PENTESTER ACADEMY

Pentesting automation with **Reconmap**

Santiago Lizardo

September 4, 2021

About the presenter

- Reconmap's founder
- +20 years doing software engineering
- Cyber security enthusiast
- https://github.com/santiagolizardo

Reconmap's origin

Pentesting pain points

- Repetition
- Ineffective collaboration
- Ineffective communication

Reconmap's mission

Reconmap's mission is to **accelerate the time it takes to do vulnerability assessment and pentesting**, through the use of templating, automation and machine learning.
From weeks to days, or days to hours.

Reconmap's approach

- Templates to avoid repetition
- Automation and ML to speed up the process

Result:

Pentesters spending more time doing research, and less time doing repetitive, boring, tedious work such as parsing files manually or creating handcrafted pentest reports for their clients.

Reconmap's Today - September 2021

- 1 year old
- Open source and SaaS
- Small but growing community
- Used in production by people around the world

Recomap's feature set

- Client, project, tasks management all in one.
- Reusable project and vulnerability templates
- Automatic pentest report generation (HTML, PDF, DOCX)
- Command line interface (CLI) and Rest API
- Integrated browser terminal
- Can scale to teams and projects of any size.
- Stats dashboard, user roles, documents, markdown, audit log, integrated search, tagging, data import/export, ...

Who is it for?

Any InfoSec professional:

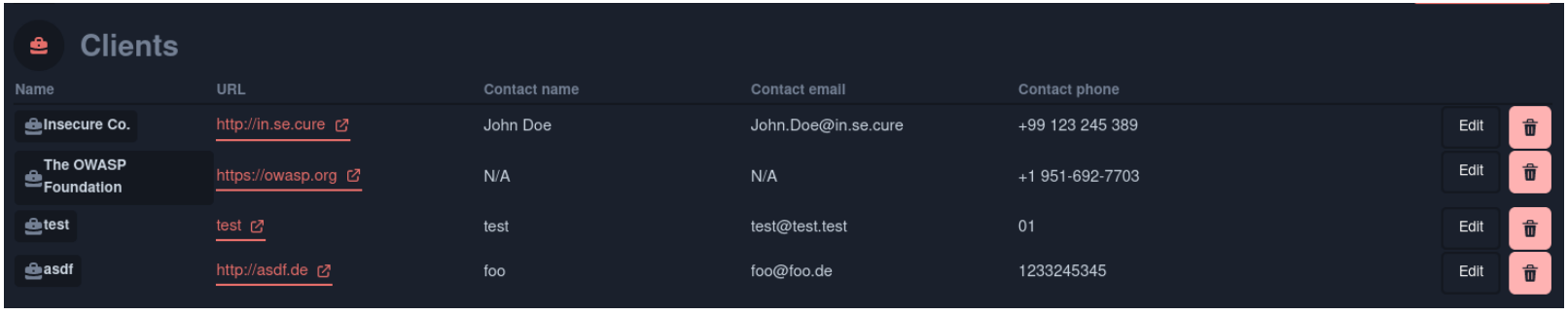
- Blue, Purple and Red teams
- Pentesters
- Bug bounty hunters
- Ethical hackers
- Security researchers

