HEROKU

1. Create a free Heroku account at https://signup.heroku.com
2. Deploy a Heroku instance of Juice Shop from the deploy button at this URL: https://github.com/bkimminich/juice-shop#setup

DOCKER

1. Install Docker on your machine
2. Start Docker
3. In the command line Run docker pull bkimminich/juice-shop
4. In the command line Run docker run --rm -p 3000:3000 bkimminich/juice-shop
5. Point your browser at http://localhost:3000 or http://192.168.99.100:3000

NODE

1. Install Node.js on your machine
2. Run git clone https://github.com/bkimminich/juice-shop.git
3. Go to the cloned folder with cd juice-shop
4. Run npm install
5. Run npm start
6. Point your browser at http://localhost:3000

WEB APPLICATION SECURITY

A HANDS ON TESTING CHALLENGE

Daniel Billing | @thetestdoctor

HELLO!

- UK based software tester
- 17 years in tech and testing
- 5 years learning security testing
- Speaker, coach, Ministry of Testing contributor, event organiser, co-host of the Screen Testing podcast

WARNING AND DISCLAIMER

Unauthorised behaviour such as hacking, undermining and defacing a system, or stealing data is illegal in the USA, UK and throughout the European Union (and many other countries).

Do not perform security or penetration testing on any systems you do not have specific authorisation to do so. You will face fines and most likely a prison sentence.

I cannot and will not be held responsible if you perform illegal activity with the knowledge and skills covered in this workshop.

AGENDA

- Introductions
- Course Objectives
- Applications Under Test
- Helpful Tools
- Threat Risk Modelling
- Vulnerabilities
- Information Gathering
- Ethical Hacking Techniques
- Learning Beyond This Workshop

OBJECTIVES

- An introduction to security testing
- Discover how security testing can be incorporated into your day to day work.
- Begin to ask the critical questions about application security
- Explore some vulnerable applications
- Have Fun!!!!

WHY DO SECURITY TESTING?


INTEGRITY
THE SECURITY TRIANGLE
AVAILABILITY
CONFIDENTIALITY

THREATS - RISKS - VULNERABILITIES

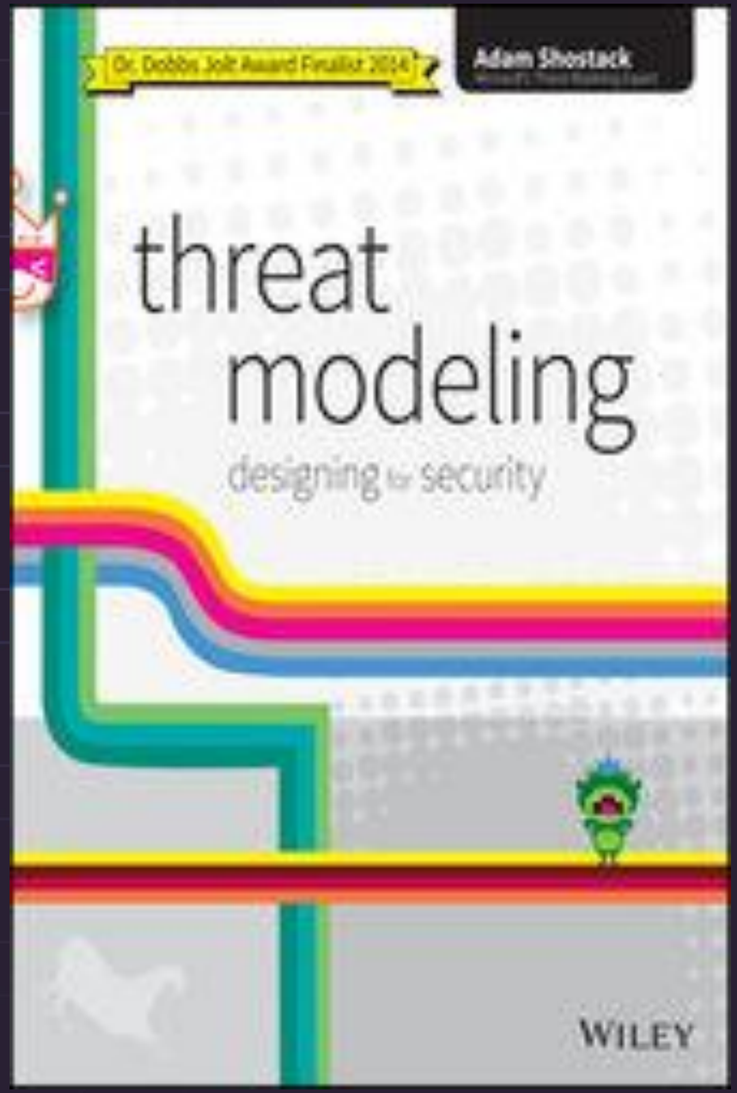
A source of danger, harm or attack to a system

