OWASP

Hassle Free Security Automation with Free and Open Source tools

Anderson Dadario
https://dadario.com.br

Thanks for having me

It’s a pleasure to be here

- Thanks OWASP team

- Thanks Michael Hildago, you rock :)

- I hope you all enjoy this talk. Actually I put quite an effort to it, as usual

Who the f*** is Anderson?

Well, that’s simple

- In summary “I’m a work in progress that mistakenly think that I’m finished”. A big error in Matrix.

- In other words I’m Gauntlet.io founder, an app security orchestration platform, security instructor for CISSP and CSSLP and etc :)

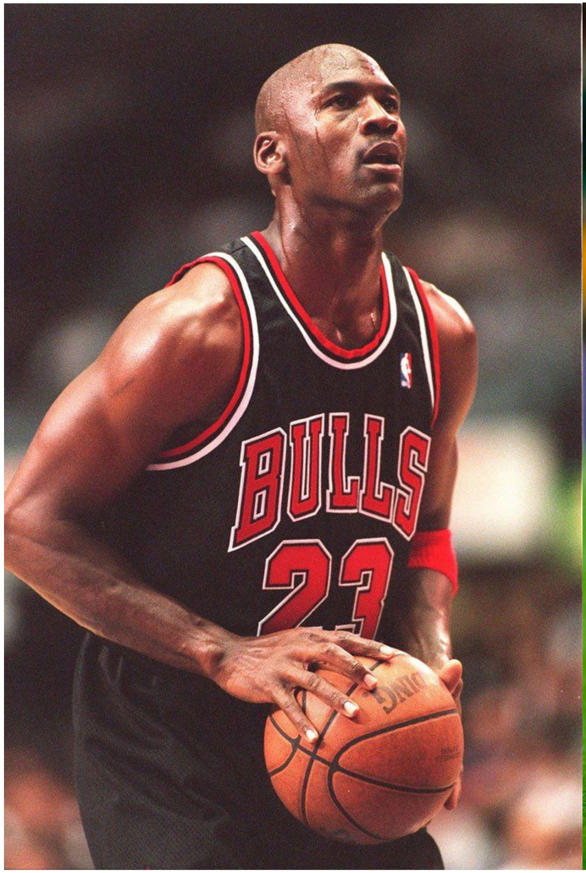
And to keep it short

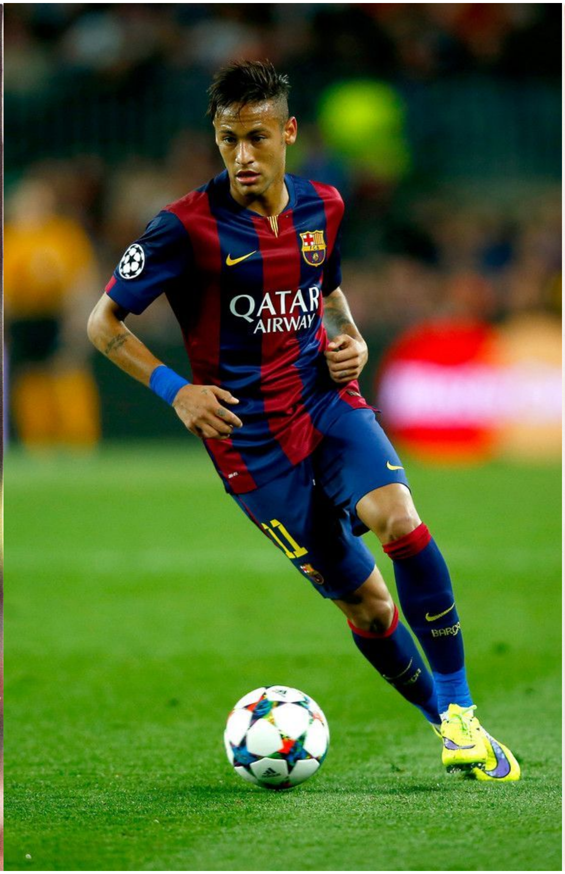
- You can always learn more about me in my personal website that I post 2 times a month and also send an application security newsletter completed biased by me

- That’s it.

Let’s go back in time then …

Do you remember the scorers?





A scorer in appsec …

- May receive a CVE, great for resumé

- May get listed in a ‘hall of fame’ page or receive a bounty $

- Contributes to expose insecurity in applications, servers, protocols and more

But what about the defenders?

Defense is underpraised [1-2]

- The best security architecture won’t appear in the news;