Individual or teams

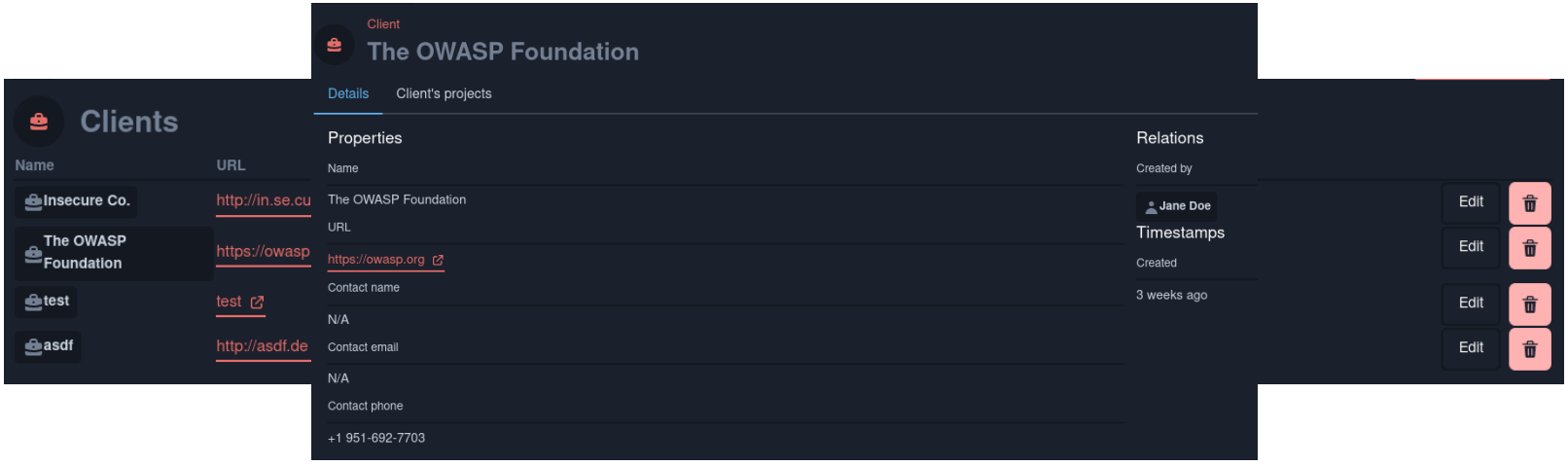
Pentesting step by step with Reconmap

1. Create client
2. Create project from scratch or template
3. Complete tasks in the project. Some might require running command automation.
4. Try exploit the vulnerabilities found
5. Generate report for client and share

