Democratising Security practices

with **Reconmap** pentest automation and reporting

Santiago Lizardo

February 7, 2021

Outline

"Penetration testing, also known as pentesting, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually."
https://pentestreports.com/what-is-a-pentest.html

"A pentester, or penetration tester, is an individual who identifies security flaws within a network or system. They are often external consultants, authorized by a company to perform security audits on their IT ecosystem, and identify any potential cybersecurity risks."
https://pentestreports.com/who-is-a-pentester.html

What is Reconmap?

- Pentest automation and reporting tool
- Open-source (code)
- Makes pentesting accessible to all IT pros (developers, devops, sysadmins, ...)

How does Reconmap work?

1. Web application is used to create engagement details
2. CLI tool runs commands and pushes results to the API
3. A pentest report is automatically generated

Reconmap feature set

- Client, project, tasks management all in one.
- Reusable project templates and vulnerability management.
- Can scale to teams and projects of any size.
- Includes user roles, search, data export/import, ...

How to get started?

Manual setup

Follow setup instructions
Requires significant time to install and maintain
Community support (chat)

SaaS

Affordable hosting
Ready in minutes
Technical support (phone, email, chat)

Staying in touch

- Github community
- Twitter updates
- Facebook
- Gitter chat