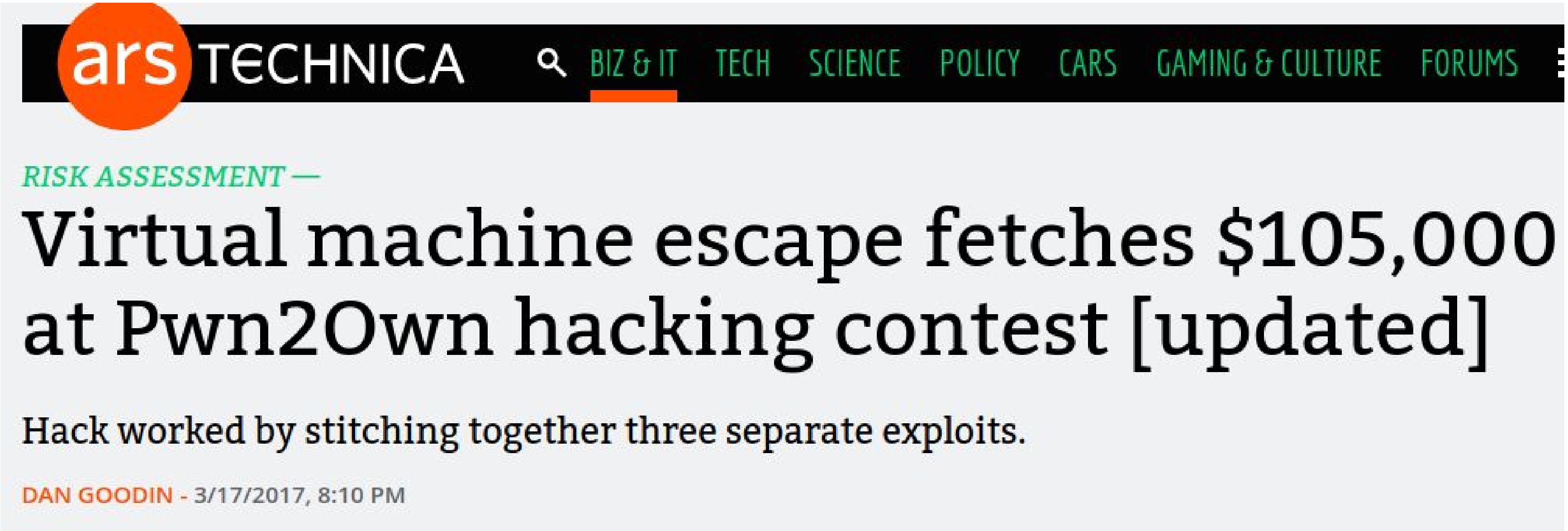
- The security and developers’ names who protected your information are engulfed by a black hole;

Defense is underpraised [2-2]

- Don’t expect to get notorious while working on defense;

- Because defense works from the shadows today. This industry focus too much in attacks.

While amazing 0 days are being pulled off …



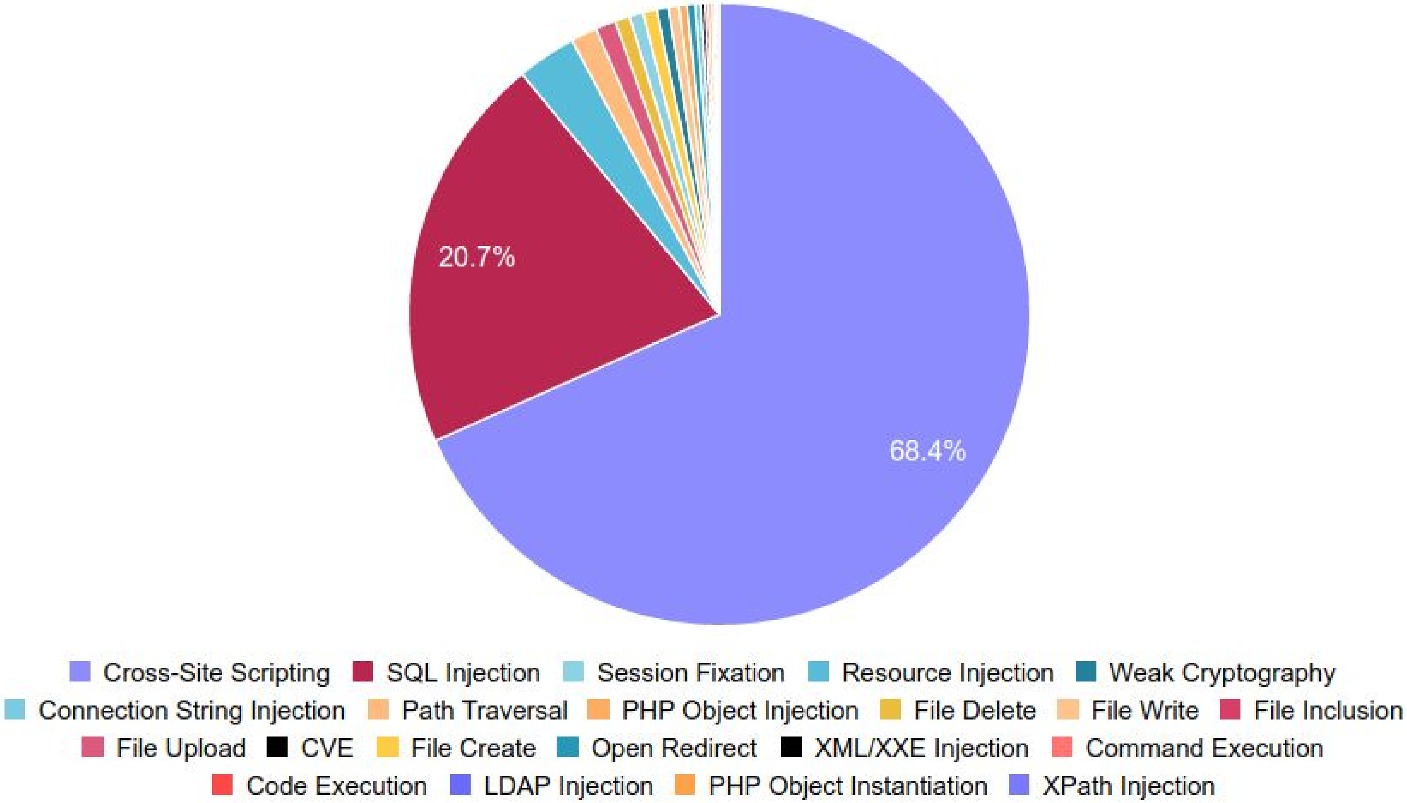
RISK ASSESSMENT —

Virtual machine escape fetches $105,000 at Pwn2Own hacking contest [updated]

Hack worked by stitching together three separate exploits.

