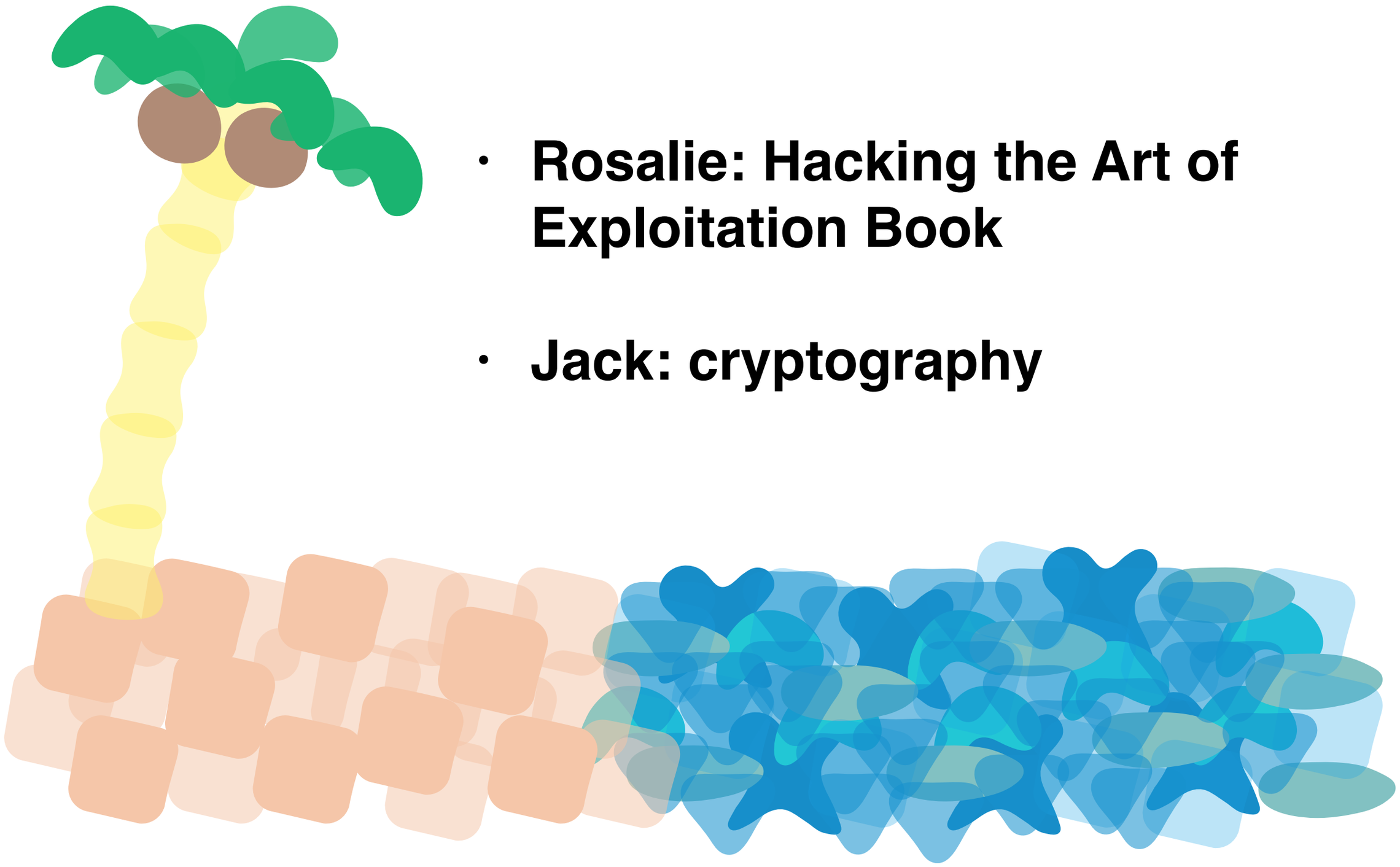
Don’t Panic!

A Hitchhiker’s Guide to Software Safety

Rosalie Tolentino and Jack Singleton

Our Journey Begins…

Exploration



- **Rosalie: Hacking the Art of Exploitation Book**
- **Jack: cryptography**

Takeaways

Understanding exploits is hard but fun

Takeaways

The design of the software can be a major blocker to security

Takeaways

Hacking the Art of Exploitation is not super useful in your day-to-day unless you're programming in C.