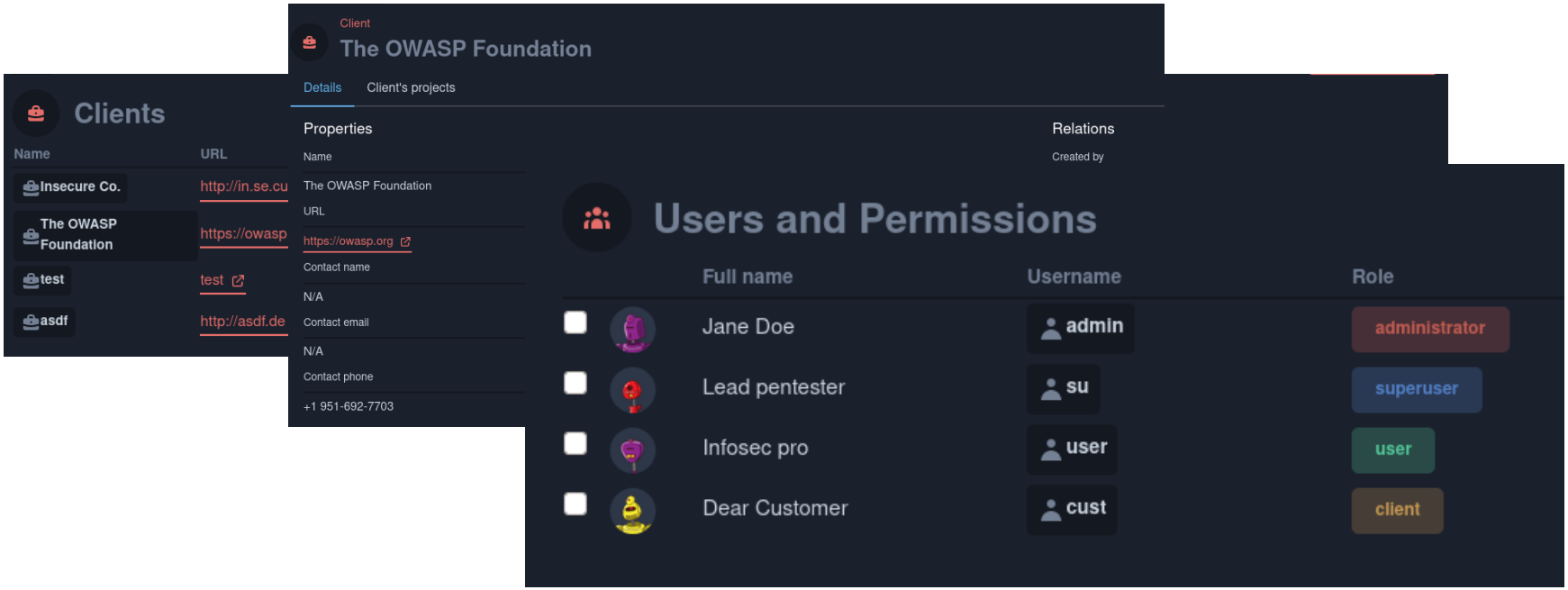
Step 1: Setup client



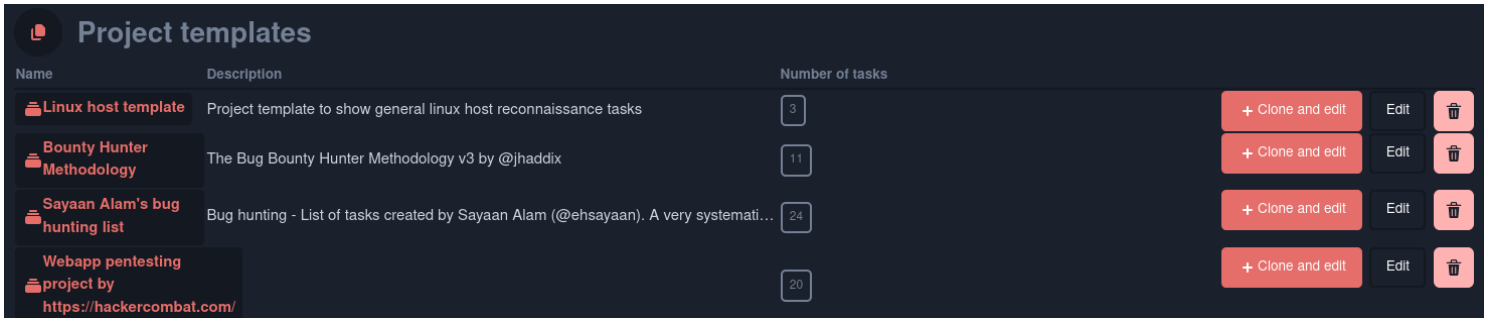
Step 1: Setup client



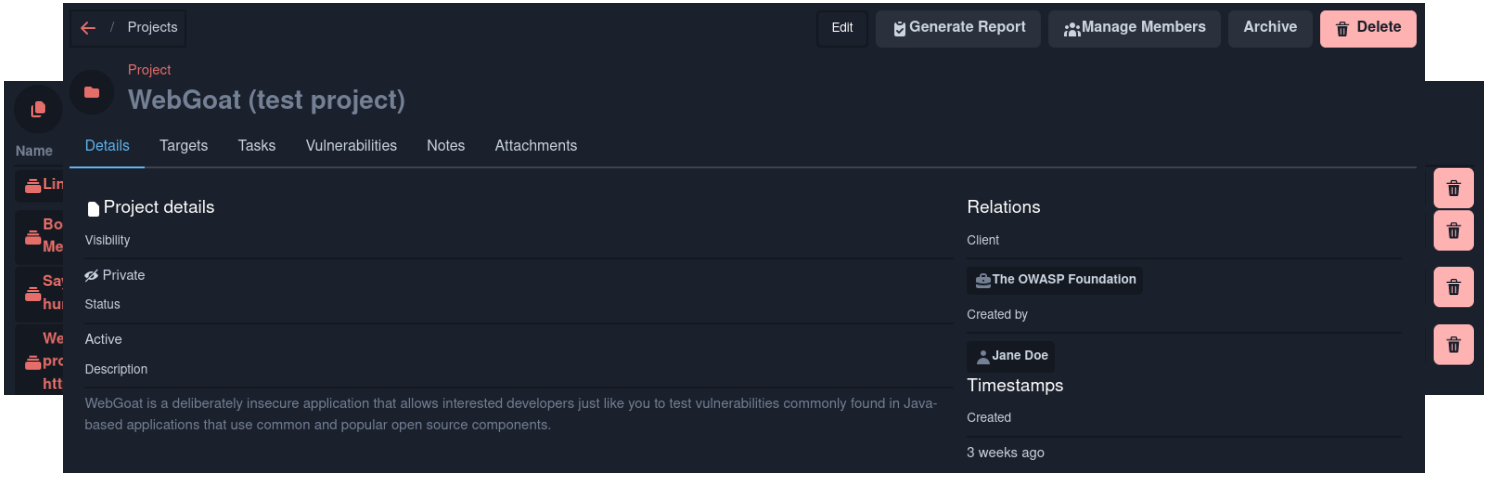
Step 1: Setup client



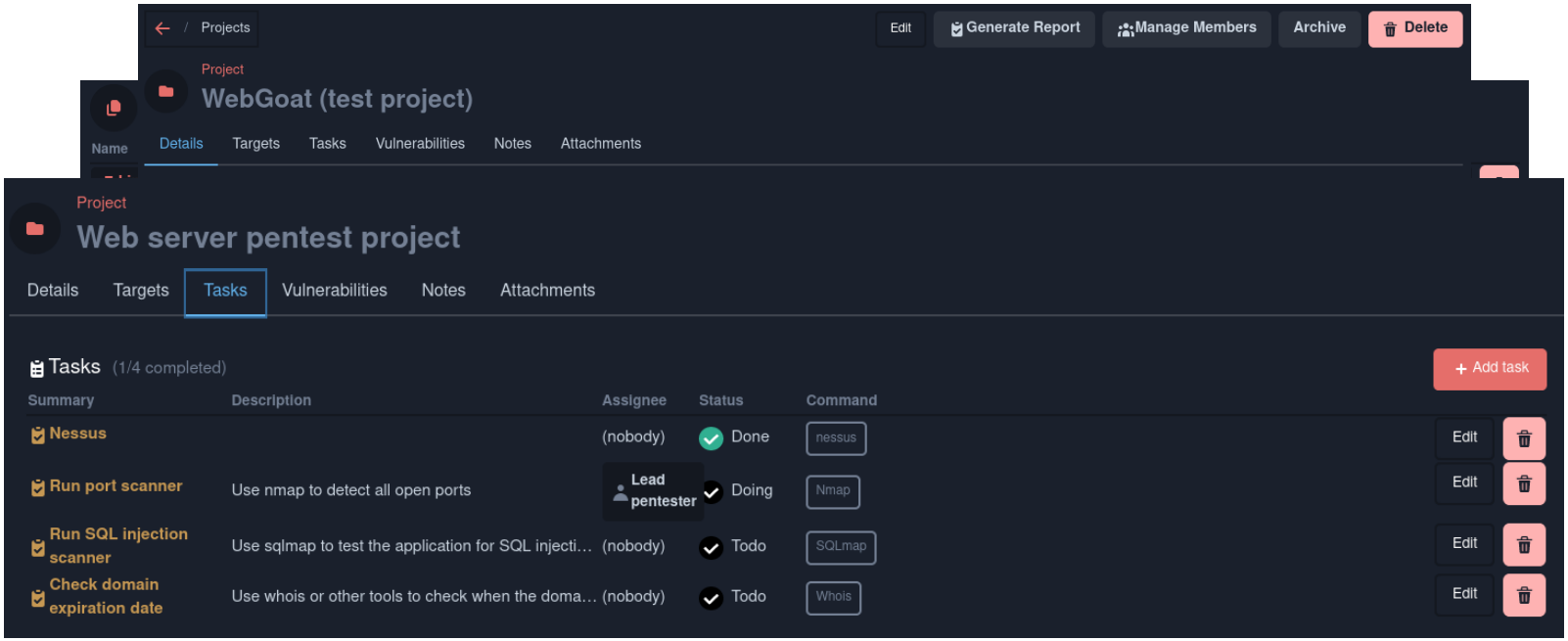