DAN GOODIN - 3/17/2017, 8:10 PM

Businesses are still falling short for SQL Injection in WP Plugins.



Source: https://blog.ripstech.com/2016/the-state-of-wordpress-security/

And SQL Injection was first announced in 1998 [1]

[1] Source: https://en.wikipedia.org/wiki/SQL_injection

Something definetely is wrong. What’s your call?

Hope for a calvary of security professionals to come and fix it?

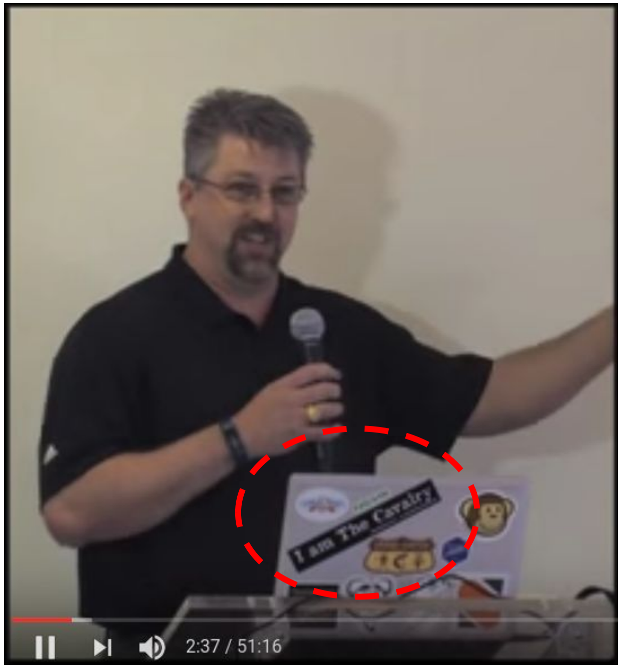
[redacted]

The Cavalry

Sorry. It ain’t coming.

I Am The Cavalry

Source: https://www.iamthecavalry.org/



Who are these guys?

Aaron Weaver and
Matt Tesauro, respectively.

They work on a few OWASP projects, including **OWASP AppSec Pipeline and OWASP Defect Dojo.**

They work on those projects because they are the calvary themselves.

Not only them, but these picture came very handy.

What about this AppSec Pipeline stuff?

AppSec Pipeline

It’s a project that aims to **automatically** embed security into an application delivery pipeline.

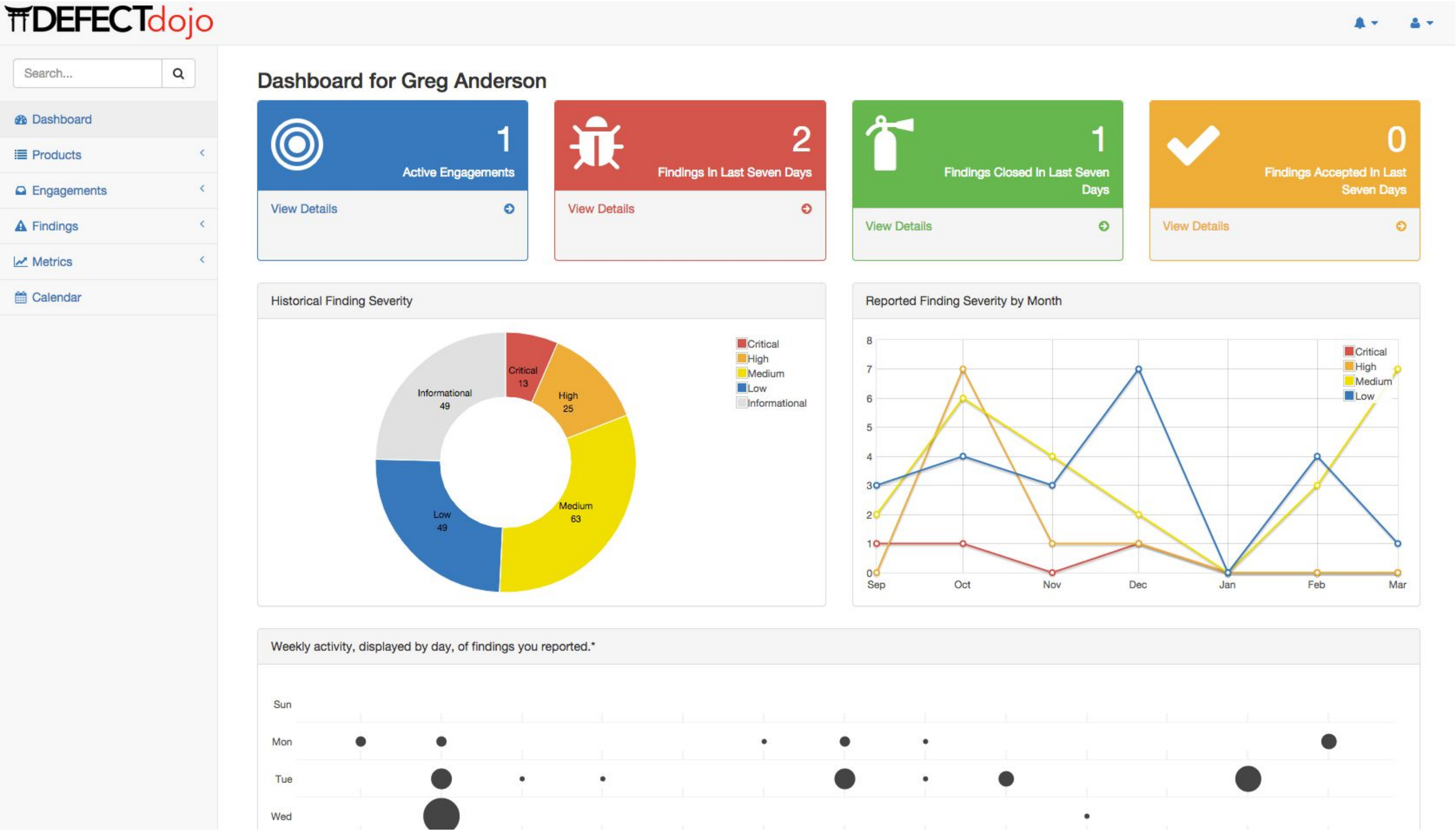
Let’s focus on why it is automated first.

