Hacking and hacking Mitigation

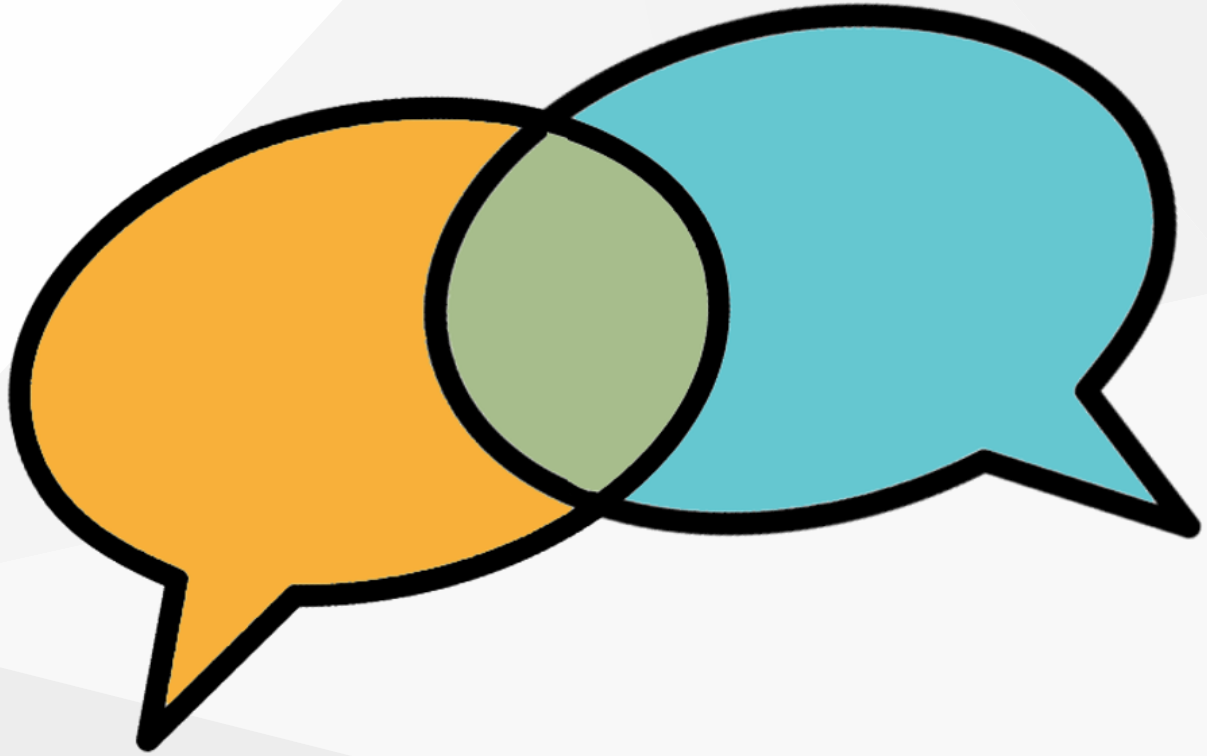
For SQL Server

… the next 60 minutes

- 🔓 Why is this important?
- 🔓 How hackers gain access?
- 🔓 How do hackers think?
- 🔓 Demos
- 🔓 Q&A

Presentation Rules

- Always ask questions
- Please interrupt me if you have a question
- This is a two-way conversation, let’s learn from each other’s experiences



Disclaimer

Any actions and or activities related to the material contained within this session are solely your responsibility.

The misuse of the information from this session can result in criminal charges brought against the persons in question. The presenters will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this session to break the law.

This session and it's demos contain materials that can be potentially damaging or dangerous. These materials are intended for educational and informational purposes only. Do not attempt to violate the law with anything contained here. If this is your intention, then LEAVE NOW!

Do not abuse this material. Be responsible.

Sander Stad

(he/him)

DATAmasterminds

Microsoft® MVP Most Valuable Professional

sqlstad.nl

sander@sqlstad.nl

sanderstad

@sqlstad

Why is this so important?

How does a hacker gain access?

