Pentesting automation with **Reconmap**

Intro for **Pentester Academy**

Santiago Lizardo

September 4, 2021

About the presenter

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

Reconmap's conception

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.

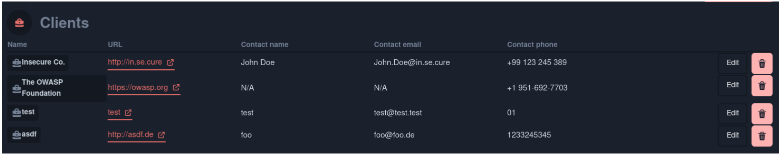
Reconmap's Today - September 2021

- 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
- Can scale to teams and projects of any size.
- User roles, documents, markdown, audit log, integrated search, tagging, data import/export, ...

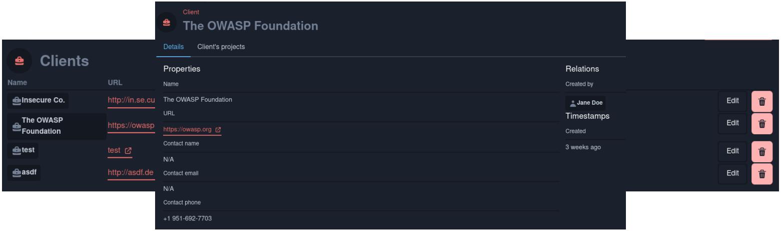
Feature: Client



Clients

Name	URL	Contact name	Contact email	Contact phone		
Insecure Co.	http://in.se.cure	John Doe	John.Doe@in.se.cure	+99 123 245 389	Edit	🗑
The OWASP Foundation	https://owasp.org	N/A	N/A	+1 951-692-7703	Edit	🗑
test	test	test	test@test.test	01	Edit	🗑
asdf	http://asdf.de	foo	foo@foo.de	1233245345	Edit	🗑

Feature: Client



Clients

Name	URL		
Insecure Co.	http://in.se.cu	Edit	🗑
The OWASP Foundation	https://owasp	Edit	🗑
test	test	Edit	🗑
asdf	http://asdf.de	Edit	🗑

Client

The OWASP Foundation

Properties

Name: The OWASP Foundation

URL: https://owasp.org

Contact name: N/A

Contact email: N/A

Contact phone: +1 951-692-7703

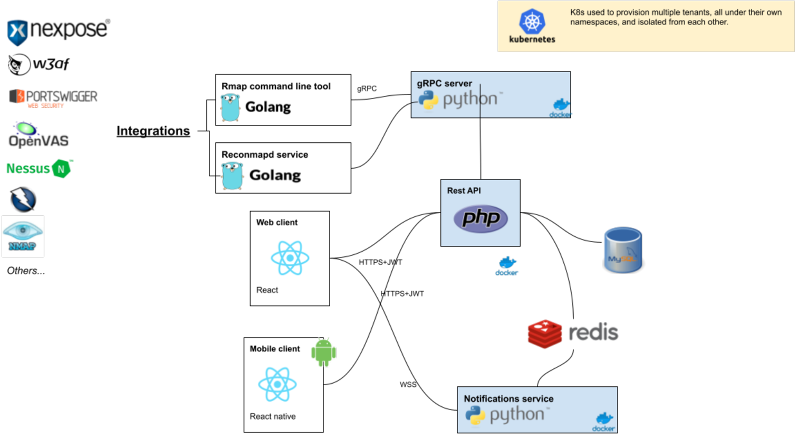
Relations

Created by: Jane Doe

Timestamps

Created: 3 weeks ago

Architecture



Coming features

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

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)
Always latest version

Staying in touch

- Github community
- Twitter updates
- Facebook
- Gitter chat