But before let me tell you something.

The truth is that Aaron and Matt are moving their focus to OWASP Defect Dojo …

And they need your help.

OWASP Defect Dojo



DEFECTdojo

Search...

- Dashboard
- Products
- Engagements
- Findings
- Metrics
- Calendar

Dashboard for Greg Anderson

1 Active Engagements — View Details

2 Findings In Last Seven Days — View Details

1 Findings Closed In Last Seven Days — View Details

0 Findings Accepted In Last Seven Days — View Details

Historical Finding Severity

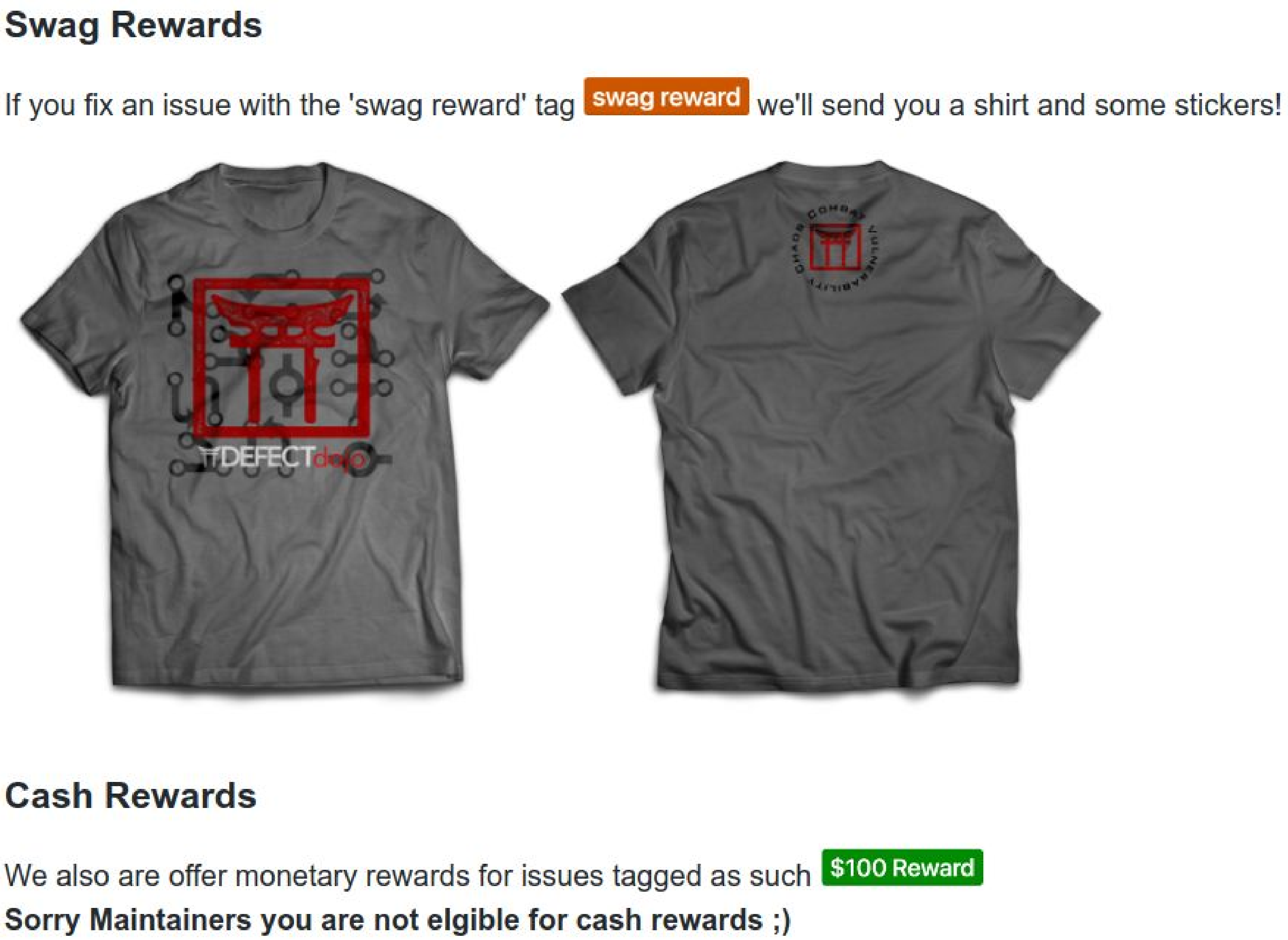
Reported Finding Severity by Month

Weekly activity, displayed by day, of findings you reported.*

“I’d love to contribute to open source, but I only work for money or swag packs.”

