Think Like a Hacker

Please

Ask questions through the app

Rate Session

Thank you!

@Brunty

Developer

Mentor & mentee

Tinkerer

Who are hackers?

“

Black hat: hacker doing evil

White hat: hacker doing good

Grey hat: hacker hacking

Top hat: hacker doing fancy stuff

@beerbikesbacon

https://twitter.com/beerbikesbacon/status/1186783818272952327

Clever

Creative

Curious

Why do they do it?

Financial gain

Reputation

Corporate reasons

Ideological reasons

Stumbled upon something

What makes you a target?

Popularity

Politics & perspective

People

Pot-luck

What can you do to start reducing risk?

No magic solution

Embed security considerations into the whole project workflow

“

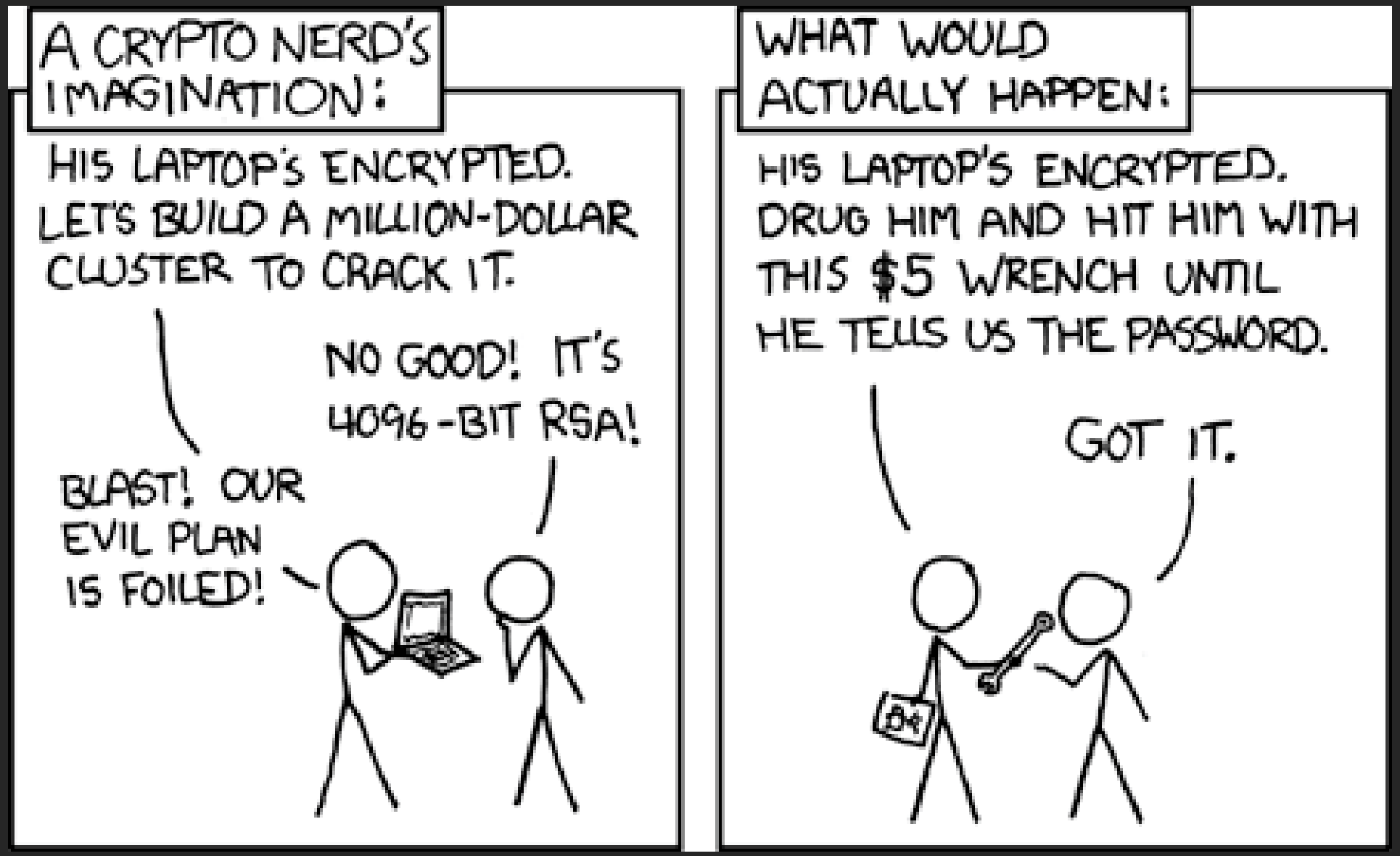
No-one has the time or money for securing their systems until it’s too late

Clinton Ingrams

https://twitter.com/cfing99

It is every developers responsibility

The people problem



https://xkcd.com/538/

@Brunty

Principle of least privilege

Limit who has access to what

Do all your devs really need 24/7 access to your production DB?

