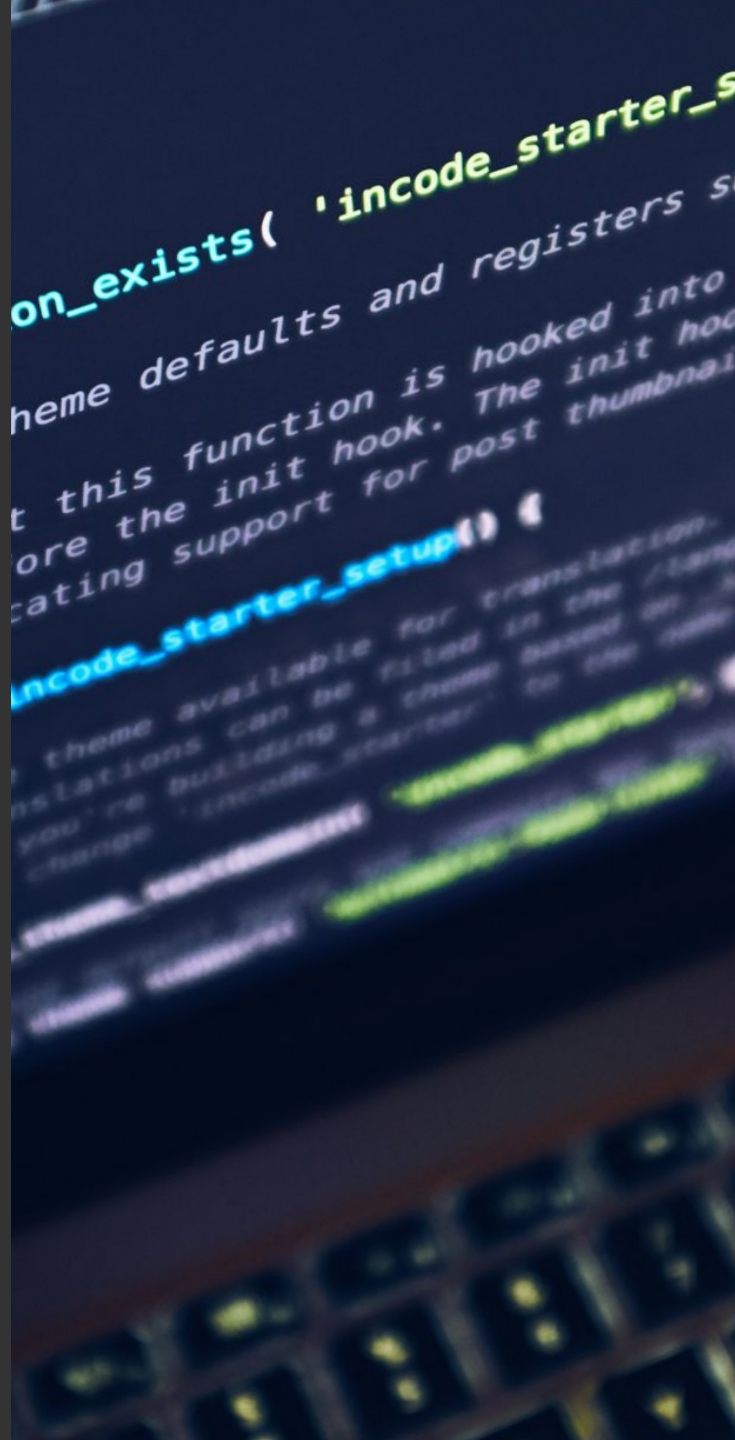
taptu

Web dev security flaws 101

Lessons learned as a pen-testing web developer



Jakob Pennington
@JakobRPenny

What's in store

1. Why all the talk about Cybersecurity?
2. XSS Demo
3. SQL Injection Demo
4. What can we developers do?

Why all the talk about Cybersecurity?

We just want to build stuff...