Is that even possible?

Of course, it is po$$ible!



Swag Rewards

If you fix an issue with the 'swag reward' tag swag reward we'll send you a shirt and some stickers!

Cash Rewards

We also are offer monetary rewards for issues tagged as such $100 Reward
Sorry Maintainers you are not elgible for cash rewards ;)

Let’s back to the point.

Why automation on a appsec pipeline matters?

People have loss aversion [1-3]

In economics and decision theory, **loss aversion** refers to people's tendency to prefer avoiding losses to acquiring equivalent gains: it's better to not lose $5 than to find $5.

Source: https://en.wikipedia.org/wiki/Loss_aversion

People have loss aversion [2-3]

“(...) If you give people a choice between a $500 sure gain and a coin-flip chance of a $1,000 gain, about 75 percent will pick the sure gain.

But give people a choice between a $500 sure loss and a coin-flip chance of a $1,000 loss, about 75 percent will pick the coin flip. (..)”

Source: https://www.schneier.com/essays/archives/2008/07/how_the_human_brain.html

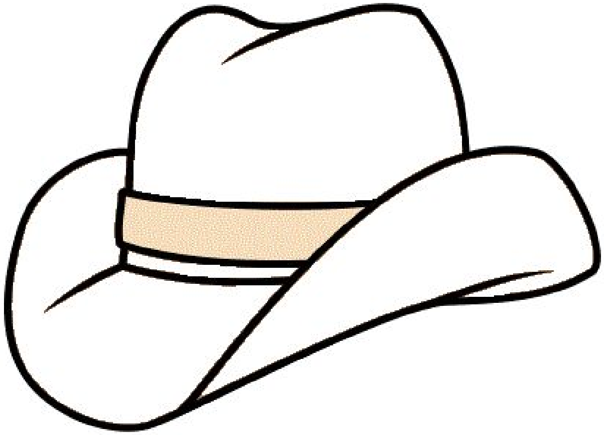
People have loss aversion [3-3]

- Investment in security is a sure loss that may or may not yield returns. The risk may not materialize. That’s the point.

- This strategy works great for testing acceptance (business idea) and discovering problems (it’s a problem when it’s a problem), but it’s not that great for security

That’s why defense is hard!

- Expect that a company’s top priority isn’t to secure information, but to make money;
- Expect the security budget to be a small cut of the overall IT budget;
- Expect 1 security engineer for 10 developers;
- Expect not ever being able to secure information properly without automation.



Let’s put the security defensor’s hat

Principles

- Security personnel must be synonym of intelligence
- Everything that doesn’t require a human brain should be automated
- Always apply the **principle of leverage**

Principle of Leverage [1-2]

“In principle, a lever allows you to use less force to lift or move objects. We may not know it, but this theory is applied in a lot of the everyday objects we use such as scissors, bottle openers and even doors.“

Source: https://fitzvillafuerte.com/the-principle-of-leverage-and-how-to-use-it-in-our-life.html