“

No developer should ever have a permanent login, or access to any credentials

David McKay

https://twitter.com/rawkode/status/1182213985661308928

@Brunty

“

That's not to say that a “Break Glass” button in the admin interface can't generate a prod database login that's valid for an hour; but it needs to log who requested it and take a reason; and notify slack, et al

David McKay

https://twitter.com/rawkode/status/1182213789686620160

Where is your data stored?

MongoDB Database Exposed 188 Million Records: Researchers

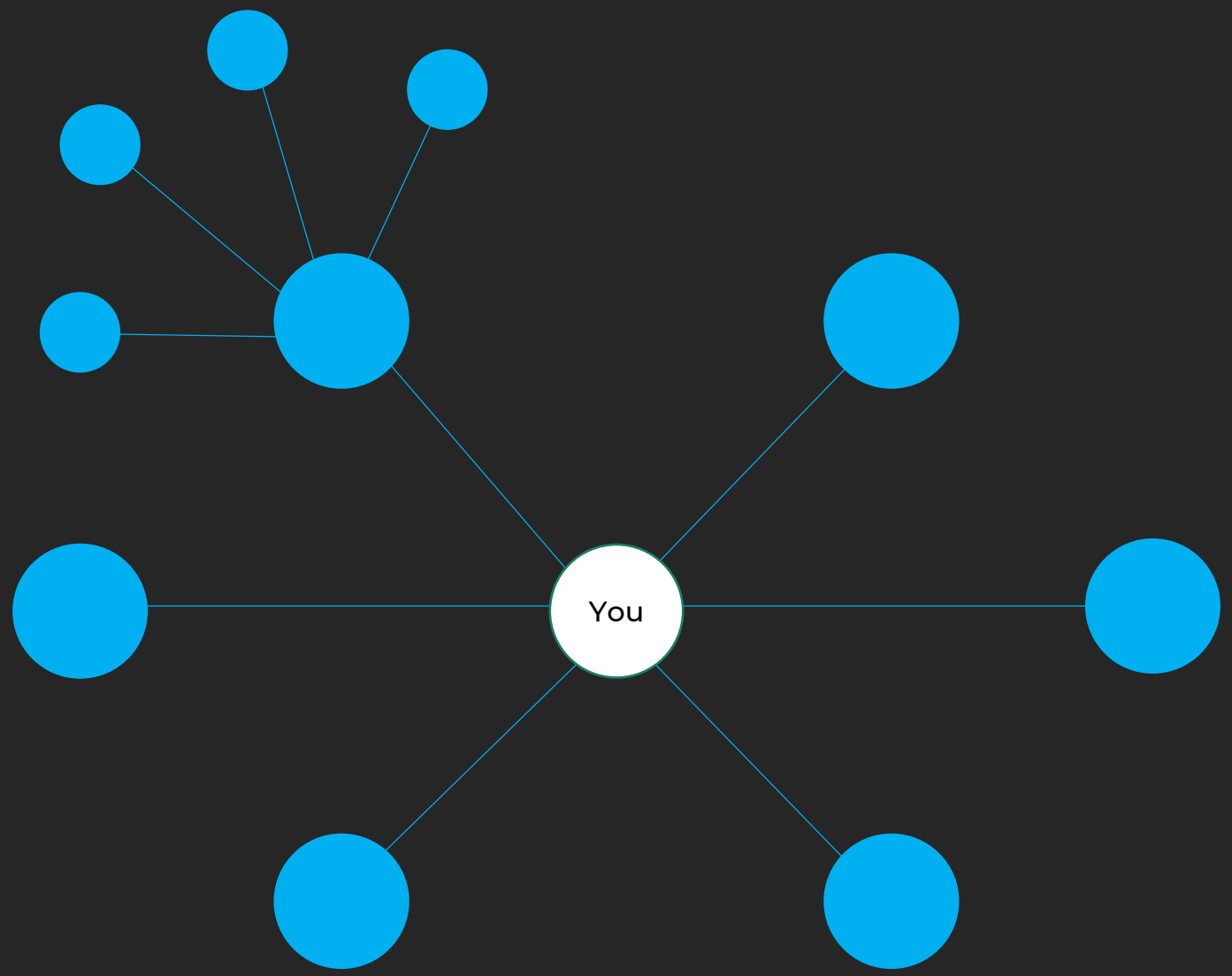
Data Apparently Originated in a GitHub Repository

https://www.bankinfosecurity.com/mongodb-database-exposed-188-million-records-researchers-a-12769

@Brunty

Who are the third parties you trust with your data?

