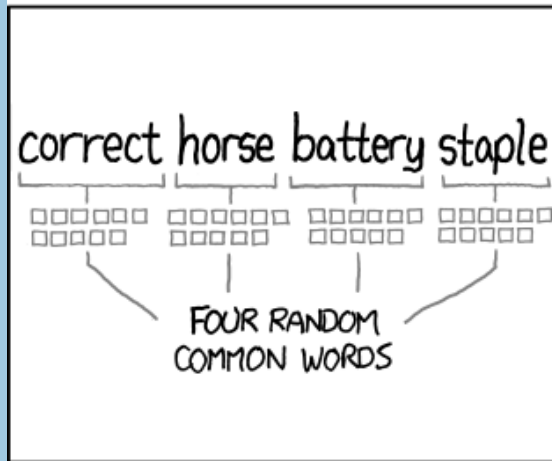
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

□□□□□□□□□□□□  
□□□□□□□□□□□□  
□□□□□□□□□□□□  
□□□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



# Wie sieht ein sicheres Passwort aus?

- mindestens 12 Zeichen lang
- je länger, desto besser
- keine Einzelwörter (wegen Wörterbuchattacken)
- aber Passphrasen / ganze Sätze
  - keine Zitate
  - keine anderen Sätze, die sich in Büchern finden
- Am besten mehrere Wörter ohne direkten Zusammenhang
- wer ein klassisches Passwort verwenden möchte:
  - Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen

# Wie bleibt mein Passwort sicher?

- Passwort nicht wiederverwenden
- Passwort alle 6 – 12 Monate bei allen Services ändern

Beispiel:

Basis-Passwort: 5aXGdeJYZwrG

Für Ebay: ebay\_5aXGdeJYZwrG

nächstes PW: ebay\_5aXGdeJYZwrG-02

Für Facebook: fb\_5aXGdeJYZwrG

nächstes PW: fb\_5aXGdeJYZwrG-02

Für Google: goo\_5aXGdeJYZwrG

nächstes PW\_goo\_5aXGdeJYZwrG-02

Usw.

Weitere Möglichkeit: Single-Sign-On mit Facebook, Google, Twitter o.ä.

Nachteile: evil ;-)

# Passwort-Manager - wie verwalte ich Passwörter?

Mit Passwort-Managern kann man komfortabel alle notwendigen Passwörter verwalten und auch sichern

Besser als das „Blatt Papier“ neben dem Rechner

Nachteil: Wird der Rechner kompromittiert, sind alle Passwörter auf einmal unsicher

Deswegen: Der Passwort-Manager muss besonders gut gesichert werden (sehr langes Passwort, 2-Faktor-Authentifizierung mit Smartphone, Key-Datei auf USB-Stick)

# Passwort-Manager - wie verwalte ich Passwörter?



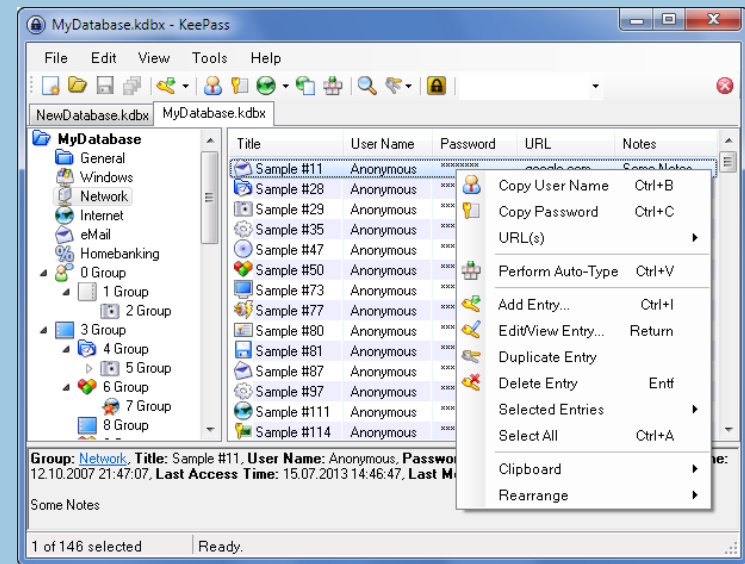
# Passwort-Manager - wie verwalte ich Passwörter?

Darauf sollte man bei der Auswahl achten:

- keine Cloud-Lösung (auch wenn es praktisch erscheint)
- Gute Verschlüsselung (AES256 oder besser)
- Verschlüsselung nicht nur der Passwörter, sondern auch der Metadaten!
- Zugriff auf mit Passwort, besser aber 2-Faktor-Authentifizierung
- Open-Source bietet die Sicherheit, dass der Code intensiv geprüft wurde

Ich nutze: KeePass

(<http://www.keepass.info>)



# WordPress: Wie stehts um die Passwörter?

- WordPress generiert selbst starke Passwörter beim Anlegen eines Benutzers
- Unsichere Passwörter sind durch den Benutzer möglich (aber nicht sinnvoll!)

Benutzerkonten-Verwaltung

Neues Passwort

Stark

Benutzerkonten-Verwaltung

Neues Passwort

Ganz schwach

Passwort bestätigen  Bestätige die Verwendung eines schwachen Passworts

# WordPress: Wie stehts um die Passwörter?

Sicherheits-Suiten (Wordfence, iThemes Securit, ...) haben eine Einstellung, um starke Passwörter zu erzwingen

Meine Empfehlung: Das Plugin WP Password Policy Manager  
(<https://de.wordpress.org/plugins/wp-password-policy-manager/>)

Diverse Möglichkeiten für starke Passwörter:

- Mindestlänge, bestimmte Zeichentypen müssen enthalten sein
- regelmäßig neue Passwörter (werden beim Login eingegeben)
- neues Passwort muss anders sein, als die letzten X Passwörter



# WordPress: Wie stehts um die Passwörter?

## WP Password Policy

ERROR: The password you entered expired 10 mins ago.

Username

Old Password

New Password

Verify Password

Remember Me

New password must...

- not be the same as your username
- not be the same as the previous one
- be at least 7 characters long
- contain mixed case characters
- contain numeric digits
- contain special characters

WordPress Password Policies by [WP Password Policy Manager](#)

Lost your password?  
← Back to LocalDotCom

Dashboard  
Audit Log  
Posts  
Media  
Pages  
Comments  
Appearance  
Plugins  
Users  
Tools  
**Settings**  
General  
Writing  
Reading  
Discussion  
Media  
Permalinks  
Password Policies  
Collapse menu

### WordPress Password Policy Manager Settings

Password Expiration Policy   
*Examples: 5 days 20 days 6 hours 3 weeks*  
Leave blank to disable Password Expiry policy.

Password Length Policy  characters  
Leave blank to disable Password Length policy.

Mixed Case Policy  Password must contain a mix of uppercase and lowercase characters.

Numeric Digits Policy  Password must contain numeric digits ( 0-9 ).

Special Characters Policy  Password must contain special characters ( eg: ., !#\$\_+ ).

Password History Policy Remember  old passwords  
Leave blank to disable password history policy.

Users and Roles Exempt From Policies   
*Users and Roles in this list are free of all Password Policies.*

Reset All Users' Passwords

# Mehr zum Thema WordPress-Sicherheit

Kostenloser Newsletter rund um WordPress-Sicherheit alle zwei Wochen:

<https://www.wp-sicherheit.info>

Twitter: @WPSicherheit und @marcnilius

Facebook-Gruppe: "WordPress Sicherheit"



**WORDPRESS  
SICHERHEIT**