Takeaways

Crypto coding hasn't been that useful (yet) but it was interesting

Takeaways

Configuring encryption algorithms can be dangerous

Resources

- **Hacking: The Art of Exploitation**
  - **by Jon Erickson**
- **Matasano Crypto Challenges**
  - **http://www.cryptopals.com**

Pentesting

hydra

crunch

tcpdump

recon-ng

nbtscan

wireshark

metasploit

edb

Information Gathering

google-dorking

netcat

Penetration

theharvester

cewl

netcraft

dnsrecon

openvas

nmap

dnsenum

Maintain & Extend Access

passthehash

msfvenom

http_tunnel

proxychains

Takeaways

Application security is just one part of being secure

Takeaways

Exploits do not have to be very advanced

Takeaways

Diligently update your software

Takeaways

Vulnerabilities live in the details

Takeaways

Only scratched the surface of Pentesting; need more than point-and-click tools

Resources

- **Offensive Security**
  - **https://www.offensive-security.com/**

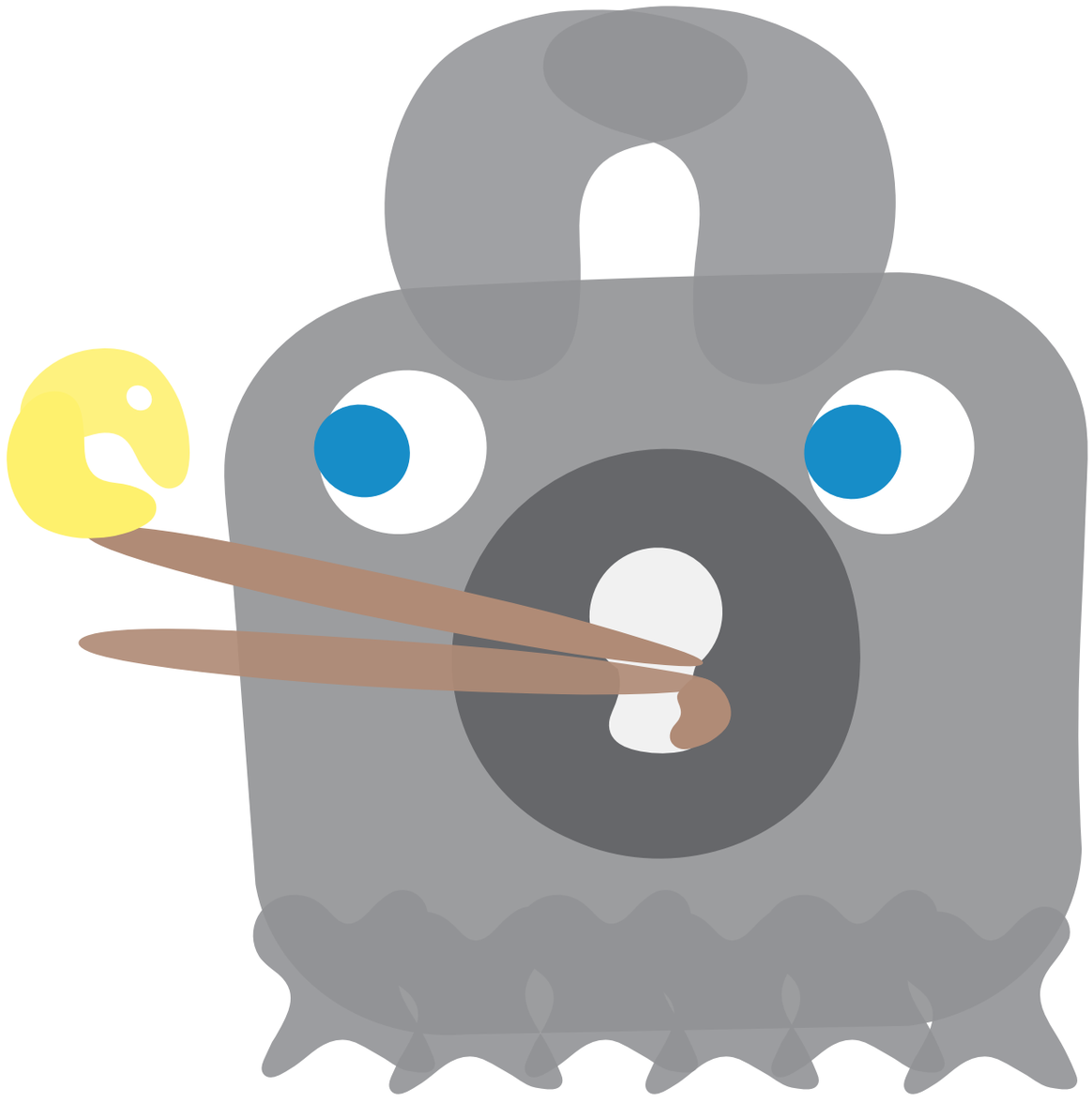
- **Kali Linux**
  - **https://www.kali.org/**