- Phishing
- USB Key Malware
- Scanning Networks for Vulnerabilities
- Guessing or Social Engineering Passwords
- Wifi Compromises
- Credentials From Third-Party Sites
- Compromising Web-Based Databases
- Insiders

How do hackers think?

Motivation

According to a recent study by Thycotic, the main motivation for hackers is:

- 🔓 51% thrill
- 🔓 29% moral compass
- 🔓 19% money
- 🔓 1% notoriety

What does it mean to be a hacker?

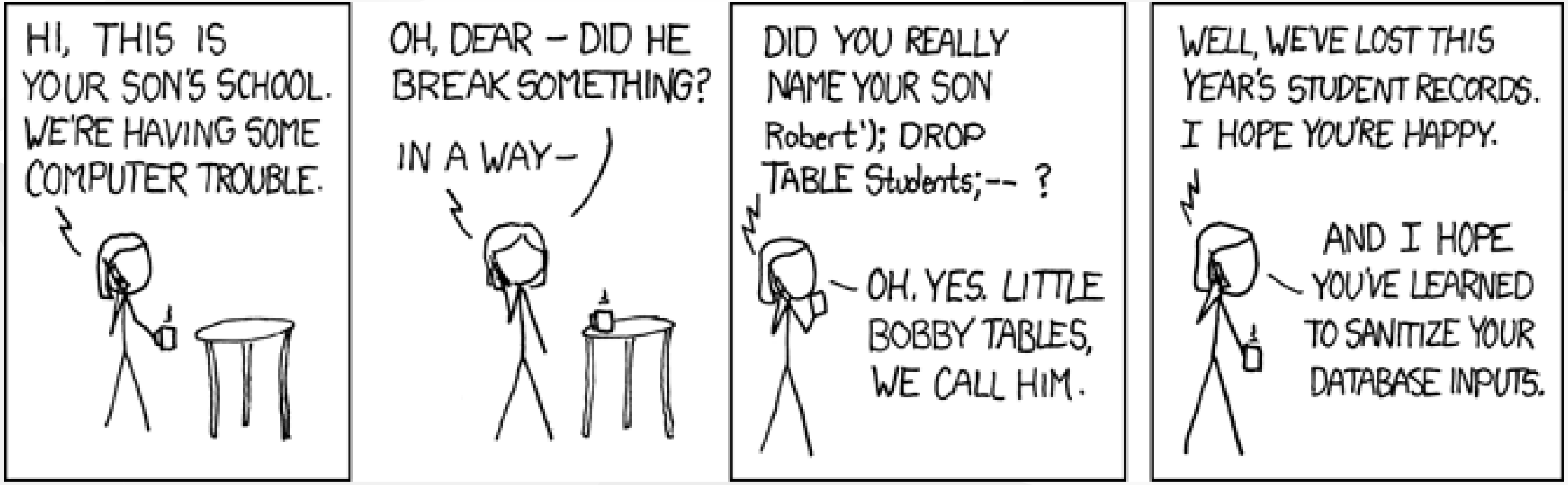
- 🔓 You either choose to be a hacker or you are a hacker
- 🔓 It's someone who experiments with the limitations of a system
- 🔓 Compulsion to experiment with the limits of a system

The way they think

- They understand a fundamental part of technology; Code
- Compulsive desire to command and control systems
- Learn very fast and adapt to systems to their advantage