Who are the third parties you trust with your customer data?



@Brunty

Shodan

https://www.shodan.io

You can’t lose what you don’t have

@Brunty

Encrypt data in transit
and at rest

HTTPS all the things

Check your repos for secrets

zricethezav/gitleaks

https://github.com/zricethezav/gitleaks

Check your public sites for secrets

Google dork queries

Curiosity

"what if..."

Don’t trust user input

“I’d like to be removed from the mailing list please”

@Brunty

“I’d like to be removed from the mailing list please”

@Brunty

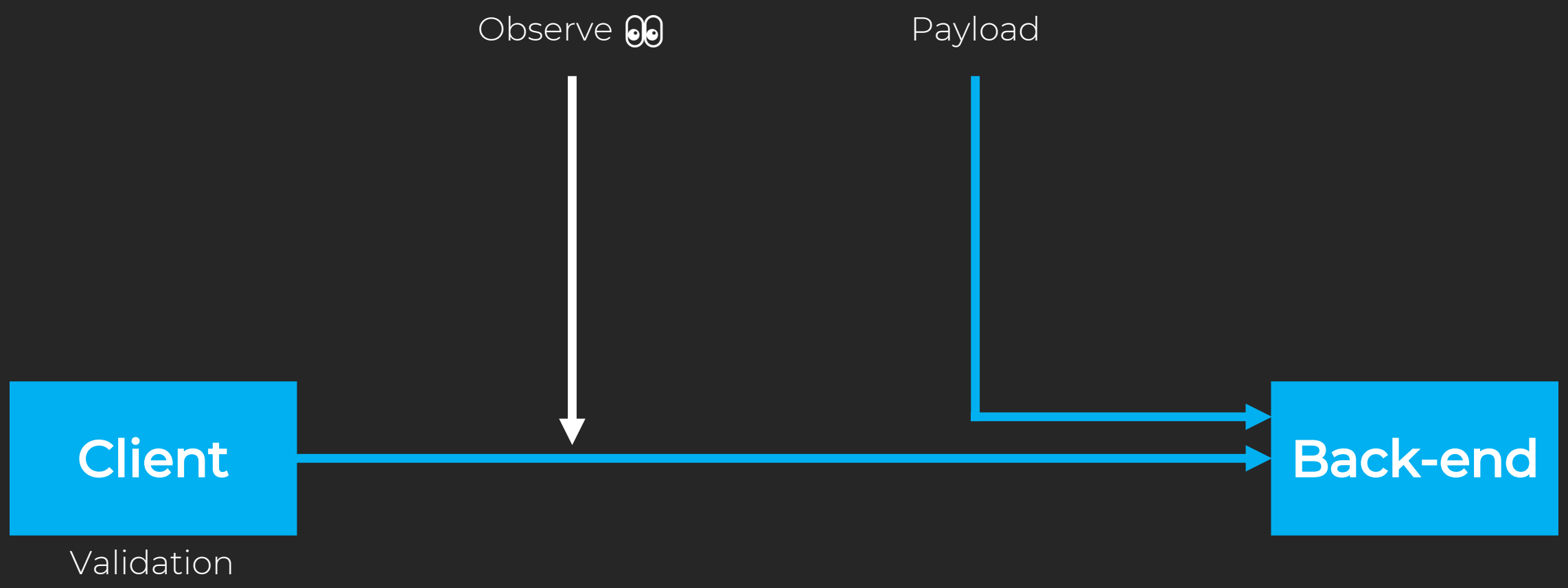
Use prepared statements

https://en.wikipedia.org/wiki/Prepared_statement

Don’t trust data

https://news.ycombinator.com/item?id=8336025

Don’t just validate client-side



@Brunty

Broken access control

Do you trust this?