- **SecLists (by Fyodor)**
  - **http://seclists.org/**

- **CVE Databases**
  - **https://cve.mitre.org/cve/**

Security Games

- **Bandit**
- **Leviathan**
- **Narnia**
- **Krypton**



Takeaways

- **Security games can be fun and addictive**
- **Get your friends to play**
- **Think beyond how software is meant to work**

Takeaways

Prerequisite knowledge is important for hands on exercises

Takeaways

Facilitation is key

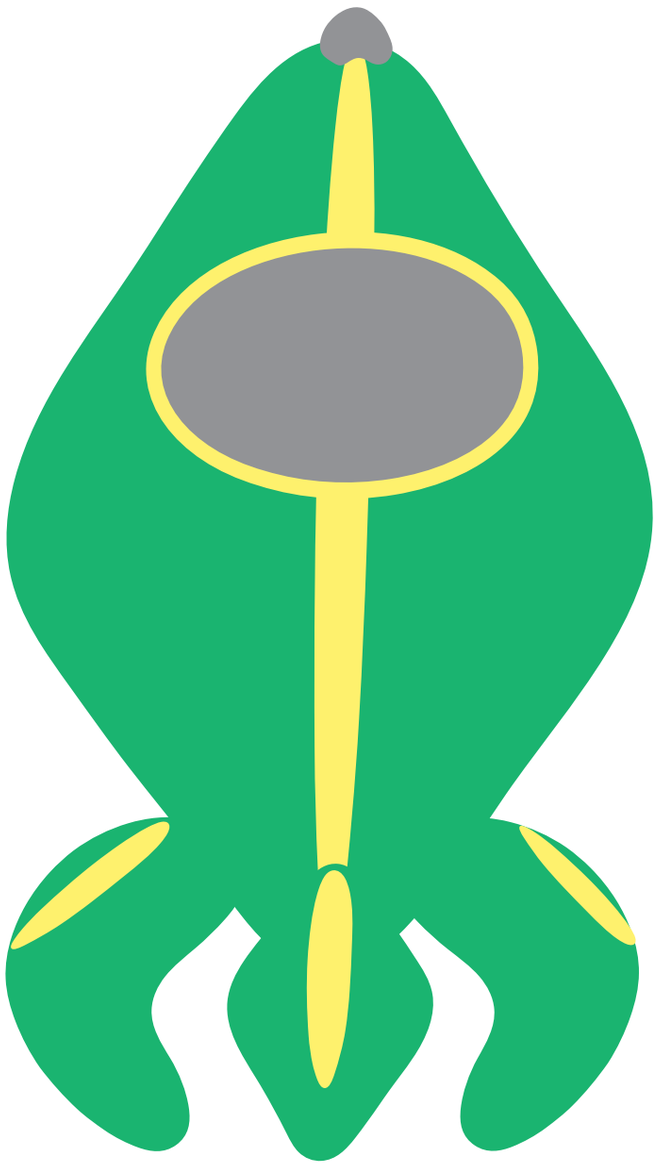
Takeaways

Not a good opportunity to write secure code.

Resources

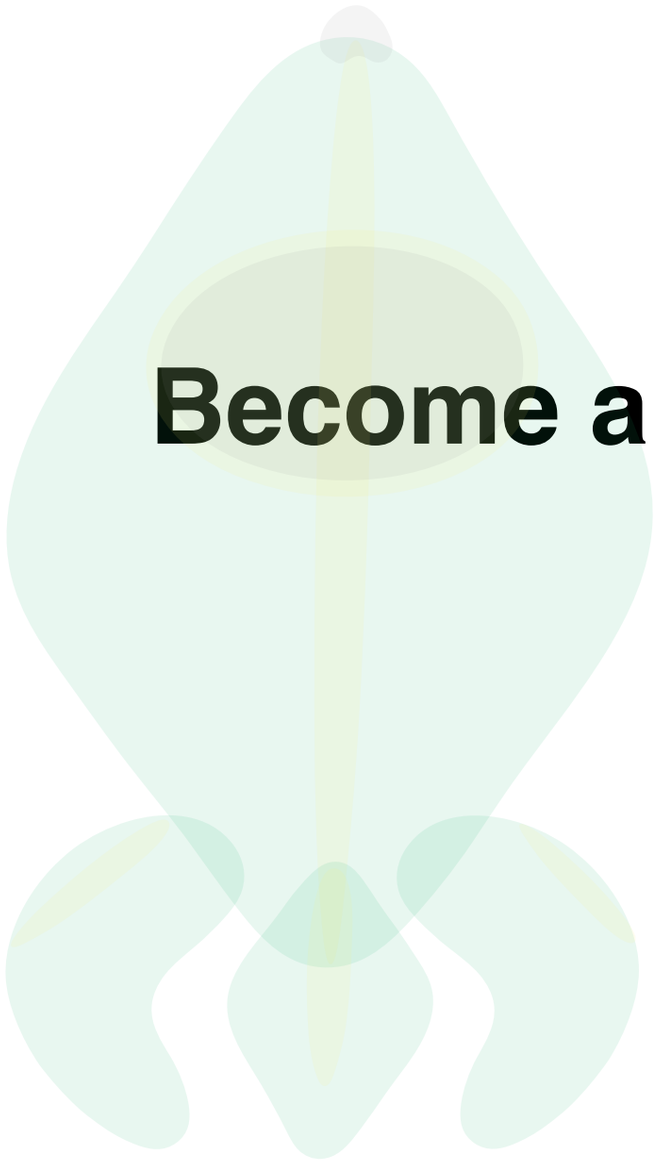
- **WebGoat**
  - **https://webgoat.github.io**
- **OverTheWire (Bandit, Leviathan, Krypton)**
  - **https://overthewire.org**

