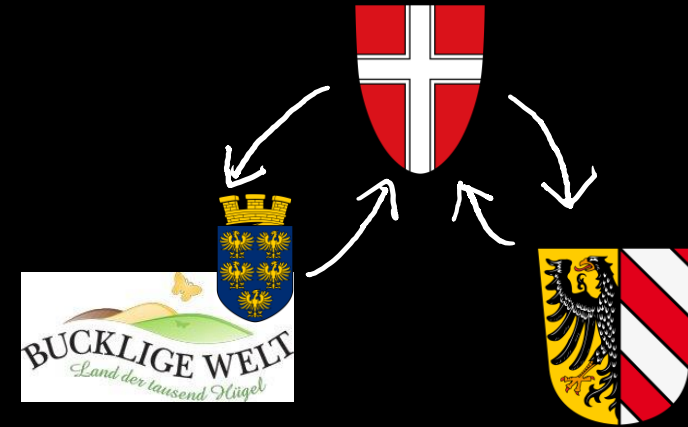# Web (and) Application Security

WUAPS

# whoami

Daniel Schwarz

lbschwarzd@fhstp.ac.at

Education:

Prof. Exp.:

# Who are you?

# Hacking webapplications is illegal

(https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/Seite.1720213.html)

But it`s also fun!

just become a whitehat and get
legally paid for it

and help making the internet a safer place

# Why is web (application) security important?

# World's Biggest Data Breaches & Hacks

*Select losses greater than 30,000 records*
Last updated: 11th June 2020

interesting story
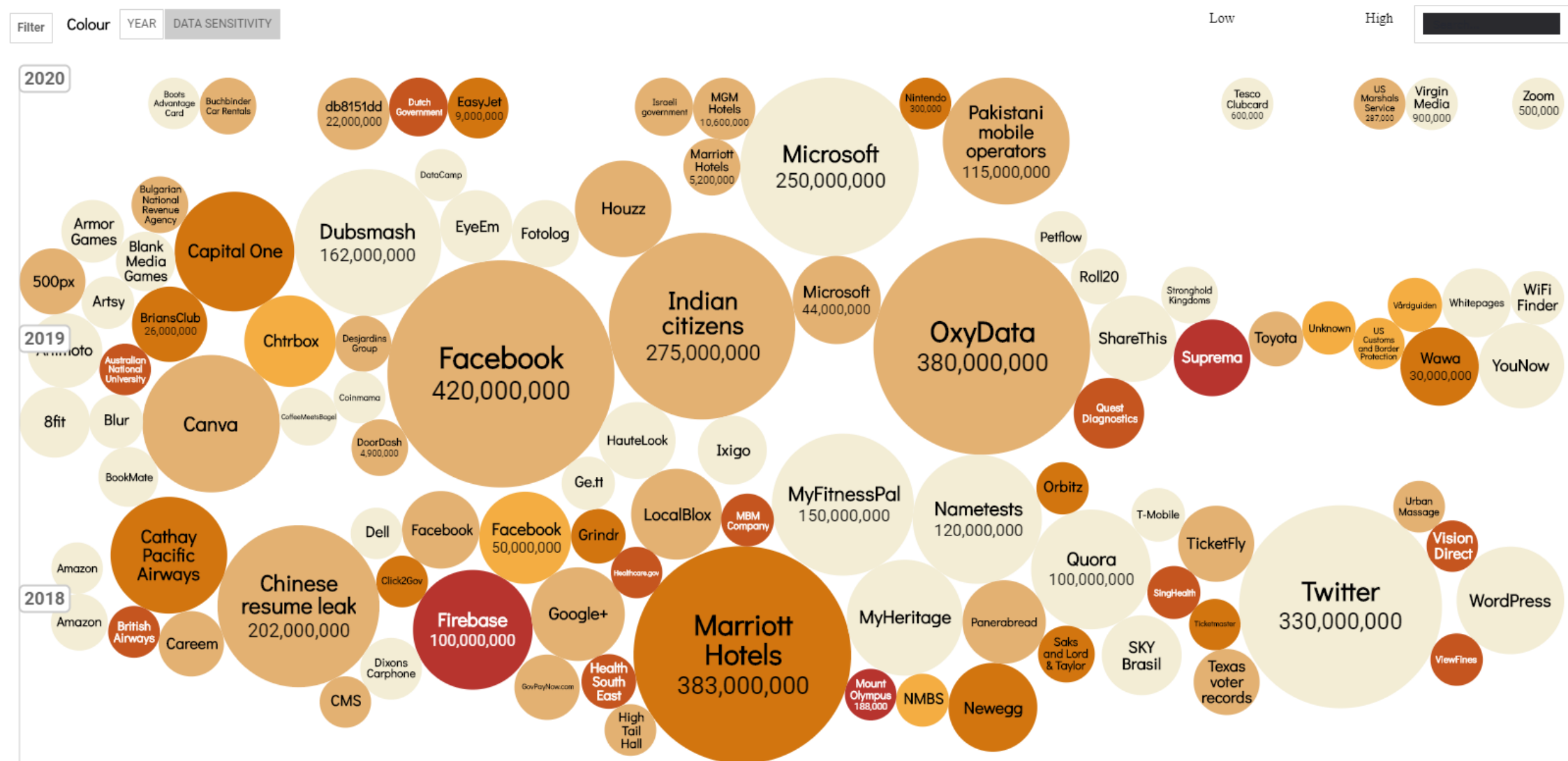
Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