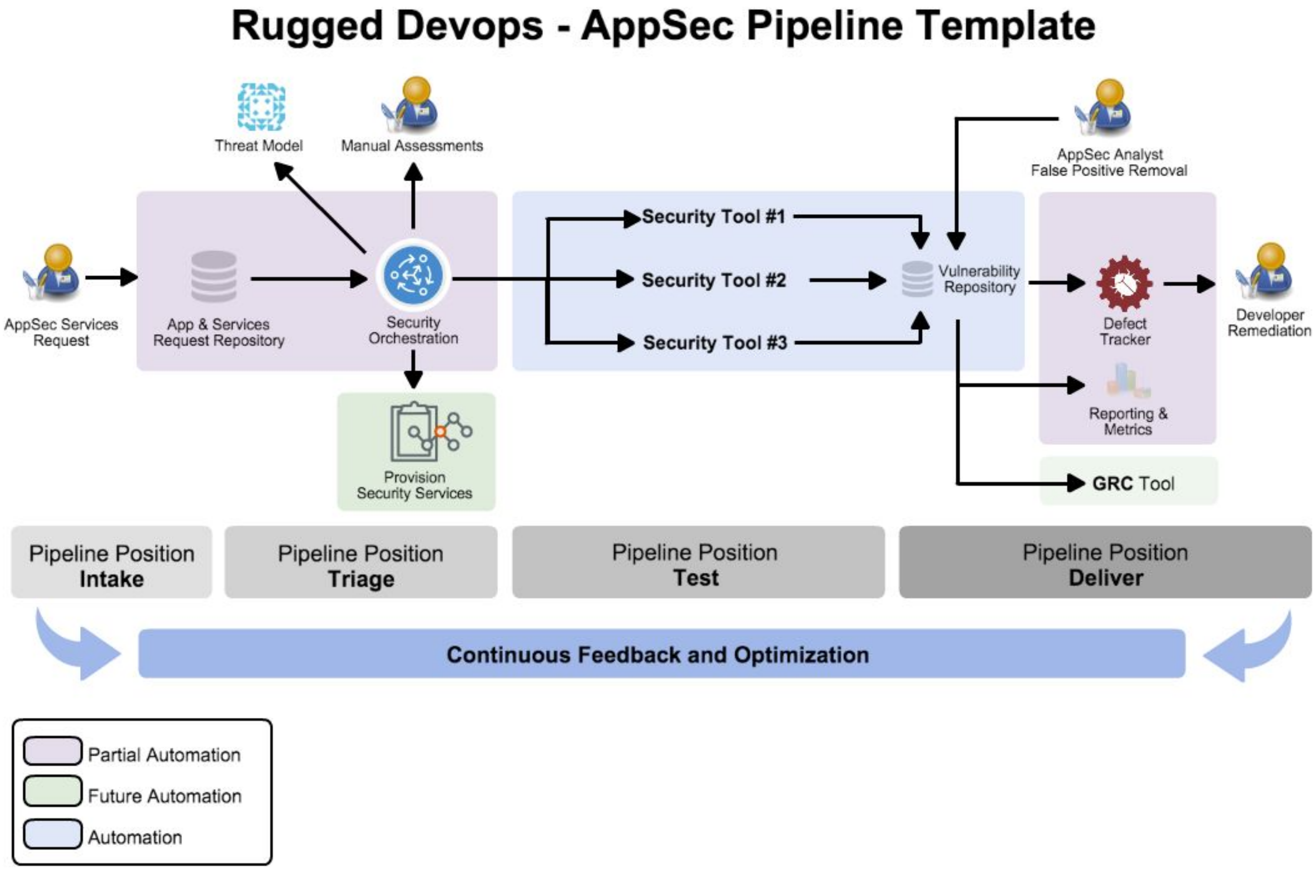
Principle of Leverage [2-2]

In security that would be to make the most security impact while using as fewer hours as possible. Examples include:

- Security training for developers;
- Secure Architecture Design;
- Security tests automation.

Let’s come back to OWASP AppSec Pipeline

OWASP AppSec Pipeline



Aaron Weaver, CC ShareAlike 3.0

The Great

- Great
    - AppSec is following App Delivery
    - It’s what should be done
    - It combines multiple tools
    - It’s end-to-end security

The Good

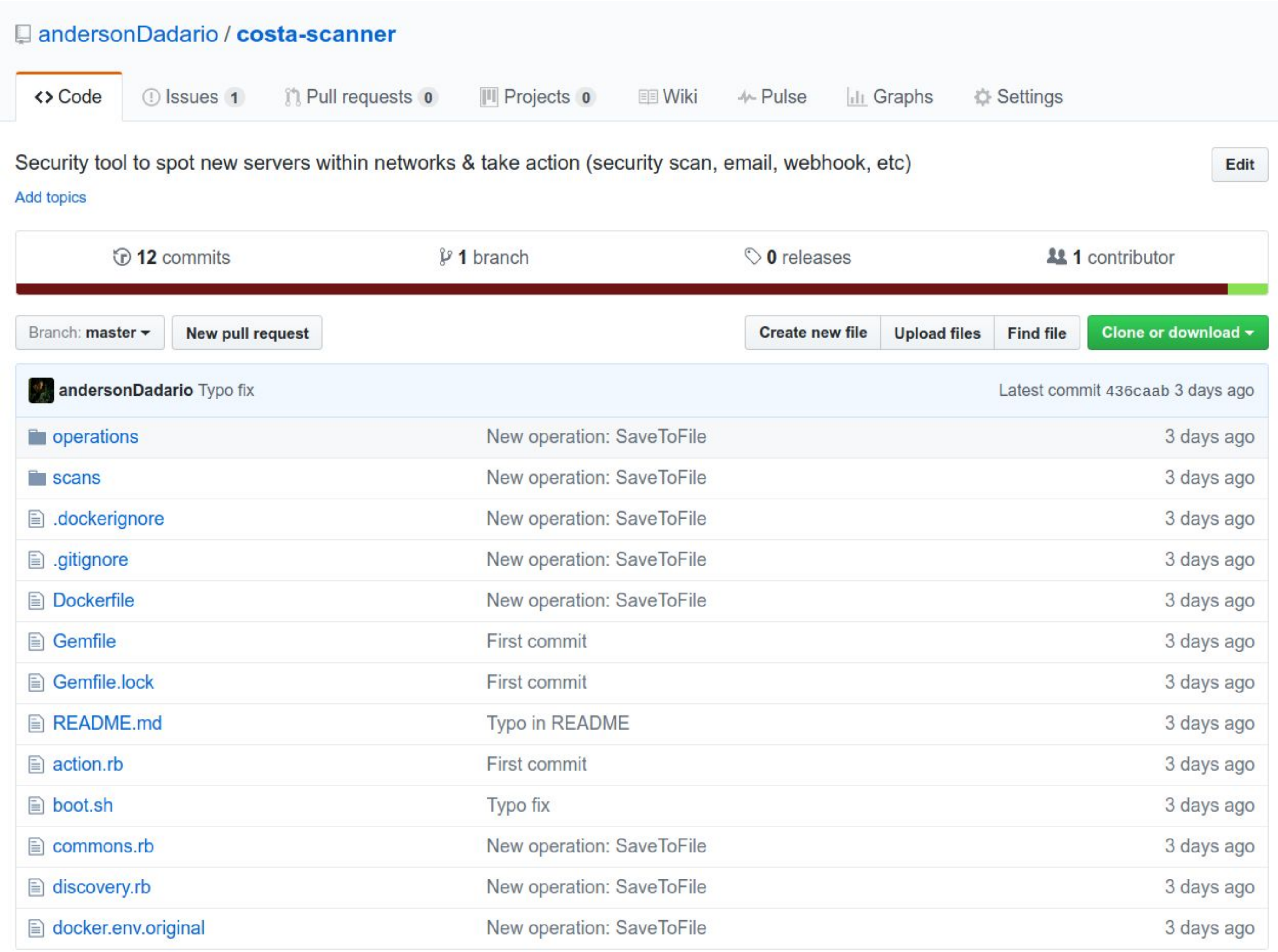
- Good
    - It’s using open open source technologies
    - There are open source technologies to each step