31c3 Conference



- **Other's mistakes and breakthroughs**
- **Blue Sky Thinking**
- **The Future of Security**
- **CTF**
- **Networking**

Takeaways



Become a part of the community.

Takeaways

CTF is (or can be) difficult

Resources

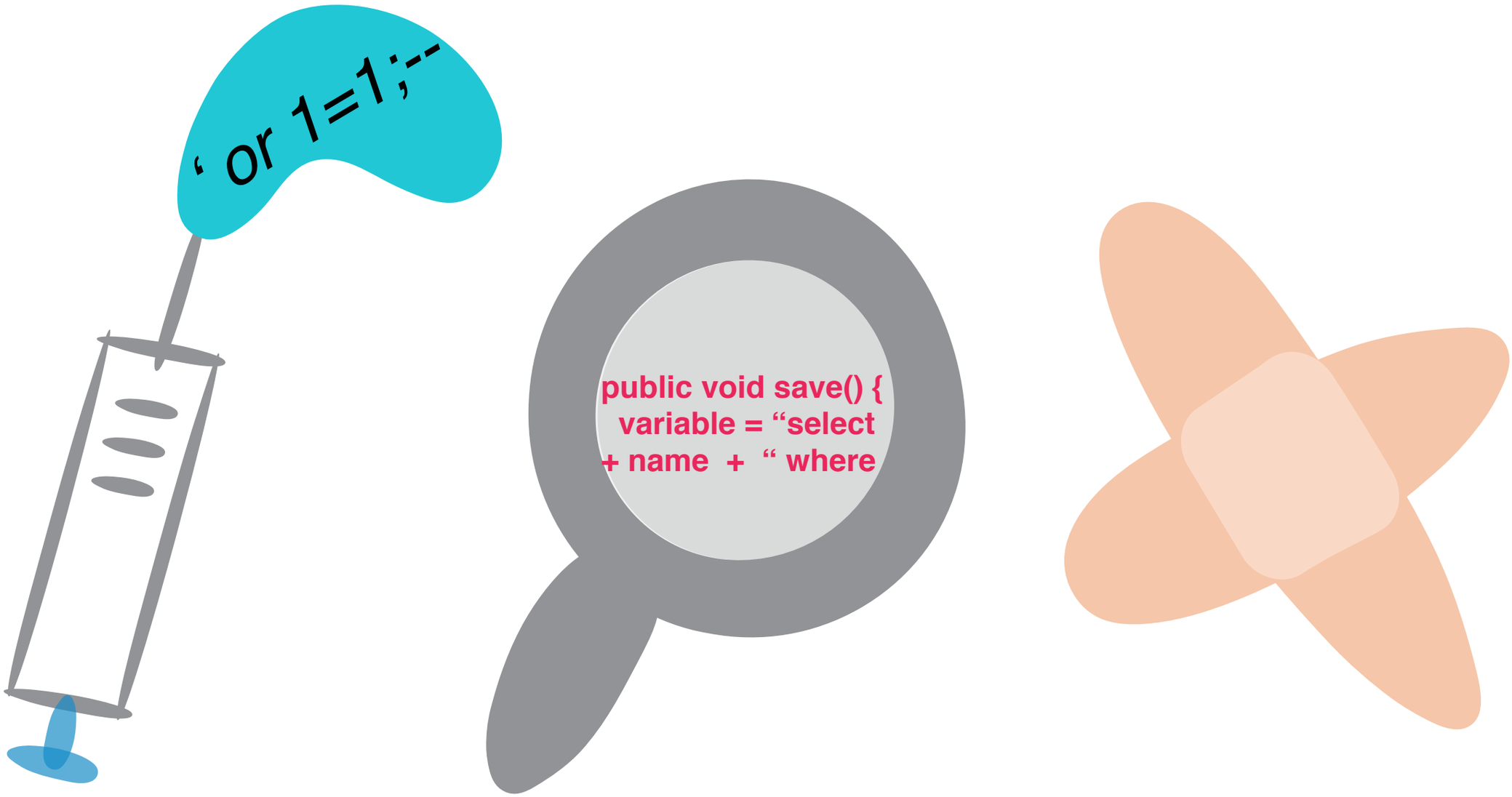
- **Chaos Communication Congress**
  - **https://en.wikipedia.org/wiki/Chaos_Communication_Congress**