Step 2: Setup project



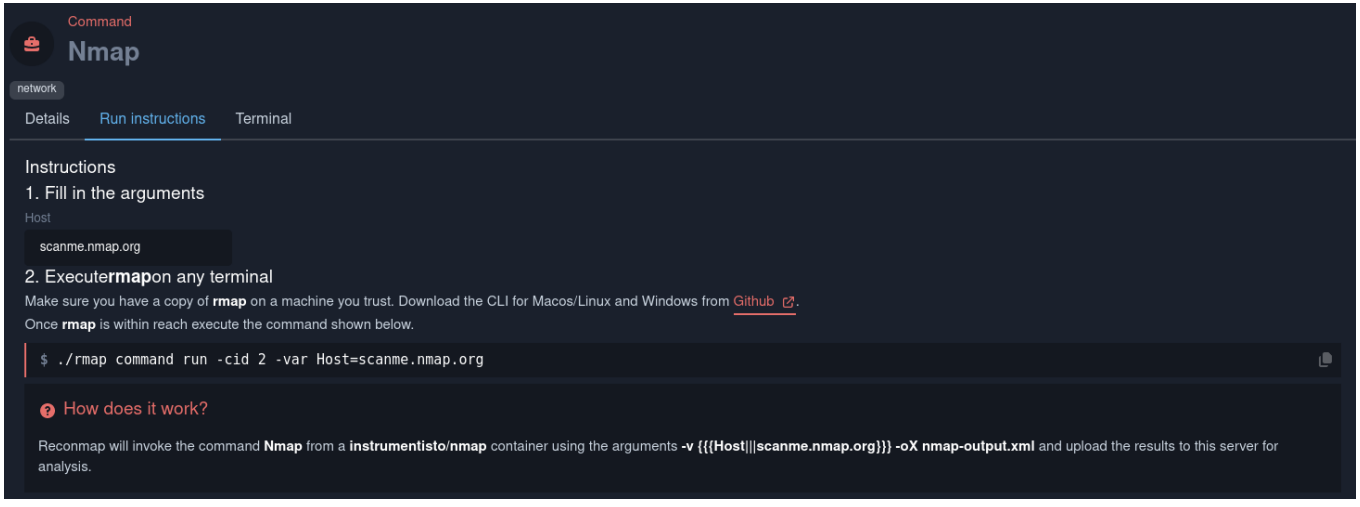
Step 2: Setup project



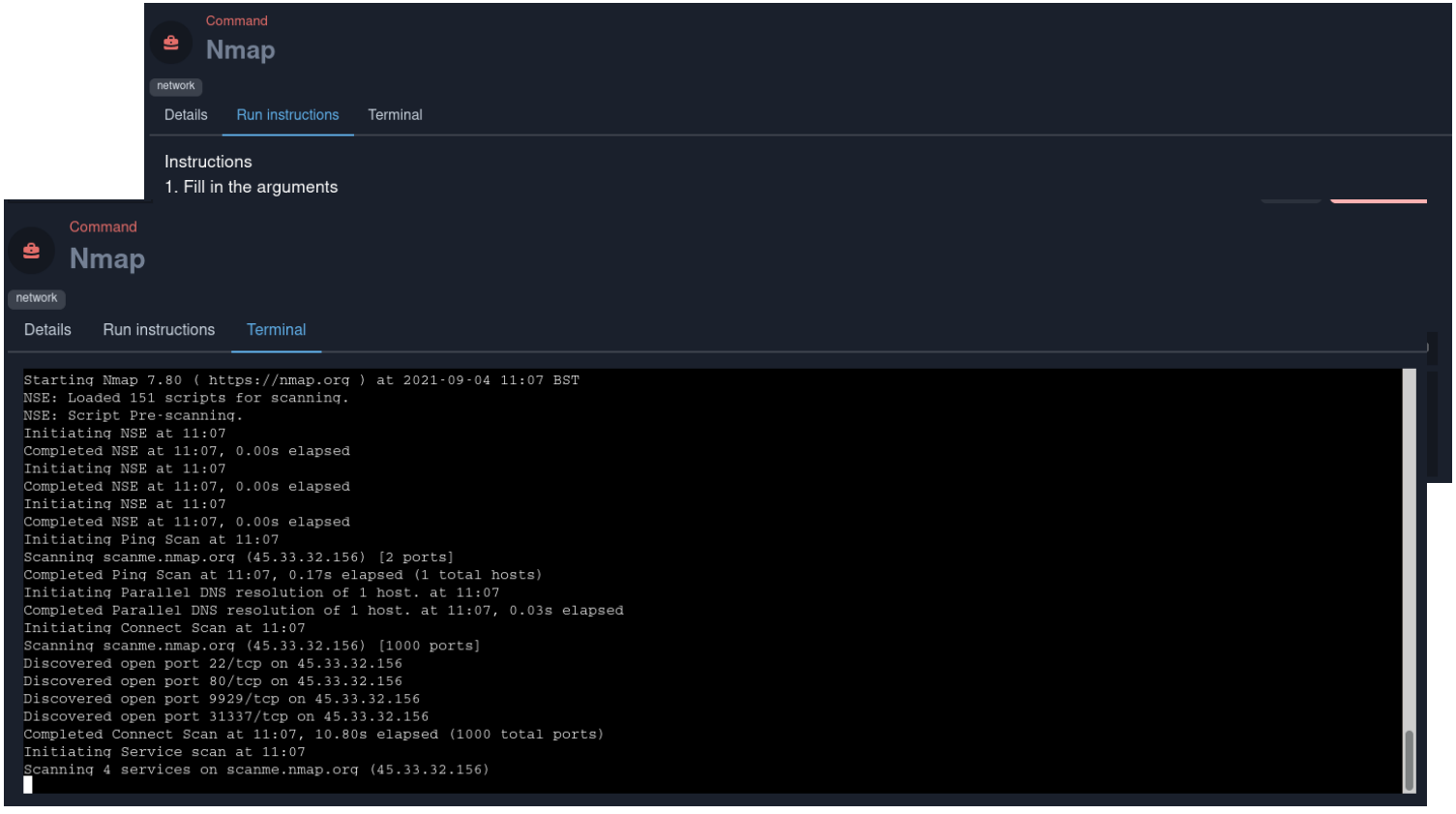
Step 2: Setup project



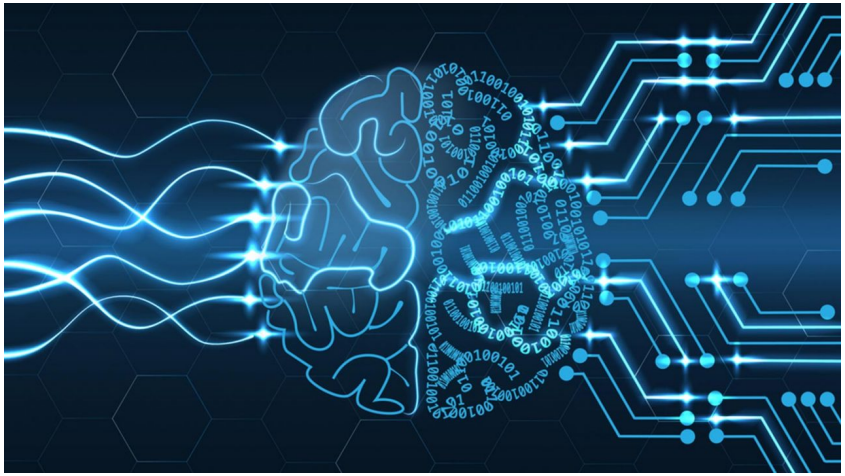
Step 3: Complete tasks and commands