CryptoLocker
Payment for private key
Private key will be destroyed on
9/20/2013
6:48 PM
Time left
71 : 57 : 22
Choose a convenient payment method:
Bitcoin (most cheap option)
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.
You have to send below specified amount to Bitcoin address 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh and specify the transaction ID, which will be verified and confirmed.
Home Page
Getting started with Bitcoin
Enter the transaction ID and press «Pay»:
2 BTC
<< Back
PAY

SCOTT MORRISON

Jack Genesin

19 hrs ·

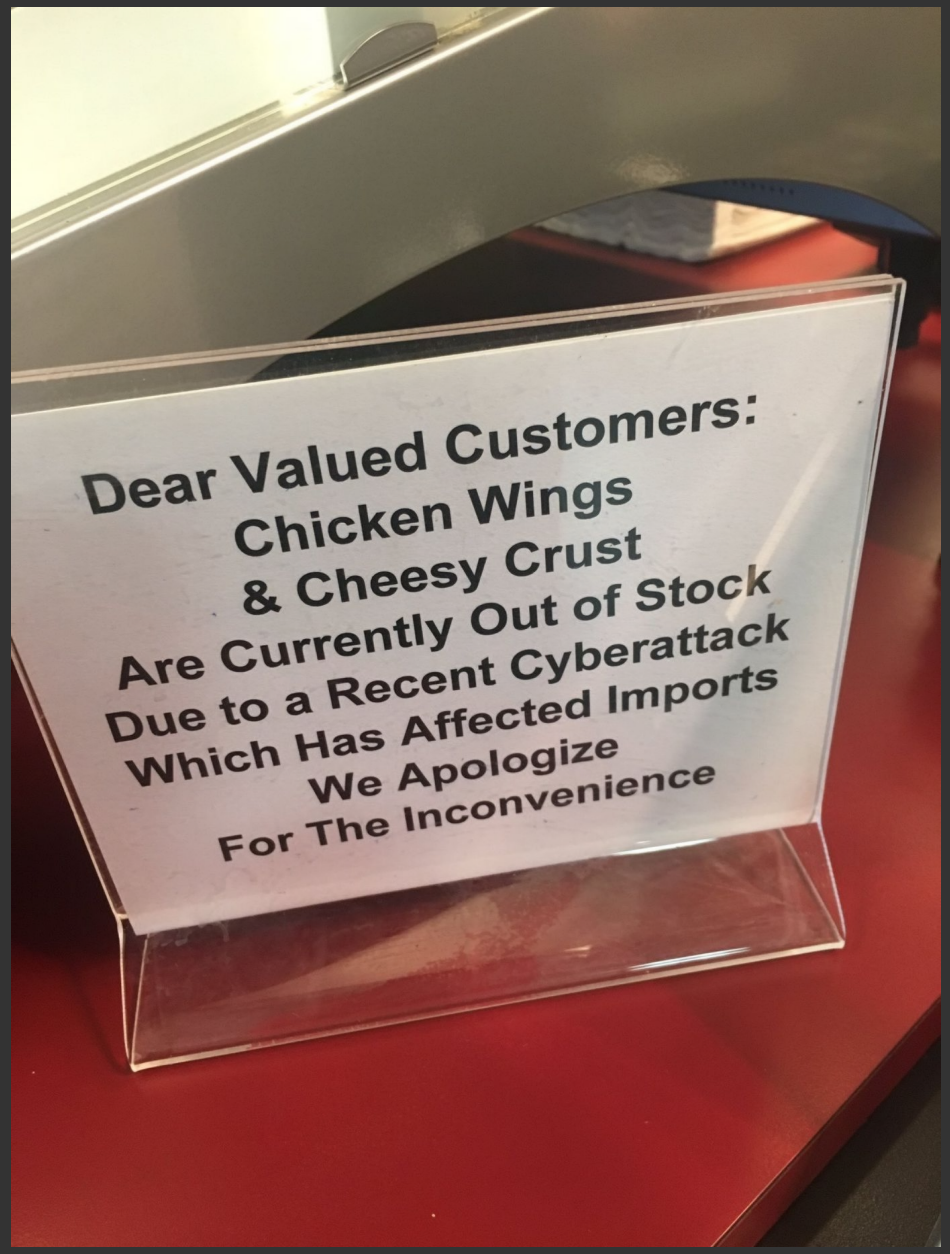
So, the PM forgot to renew his website and it expired today...
Most fun I've had with $50 in a long time.