- **CTF Write Ups**
  - **https://github.com/ctfs/write-ups-2014/tree/master/31c3-ctf-2014**

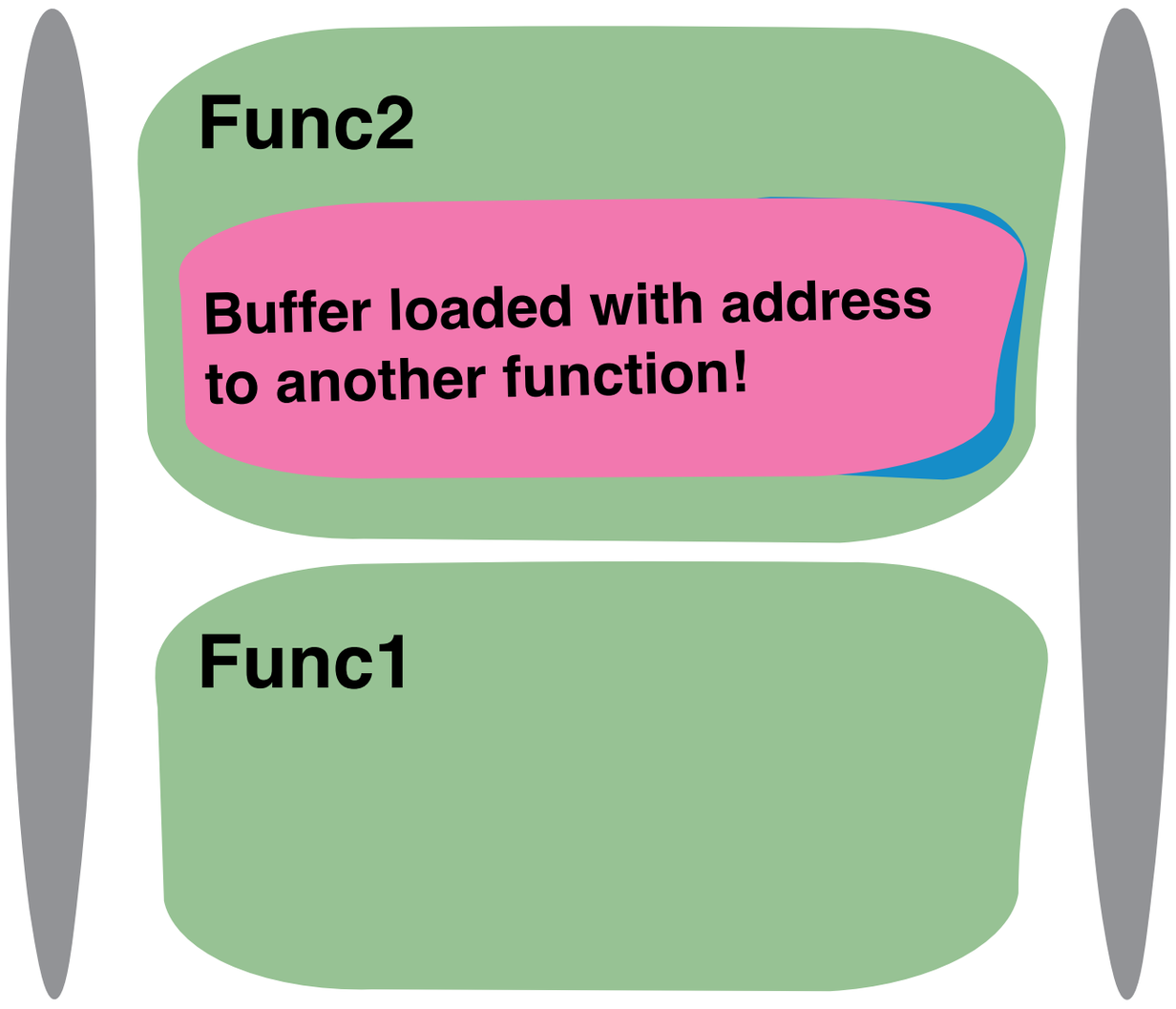
OWASP

- **Open Web Application Security Project**
- **3rd Party & Non Profit**
- **OWASP Top 10**

Injection Workshop



Buffer Overflow



- Technically heavy
  - Assembly
  - Memory segmentation
  - Only the beginning...