**Figure 2.** What tactics are utilized? (Actions)

45% of breaches featured Hacking

Errors were causal events in 22% of breaches

22% included Social attacks

17% involved Malware

8% of breaches were Misuse by authorized users

Physical actions were present in 4% of breaches

Web application

Backdoor or C2

Desktop sharing software

Command shell

Other

Physical access
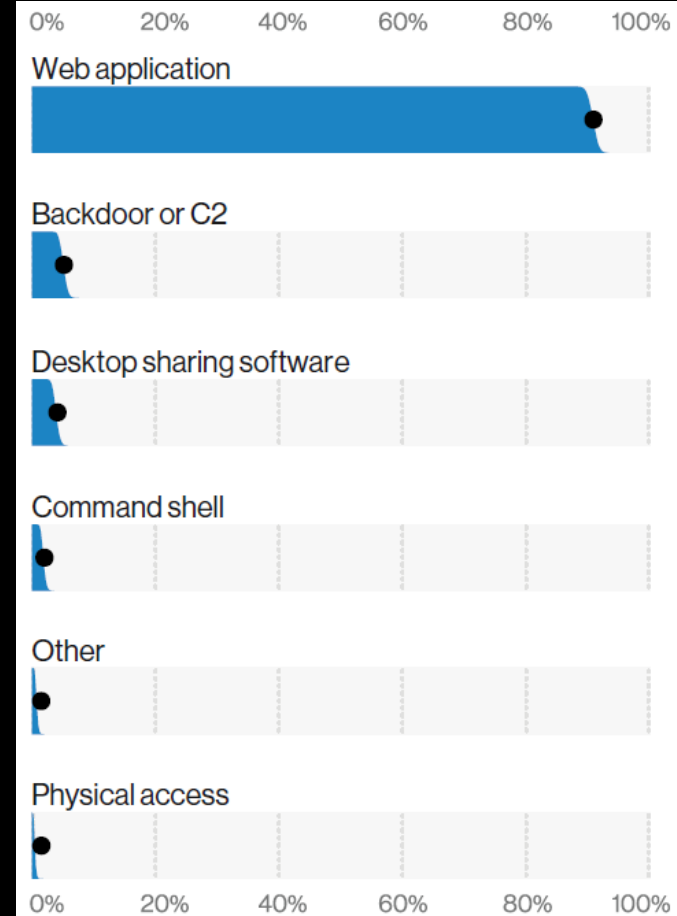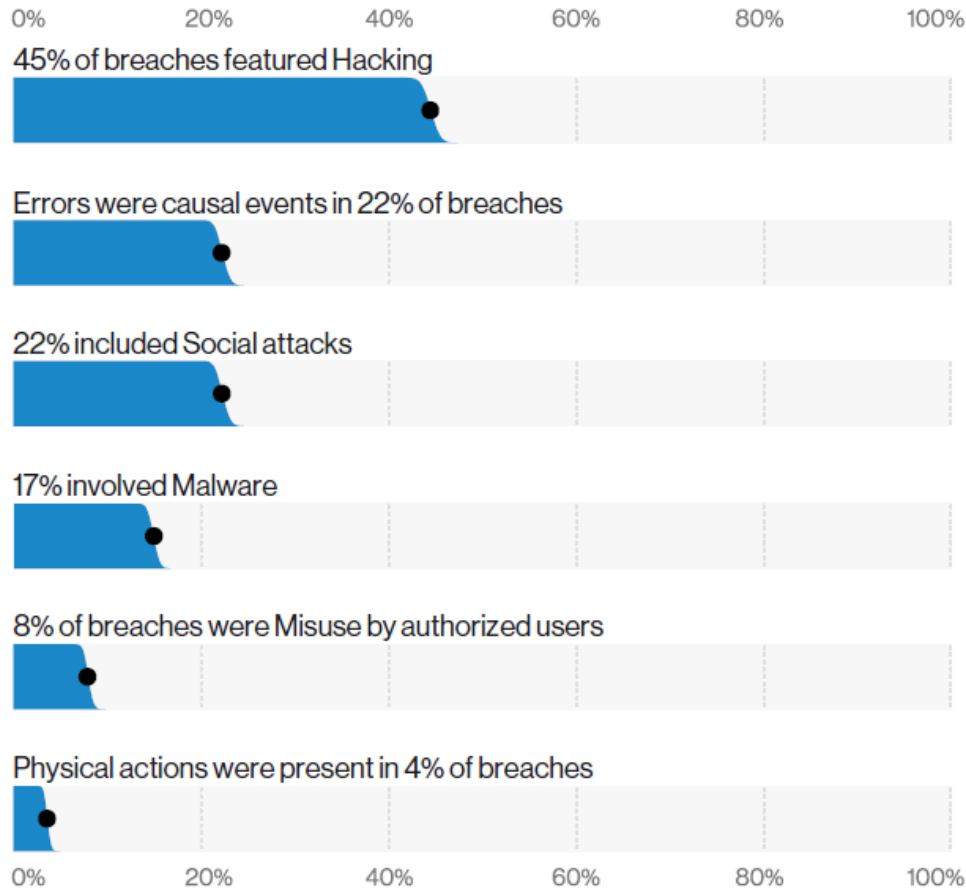
**Figure 21.** Top Hacking vectors in breaches (n = 1,361)

Source: Verizon 2020 Data Breach Investigation Report

# Why is it so hard to do it right?
## = secure

The web is a complex combination of different technologies which evolved over time

# You have to care about:

## server-side code
gets untrusted input

## browser
runs different applications at the same time

## client-side code
runs in an untrusted environment

## the user
well… we all know them…

# Rough Overview

1. >> Introduction <<
2. Basic Principles and Resources
3. Architecture & Basic Web Procedure
4. Authentication and Session Management
5. Authorization
6. Server and Backend Attacks
7. Remaining Client Attacks
8. General Topics
9. Conclusions

# Overall Conditions

- Grading
  - 50% Lab
    - more about that in the first lab session
  - 50% Theory
    - eCampus exam at the end of this course
    - You need to collect more than 25 of 50 points for a positive grade

- Attendance
  - Needs to be recorded on eCampus

- Breaks

- Camera

- Recording

- Material
  - Released under CC Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)
  - https://creativecommons.org/licenses/by-sa/4.0/
  - https://github.com/dschwarz91/websec-lecture

# After this course, you will be able to...

… explain the most common vulnerabilities in today's web applications

… identify vulnerabilities in web applications and give recommendations how to fix them

… use some of the most important tools to efficiently examine web applications

Any questions before we start?