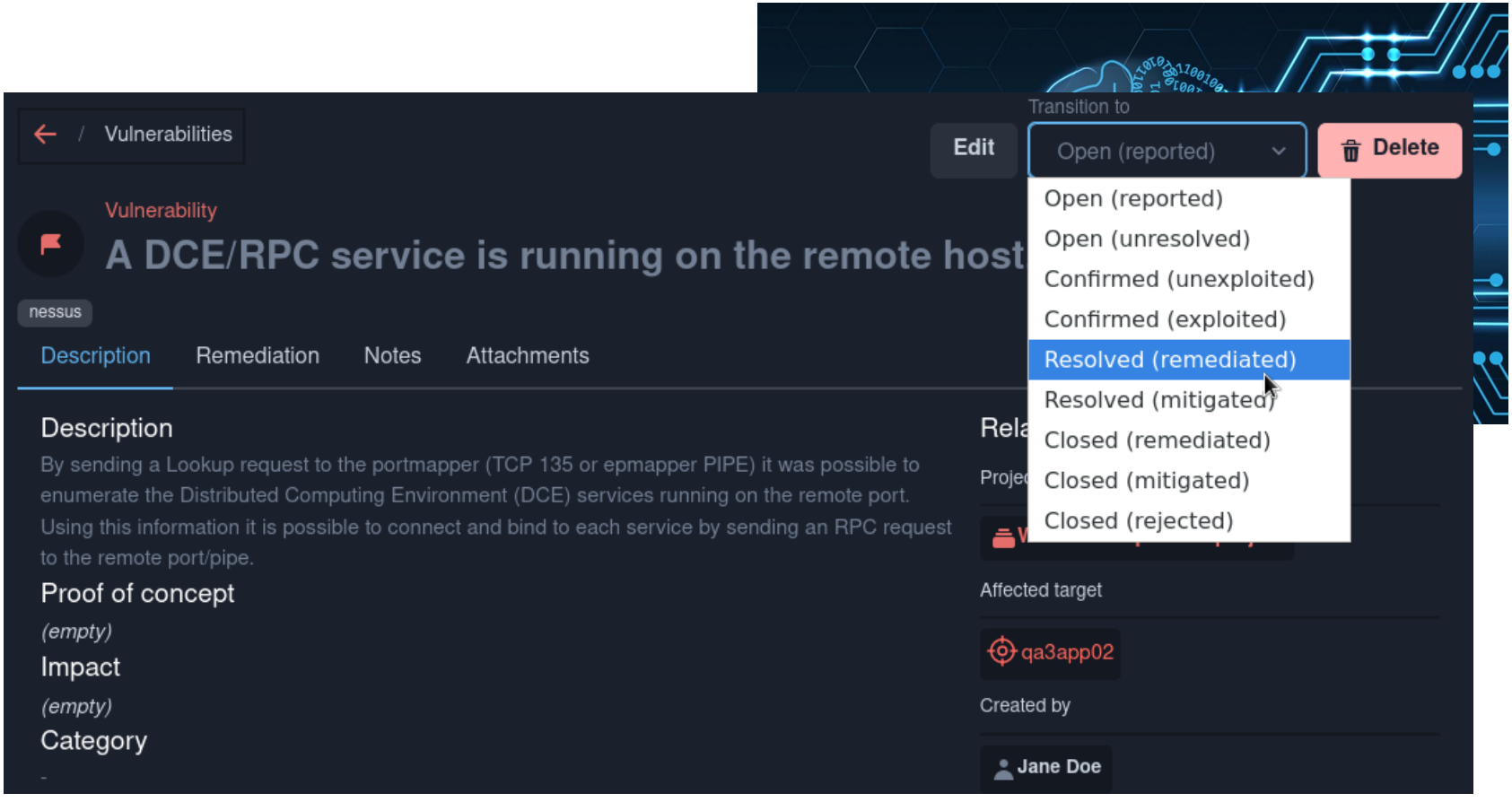
Step 3: Complete tasks and commands



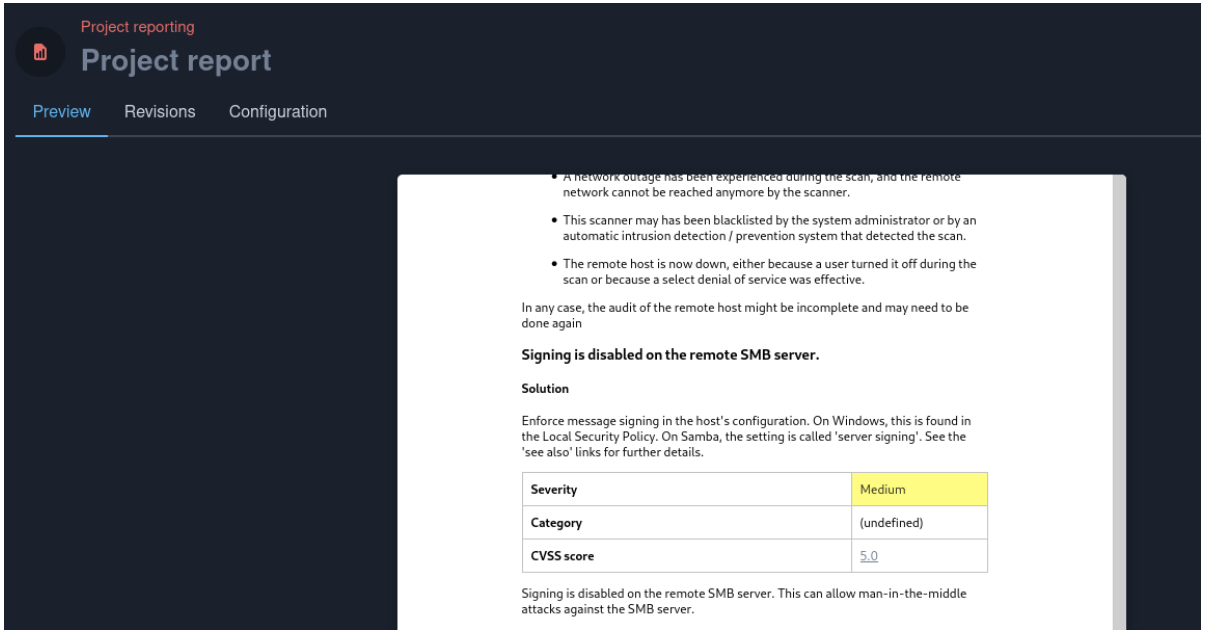
Step 4: Exploit vulnerabilities



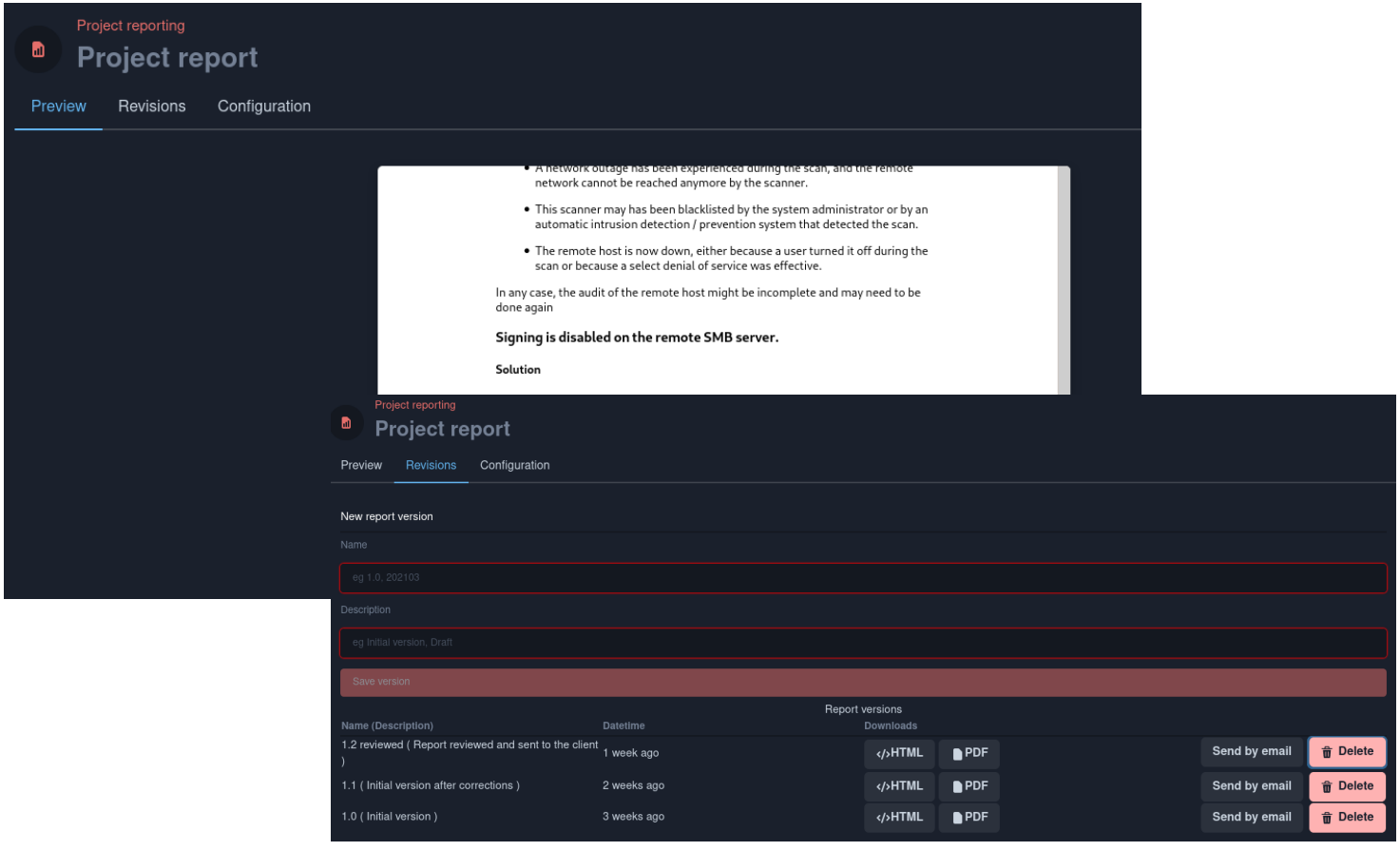
Step 4: Exploit vulnerabilities