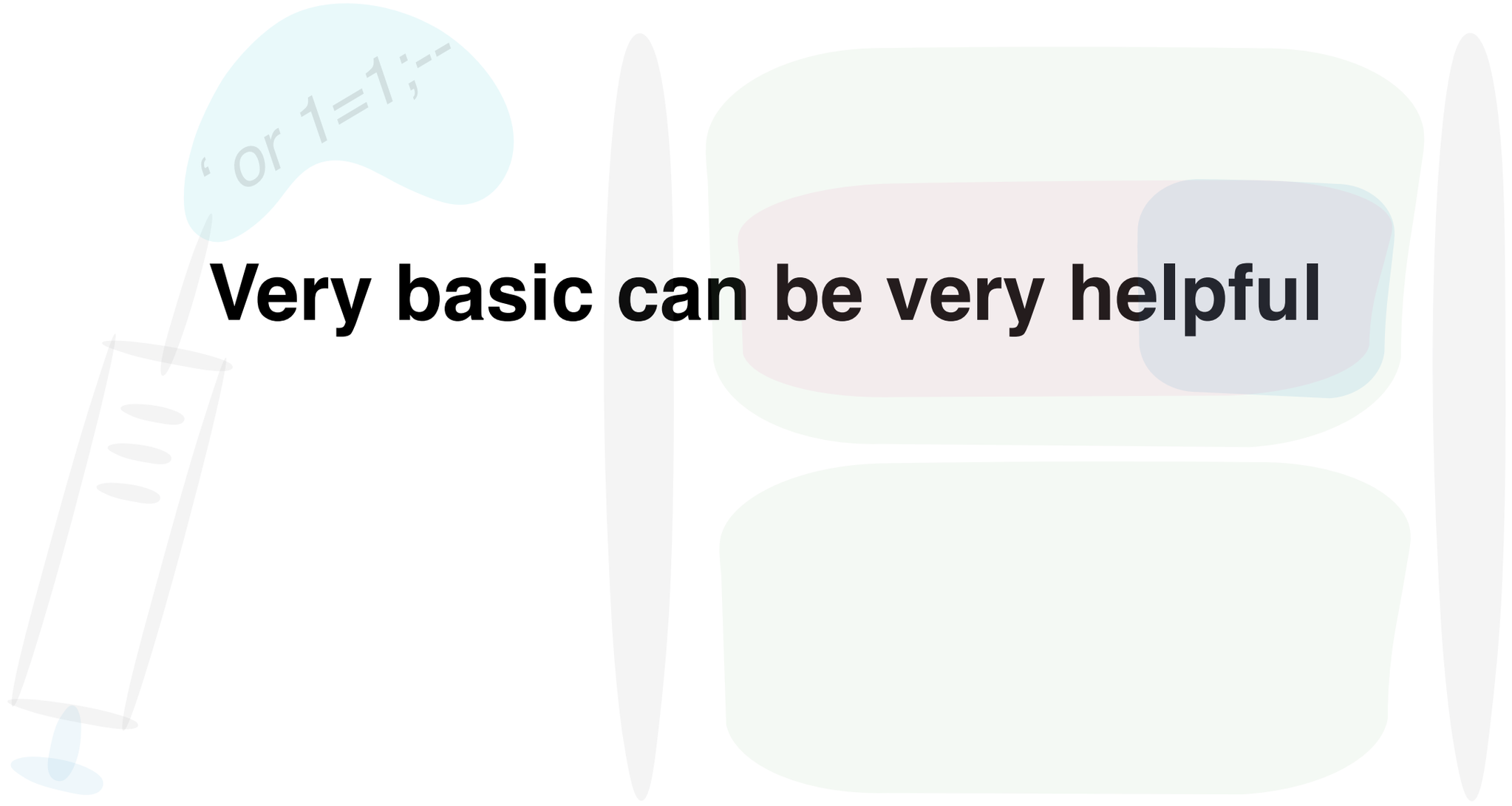
Takeaways

Hands-on is helpful

Takeaways

Specific, classic exploits transfer to other applications; for example, SQL Injection to Shell Injection