Scott Morrison

www.scottmorrison.com.au/ ▾

Scott Morrison. Read the full story of how Jack Genesin bought the PM's domain here. Music courtesy of XOFF Records Song – Scotty Doesn't Know – Lustra.

About Scott · Electorate of Cook · Grants and Funding · Local News


Dear Valued Customers:
Chicken Wings
& Cheesy Crust
Are Currently Out of Stock
Due to a Recent Cyberattack
Which Has Affected Imports
We Apologize
For The Inconvenience

Breaches in 2018

What a year it has been...

Facebook

API data leak

50 - 90 million access tokens Stolen

MEGA

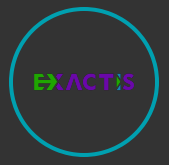
Compromised browser extension

Leaked credentials of popular websites

Apple

Hacked by 16yo Australian

1TB + customer data stolen



Exactis

Misconfigured ElasticSearch DB

340 million records stolen

MyFitnessPal

Unknown

150 million user accounts compromised

Orbitz

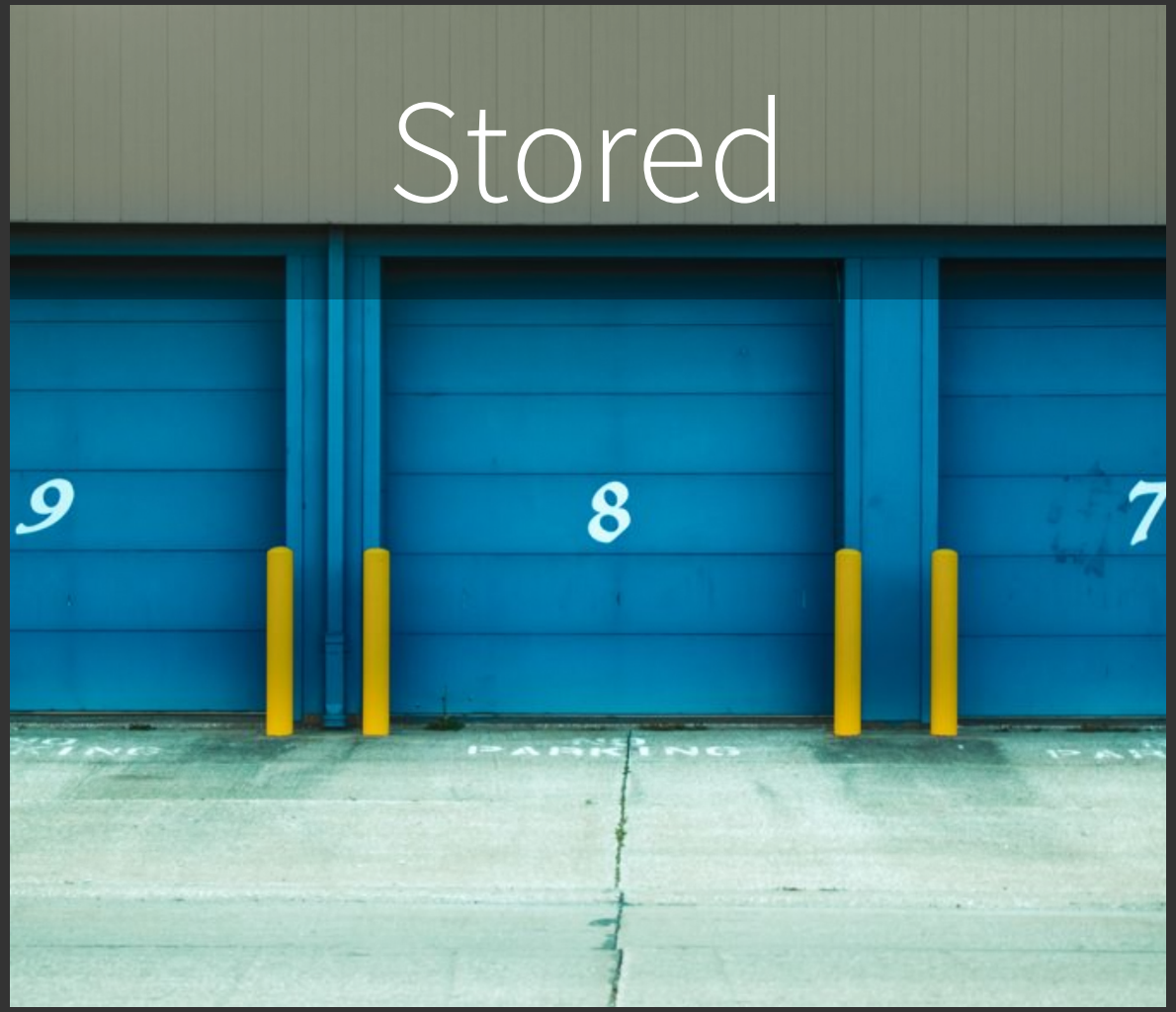
Legacy website breached

880,000 credit card details exposed

Vulnerability 1

Cross-Site Scripting (XSS)

What is Cross-Site Scripting



Demo 1

Cross-Site Scripting

Common XSS Attacks

- Steal session cookies
- Perform actions on the user's behalf
- Intercept credentials
- Keylogger
- Crypto mining
- Modify content / behaviour
- Create a botnet
- BeEF Framework
- Can lead to a shell

  Misconfigured Election apps

Cross-Site Scripting Mitigation

Don't Trust User Input

- Sanitise before printing
  Always...
- Sanitise before storing
  If your API is serving multiple apps
- Your framework is here to help you
  Don't fight it
- Be wary of vulnerable dependencies
- Content-Security-Policy and X-XSS-Protection headers
- All Content over HTTPS with HSTS

Vulnerability 2

SQL Injection

How SQL Injection Works

SELECT * FROM users WHERE firstName LIKE '${query}' AND username != 'admin'

SELECT * FROM users WHERE firstName LIKE 'Jakob' AND username != 'admin'

SELECT * FROM users WHERE firstName LIKE '' OR 1=1 --' AND username != 'admin'

Demo 2

SQL Injection

SQL Injection Mitigation

Seariously!

Don't trust user input

- Paramaterised queries
- Stored Procedures
- Utilise trusted frameworks

  Find out how people avoid SQLi in ${myFavouriteFramework}

Oh my Jakob...

What do we do?

Penetration Testing

Penetration Testing

Should not be the core of your secure software development program.