Demos

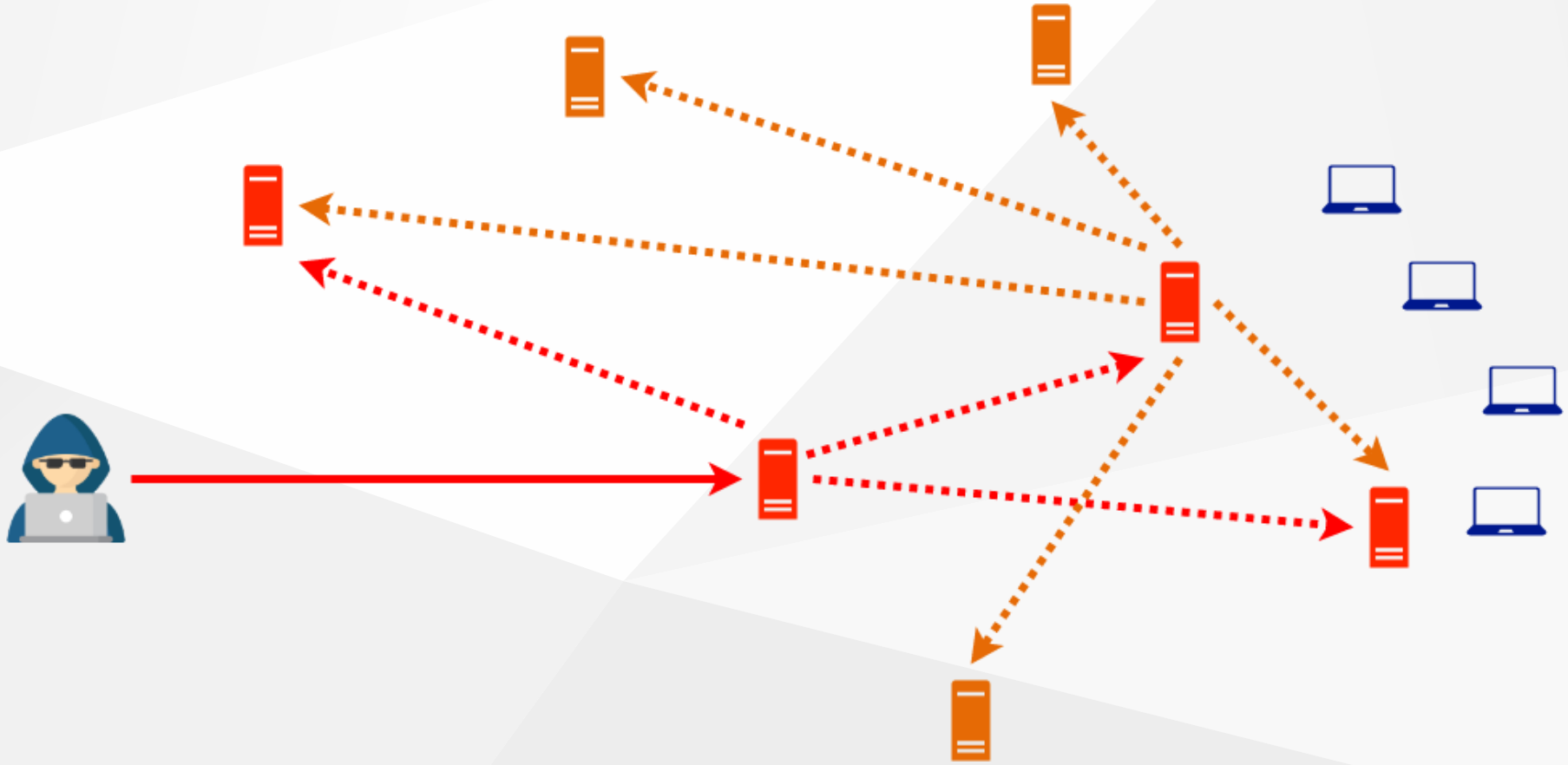
Demo 1: SQL Injection



How to prevent SQL Injection

- 🔒 Parametrized queries
- 🔒 Input validation
- 🔒 Supply the parameters for the SQL statement
- 🔒 Use stored procedures
- 🔒 Use character-escaping functions
- 🔒 Set the correct privileges
- 🔒 Implement a Web application firewall (WAF)

Lateral movement



Metasploit

Golden Ticket

How to prevent against Golden Ticket attack

- Change the KRBTGT password regularly
- Minimize the number of accounts that can access the KRBTGT password hash
- Minimize opportunities for hackers to steal privileged credentials
- Monitor your IT environment for suspicious activity

Pointers to remember

- Security is a mindset
- Hackers think differently
- People are the weakest link
- Think about your choices with security in mind

Resources

- Try Hack Me: https://tryhackme.com/
- Center for Internet Security: https://www.cisecurity.org/
- STIG: https://public.cyber.mil/stigs/
- OWASP: https://owasp.org/www-project-top-ten/