Takeaways



Very basic can be very helpful

Takeaways

We need to teach people about the layer they are used to working in

Takeaways

The architecture of your creation can work against you

Resources

- **Injection Workshop**
  - **https://github.com/jacksingleton/injection-workshop**
- **Joy and Buffers Overflowing**
  - **https://github.com/rosatolen/joy-and-buffers-overflowing**

Top 10 Workshops

- **Cross Site Scripting**
  - **Any Javascript, HTML, CSS working against you.**

- **Cross Site Request Forgery**
  - **Your browser is not your friend.**

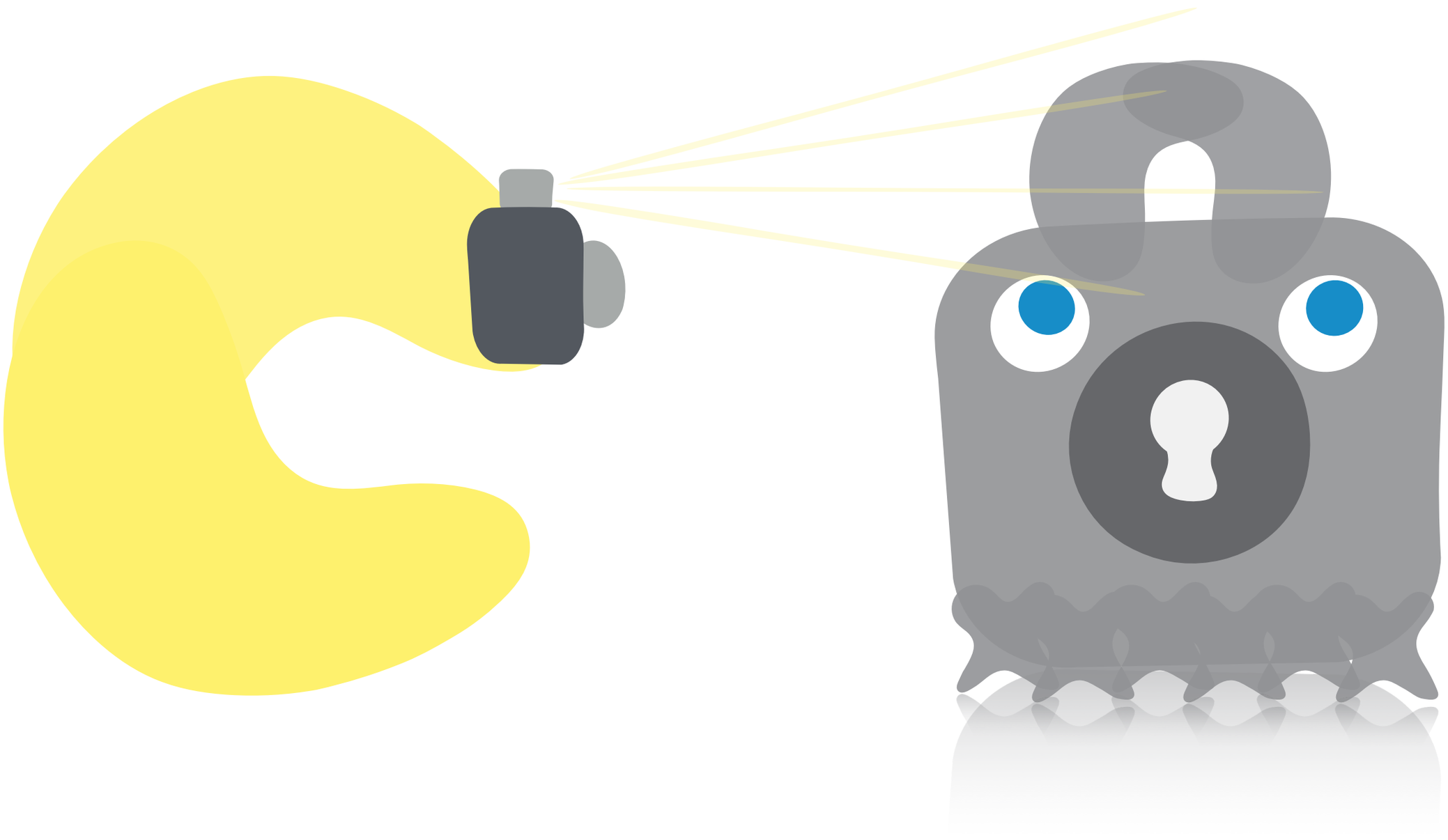
- **Vulnerable Dependencies**

Takeaways

Exploit… Discover Code Vulnerability… Fix!