The Bad

- Bad (it applies for all appsec pipelines)
  - Not all open source technologies are maintained, thus it relies in a few commercial solutions
  - Require a significant amount of effort to implement
  - It’s hard to customize to each company

What if you could implement some appsec automation from Day 0?

Introducing CostaScanner



andersonDadario / **costa-scanner**

Security tool to spot new servers within networks & take action (security scan, email, webhook, etc)

12 commits · **1** branch · **0** releases · **1** contributor

andersonDadario Typo fix — Latest commit 436caab 3 days ago

operations	New operation: SaveToFile	3 days ago
scans	New operation: SaveToFile	3 days ago
.dockerignore	New operation: SaveToFile	3 days ago
.gitignore	New operation: SaveToFile	3 days ago
Dockerfile	New operation: SaveToFile	3 days ago
Gemfile	First commit	3 days ago
Gemfile.lock	First commit	3 days ago
README.md	Typo in README	3 days ago
action.rb	First commit	3 days ago
boot.sh	Typo fix	3 days ago
commons.rb	New operation: SaveToFile	3 days ago
discovery.rb	New operation: SaveToFile	3 days ago
docker.env.original	New operation: SaveToFile	3 days ago

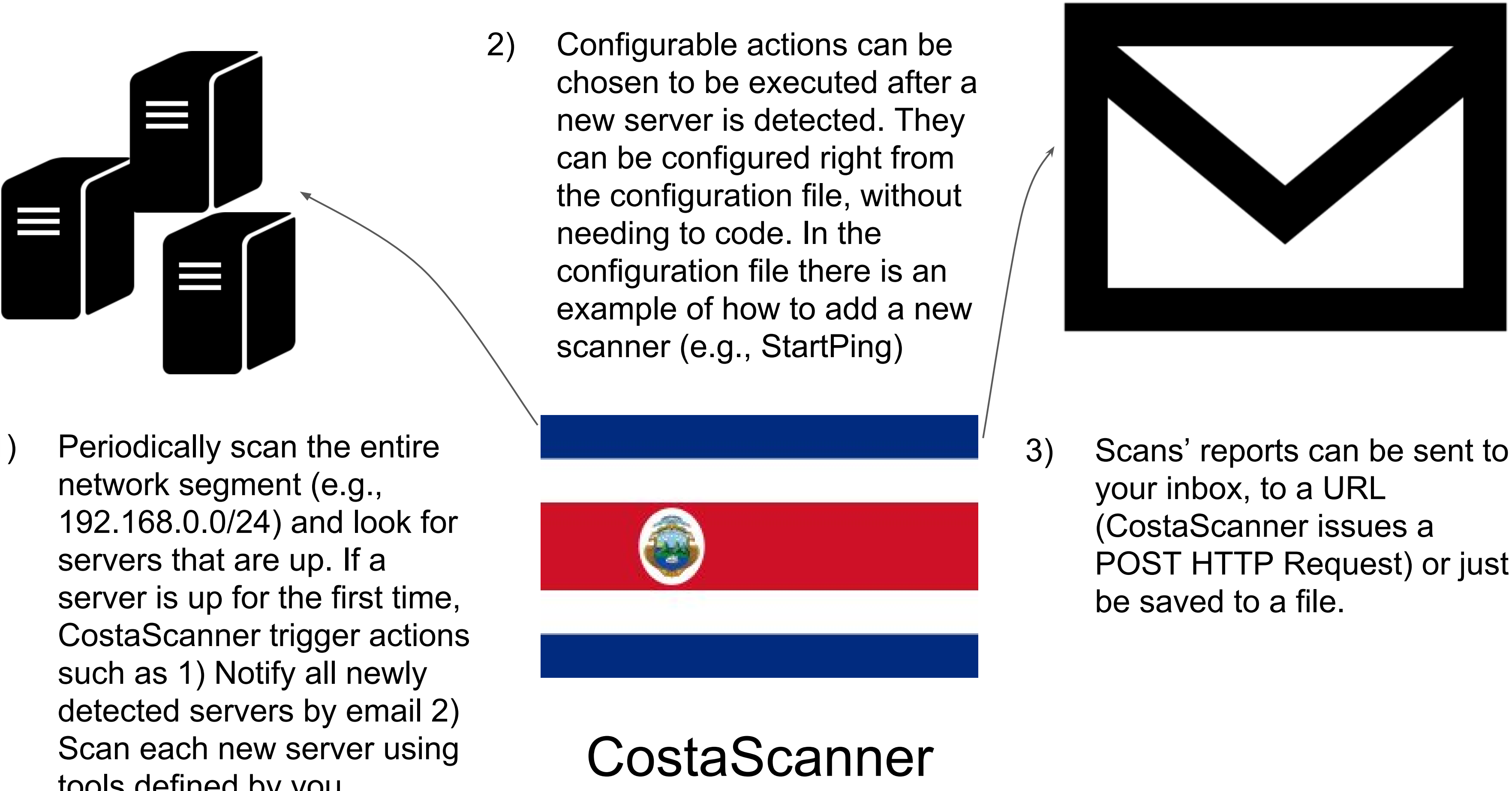
CostaScanner activities

1) Performs a periodic network asset discovery and when detect a new server it

2) Run one or many scans with any installed tool (e.g., nmap) and

3) Sends a report to you by email, webhook or just save the output to a file.

How it works



1) Periodically scan the entire network segment (e.g., 192.168.0.0/24) and look for servers that are up. If a server is up for the first time, CostaScanner trigger actions such as 1) Notify all newly detected servers by email 2) Scan each new server using tools defined by you. CostaScanner stores asset data in the “database.txt” file

