Passwortschutz: Sicherheitsaspekte

Ihr Feind: Der "Hacker"

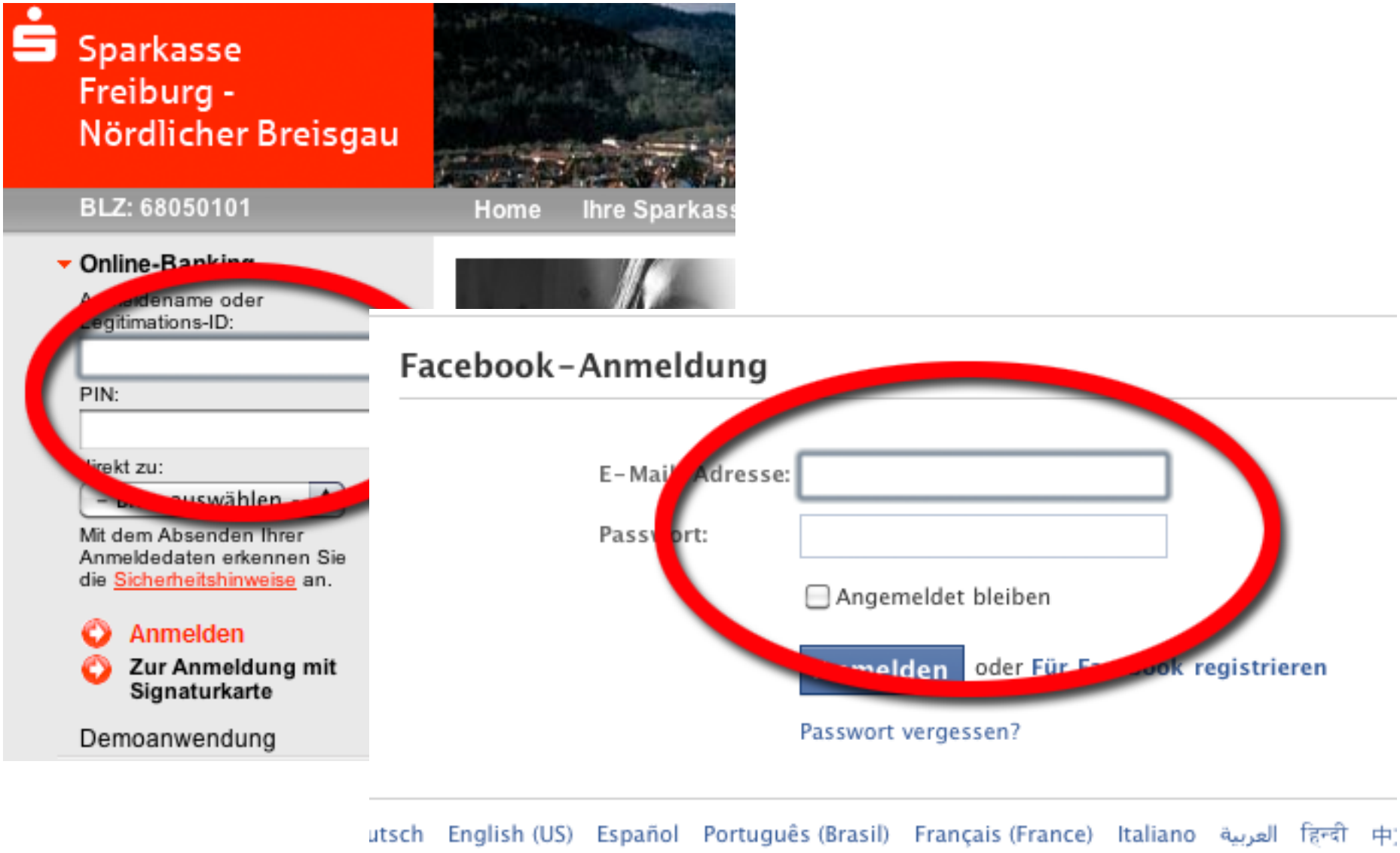
Hacker hat im technischen Bereich mehrere Bedeutungen. Das Wort wird alltagssprachlich gebraucht, um jemand zu bezeichnen, der über ein Netzwerk in Computersysteme eindringt und zugleich Teil einer entsprechenden Subkultur ist.

(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



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

1. Haustier
2. Hobby
3. Geburtsname der Mutter
4. Geburtsdatum aus Familie
5. eigenes Geburtsdatum
6. Name aus der Familie
7. eigener Name
8. Lieblingsfußballmannschaft
9. Lieblingsfarbe
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/

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 unbekannten 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 $^{\text{Passwortlänge}}$

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)

Quelle: http://www.1pw.de/brute-force.html

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

Quelle: http://www.1pw.de/brute-force.html

Tipp 2

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

schlecht: hansi

besser: me1N_hansi

Analysemethode: Verwendung eines "Dictionaries" (Wörterbuchangriff)

= Verwendung eines Wörterbuchs (sog. "Passwortlisten")