1. **How do you identify that your code is insecure?**
2. **How do you show someone why that is important?**
3. **How do you fix it?**

Threat Modeling



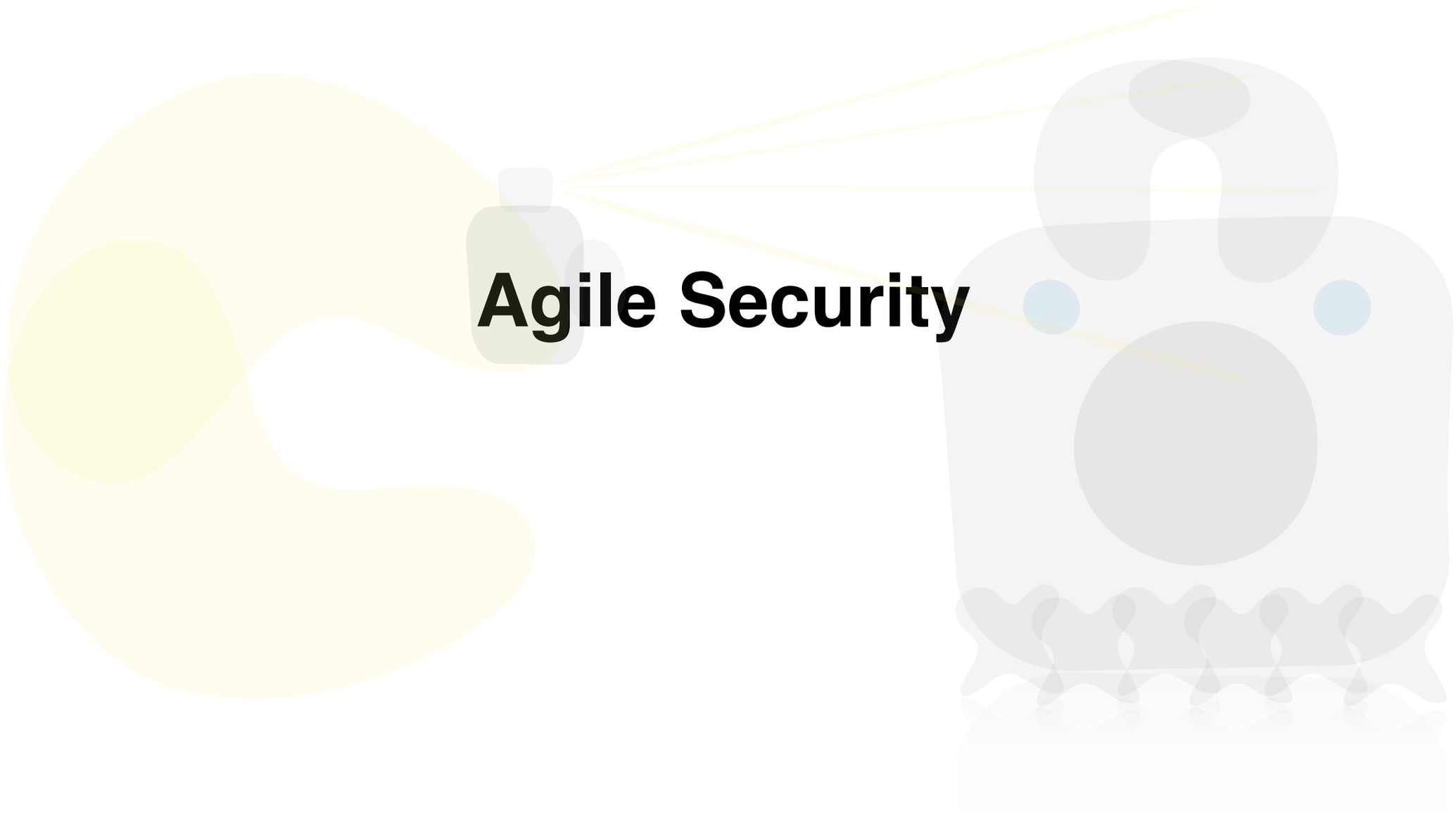
Takeaways

Secure Delivery is not just technical

Takeaways

Make it relevant to their project

Takeaways



Resources

- **Elevation of Privilege Card Game**
  - **http://www.microsoft.com/security/sdl/adopt/eop.aspx**

- **Attack Trees**
  - **https://www.schneier.com/paper-attacktrees-ddj-ft.html**

Overall Lessons

Security is huge:

- **Focus on the most relevant sections**
- **Team up with the community**
- **Find good mentors**

Overall Lessons

Architecture built without security in mind leads to unintentional, endemic problems

Overall Lessons

We need more resources on writing secure code

Overall Lessons

“Security is not a product, it's a process”
(Bruce Schneier)

Overall Lessons

Agile Security as the New Frontier

Thanks!
github.com/jacksingleton
github.com/rosatolen

Questions