@Brunty

123457
?

https://en.wikipedia.org/wiki/Attribute-based_access_control

@Brunty

Don’t trust users ~~input~~

Broken authentication

https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

Hash passwords properly

Don’t re-use passwords

https://blog.lastpass.com/2018/05/psychology-of-passwords-neglect-is-helping-hackers-win.html/

haveibeenpwned.com

@TroyHunt

Breaches you were pwned in

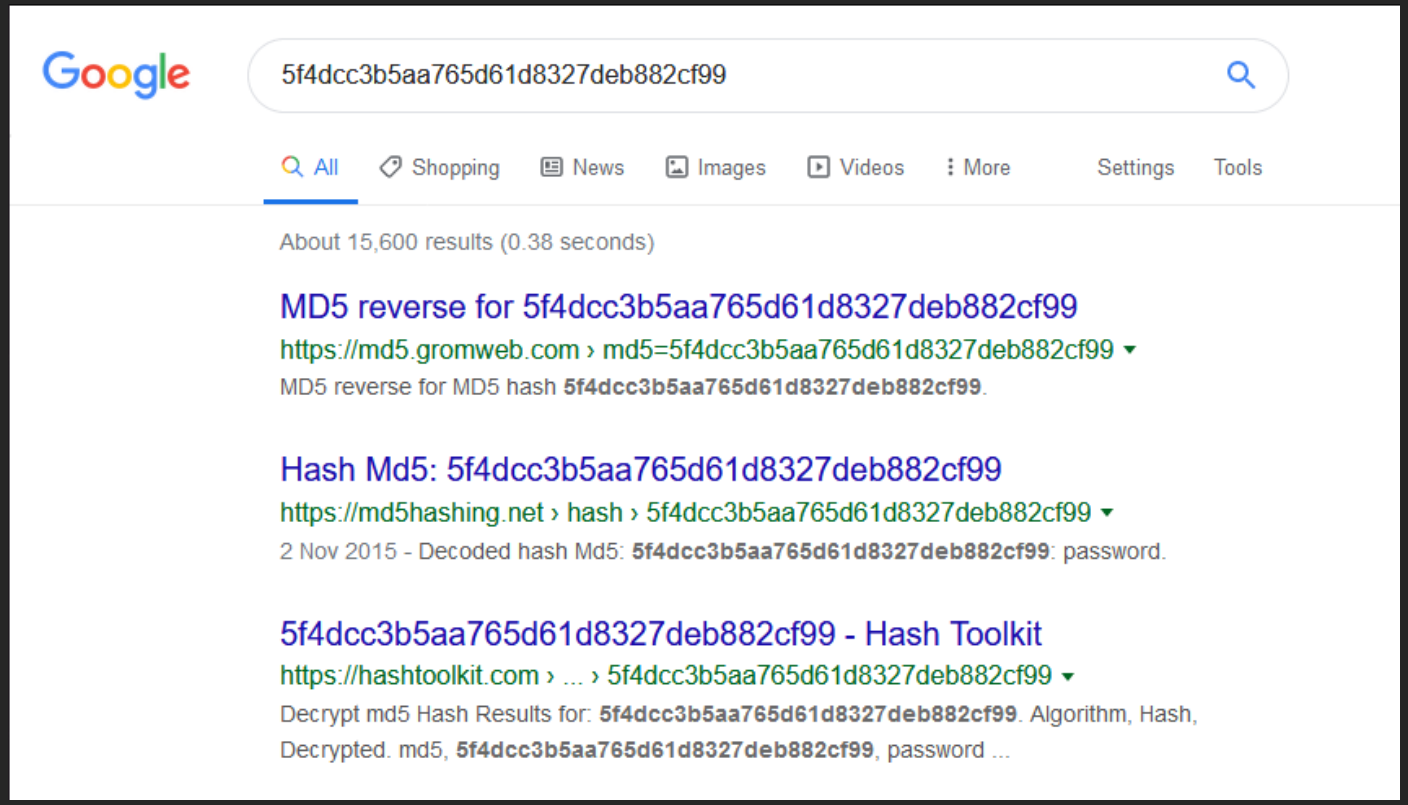
A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Don’t allow your users to re-use passwords

5f4dcc3b5aa765d61d8327deb882cf99



password

@Brunty

pwned passwords API

https://www.troyhunt.com/pwned-passwords-version-5/

@Brunty

Use

Multi Factor Authentication

But not SMS

What packages do you trust in your application?

https://help.github.com/en/articles/listing-the-packages-that-a-repository-depends-on#supported-languages

More packages than you think

Front-end

Mobile App(s)

Back-end

Platform / OS

Infrastructure

Keep them up-to-date

You have more surface area than you might think

@Brunty

No magic solution

Mistakes will happen

Mostly, it's not like the movies.
(Sorry)

@Brunty

Evaluate who you trust with data

Security at all stages of the project

Principle of least privilege

Encrypt data in transit and at rest

Check for public secrets

Don’t trust users & input

Hash passwords properly

Ensure your components aren’t vulnerable

OWASP Top Ten

Always be curious

Please

Remember to rate this session

Thank you!

Danke!