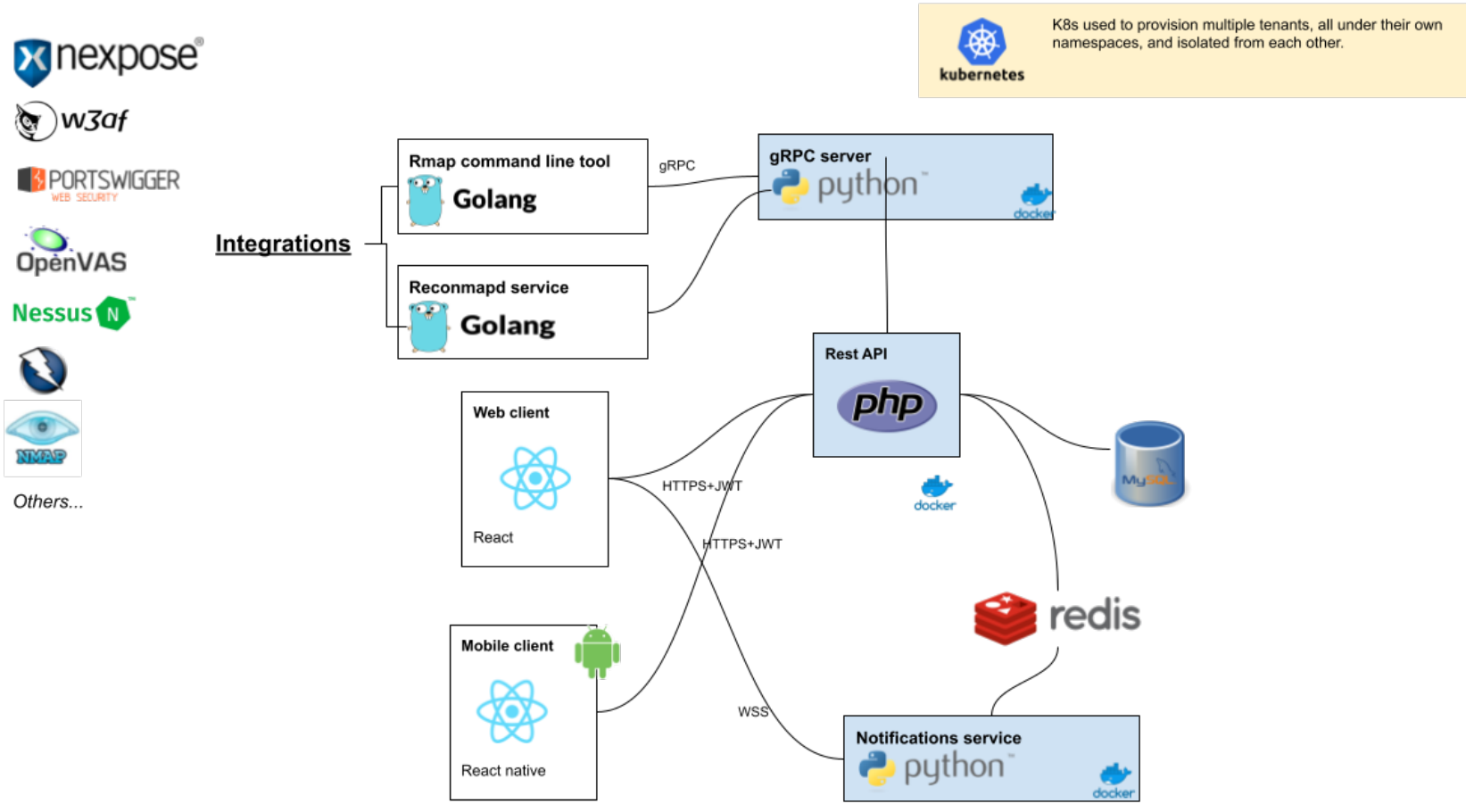
Step 5: Generate pentest report



Step 5: Generate pentest report



Architecture



Coming features

- Complex workflows (reviewers)
- Independent customer's portal
- Secret management
- More integrations

How to get started?

Manual setup

Follow setup instructions

Easy to install, more difficult to maintain
Community support (chat)

SaaS

Affordable hosting

Ready in minutes
Technical support (phone, email, chat)
Always latest version

Staying in touch

- https://github.com/reconmap
- https://twitter.com/reconmap
- https://facebook.com/reconmap
- Gitter chat

PENTESTER ACADEMY

- https://www.pentesteracademy.com
- https://twitter.com/DamianGoh13