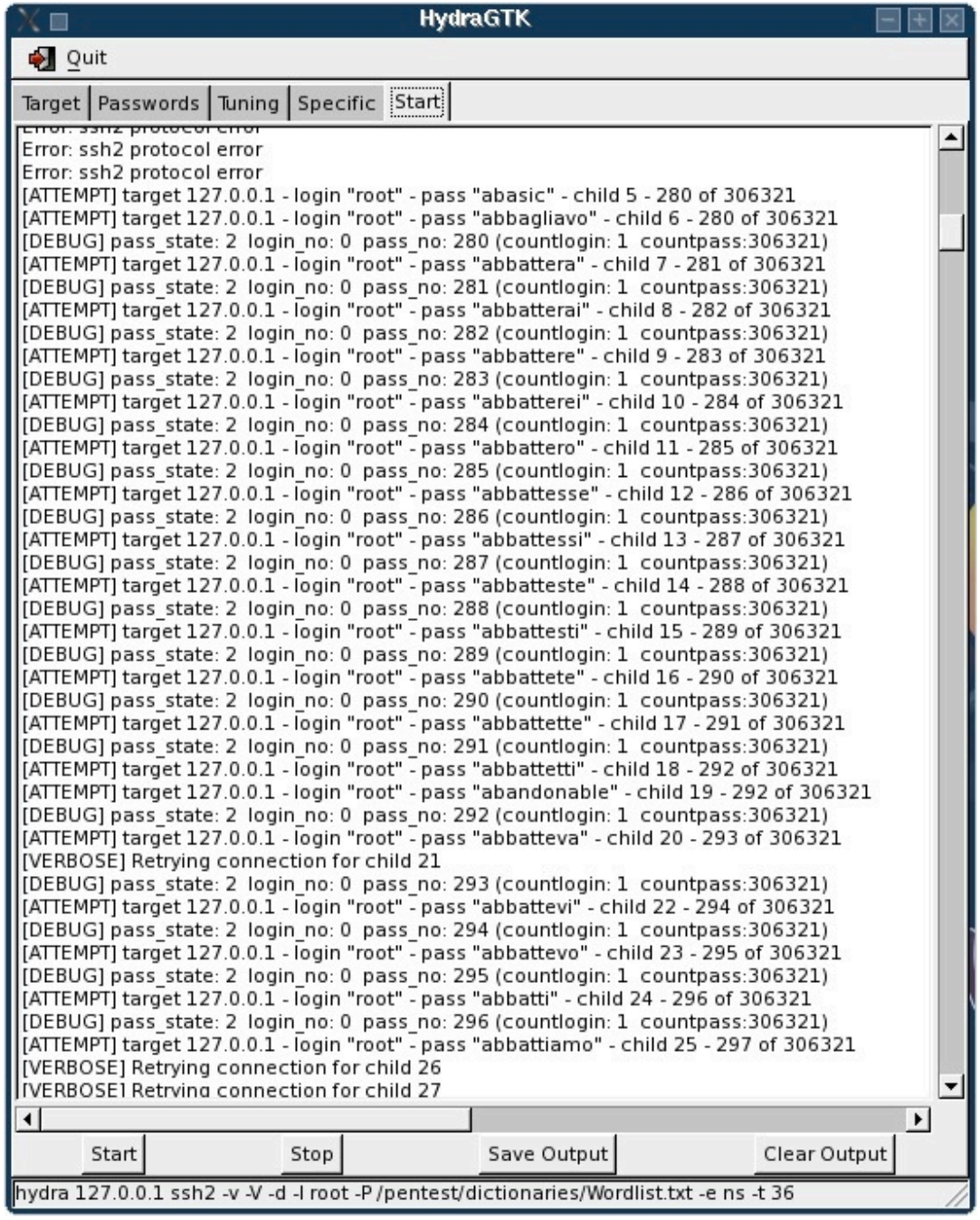
Vorgehen der Hacker

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



Tipp 3

- Passwort sollte nicht in einem Wörterbuch zu finden sein

schlecht: raumschiff ; apfelsine

besser: raumschiff77; apfelsineR

SQL-Injection

Passworteingabe

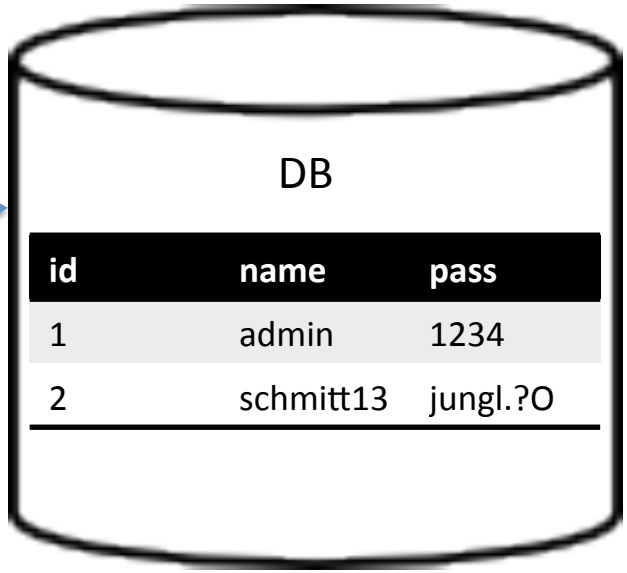
Username: admin

Passwort: 123456

abschicken

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

Login



SQL-Injection

Passworteingabe

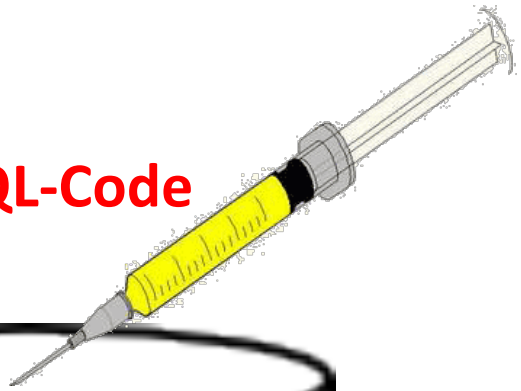
Username: admin

Passwort: 123456

abschicken

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

Login



SQL-Code

DB

id	name	pass
1	admin	1234
2	schmitt13	jungl.?O

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[1] an ergebnis.php übergeben. Überprüfen Sie die Lauffähigkeit: Rufen Sie index.php über den Localhost auf und schicken Sie das Formular ab.

[1]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!