THREAT RISK MODELLING

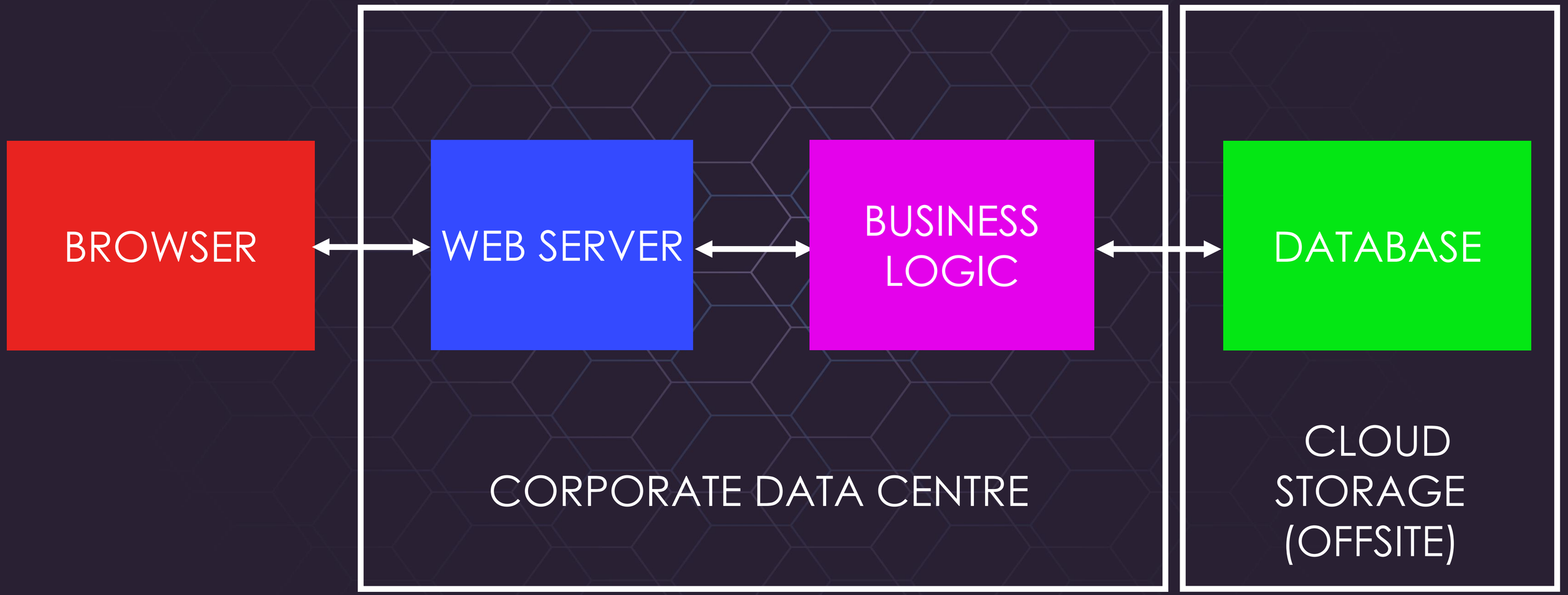
“Threat modelling is about using models to find security problems, abstracting away a lot of details to provide a look at a bigger picture, rather than the code itself…you model as a way to anticipate threats that could affect you”

Threat Modelling: Designing for Security

Adam Shostack



THREAT RISK MODELLING



STRIDE

HTTPS://MSDN.MICROSOFT.COM/EN-US/LIBRARY/EE823878(V=CS.20).ASPX

S - SPOOFING

T - TAMPERING

R - REPUDIATION

I - INFORMATION DISCLOSURE

D - DENIAL OF SERVICE

E - ELEVATION OF PRIVILEGE

ACTIVITY 1:
BUILD A THREAT MODEL

THREATS - RISKS - VULNERABILITIES

The likelihood that a threat will cause danger or harm to a system

INFORMATION GATHERING

USEFUL TECHNIQUES

SPIDERING
VIEWING SOURCE CODE
REQUESTS AND RESPONSES
ANALYSIS OF ERROR CODES
SEARCH ENGINE DISCOVERY
SOCIAL ENGINEERING

ACTIVITY 2:
EXPLORE AND GATHER INTELLIGENCE

THREATS - RISKS - **VULNERABILITIES**

A vulnerability leads to an attack on the system, if exploited

DISCOVERING VULNERABILITIES

INJECTION

BROKEN AUTHENTICATION

SENSITVE DATA EXPOSURE

CROSS SITE SCRIPTING

INSECURE COMPONENTS

INSECURE LOGGING AND MONITORING

LEARNING BEYOND THIS WORKSHOP

- OWASP
  - Top 10, OpenSAMM, Testing Guide and ASVS
- SANS
- Bloggers and Podcasters
  - Troy Hunt
  - Graham Cluely
  - Scott Helme
  - Karen Elazari
  - Many many others
- Pluralsight
  - Many Appsec courses, including by Troy Hunt
- Advanced
  - CEH (Certified Ethical Hacker)
  - OSCP (Offensive Security Certified Professional)
- Kali - linux distro - has many useful tools

CONTACT ME

Twitter @thetestdoctor

Email: daniel.billing@thetestdoctor.co.uk

Ministry of Testing and testers.io Slack

THE *TEST* DOCTOR

THANK YOU!