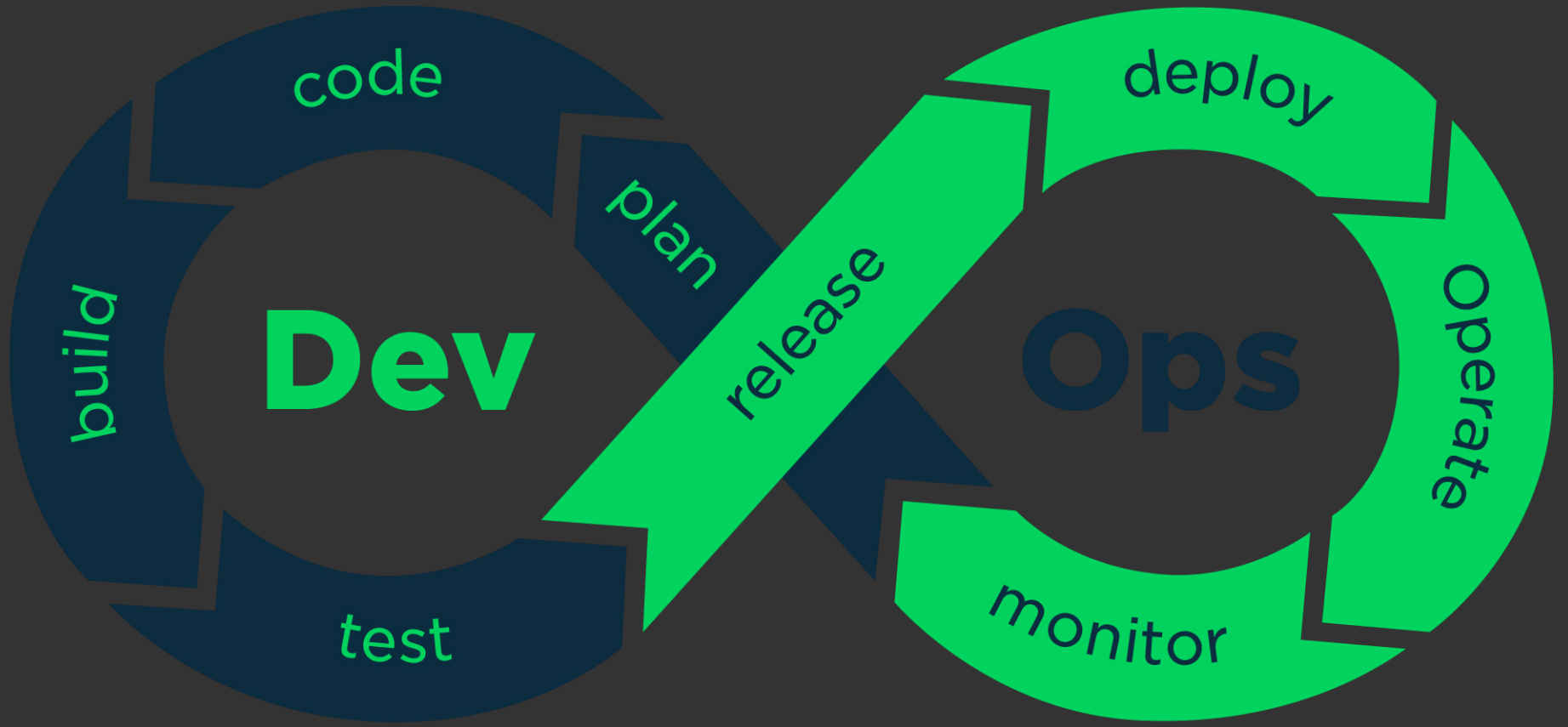
Education

Become familiar with common threats + attacks

1. OWASP Top 10
2. OWASP Testing Guide
3. Do some challenges
   - Pentester Labs
   - HackTheBox
4. Secure Software Development Training

DevOps

Development + Operations



DevSecOps

Development + Security + Operations

DevSecOps

Development + Security + Operations

Pre-commit	Commit (CI)	Acceptance	Production (CD)	Operations
IDE plugins	Static Code Analysis	Infrastructure as code	Configuration checking	Pen-testing
Git hooks	Unit Testing	Scanning	Secret management	Bug Bounties
Peer reviews	Dependency Management	Security acceptance tests	Hardening	Scanning
Secure coding standards				Monitoring

Jakob Pennington

Cybersecurity / Software Specialist
@Taptu IT Advisory

jakob.pennington@taptu.com.au

linkedin.com/in/jakobpennington

medium.com/@jakob.pennington

@JakobRPenny