Smersh

pentest oriented
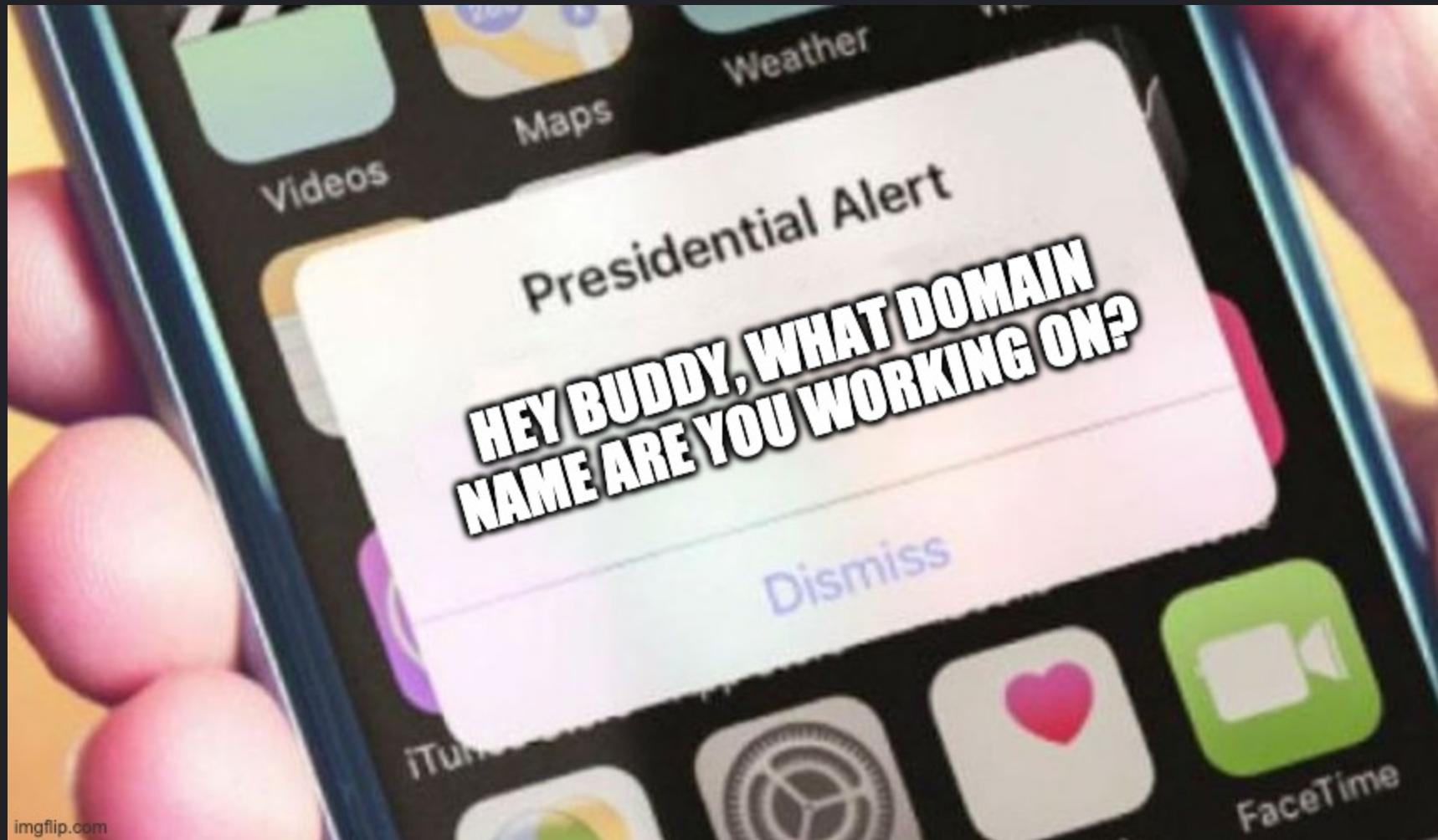collaborative tool!

Houziaux Mike

IT Engineer

- Pentester @Orange Cyberdefense
- CTF player for @Inshallack
- Vice-captain 0xCD
- Open source Contributor (Symfony, rawsec)
- Smersh tool creator
- Engineer graduated from CNAM

@jenaye_fr

Summary

- Why and who created it ?
- Technologies
- Live demo
- Features coming soon

Contributors

Features

- Atomic roles management
- Behat / Cypress tests
- Include codiMD and Bitwarden
- Vulnerabilities Database
- API (protected using JWT)
- Projet management
- Preview state of mission
- Generate report

Smersh - 1.1.2

En

Logout - jenaye

Dashboard

Clients

Hosts

Impacts

Missions

Users

Vulnerabilities

Start date :

End date :

Nmap ⬤ Nessus

FAME MISSION WEB - **Edit**

Scope	Hackers	Client	Credentials	CodiMD	Steps

https://jenaye.fr

ReactJS SQLi - Low

LFI - Critical

Add

https://github.com/Darkweak/Souin

XSS - Medium

Add

Ex : https://poule.op   - Ex : Reactjs (optionnal)   **Add new host manualy**

Import host file   Select File   No file selected...   Submit

Generate report   **Dump data to json file**   Download burp configuration

8

Smersh-cli

command-line client

https://github.com/CMEPW/smersh-cli

`pip install smersh-cli`

LIVE DEMO!

WHAT COULD GO WRONG?

PENTESTER

SMERSH

GHOSTWRITER / DRADIS

11

What's coming soon ?

- Real time notification (Mercure)
- Password to protect mission
- Custom checkliss
- Proxy support

Questions / Ideas ?

"

cmon help us !

- https://twitter.com/Smersh_sec
- https://github.com/CMEPW/

Official discord (Porchetta industries)

- https://discord.gg/JVCV6ykY

"