2) Configurable actions can be chosen to be executed after a new server is detected. They can be configured right from the configuration file, without needing to code. In the configuration file there is an example of how to add a new scanner (e.g., StartPing)

3) Scans’ reports can be sent to your inbox, to a URL (CostaScanner issues a POST HTTP Request) or just be saved to a file.

CostaScanner

Questions & Answers

Q: Is it a tool to replace OWASP AppSec Pipeline?
A: No. At least no plans for now. It's a tool meant to be run since your 1st day in a company without trouble to help you automate security tests.

Q: What is your vision for it?
A: It has a lot of potential to become a full fledged no-brainer appsec pipeline tool, but I'll only working on it myself when people use it, so please do it.

Q: What else can be done with CostaScanner?
A: Implement a discovery for repositories, allow scanners that are API based, create a web interface to manage discovered assets, create policies to work on issues. There are so many cool things, but they require time and effort. I'd love to see your contribution :)

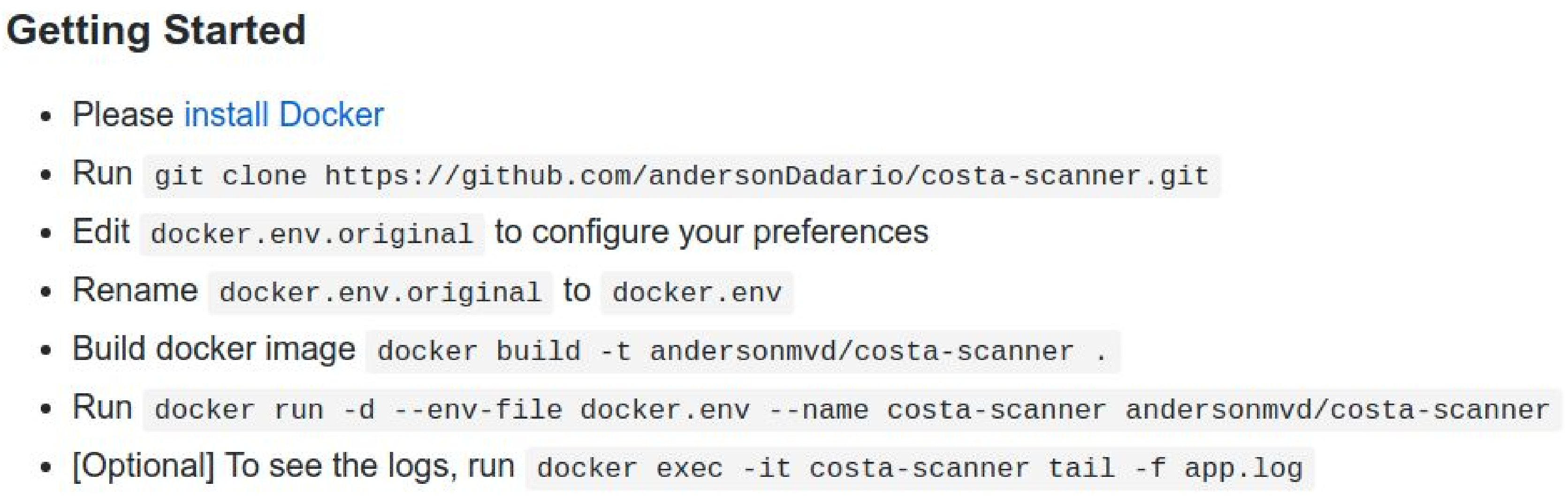
Go beyond

Integrate CostaScanner with some amazing and active maintained OWASP tools:

OWASP Glue: chain multiple security static and dynamic tools;

OWASP OWTF: run multiple dast tools at once focused on OWASP testing guide.

Running CostaScanner



Getting Started

- Please install Docker
- Run `git clone https://github.com/andersonDadario/costa-scanner.git`
- Edit `docker.env.original` to configure your preferences
- Rename `docker.env.original` to `docker.env`
- Build docker image `docker build -t andersonmvd/costa-scanner .`
- Run `docker run -d --env-file docker.env --name costa-scanner andersonmvd/costa-scanner`
- [Optional] To see the logs, run `docker exec -it costa-scanner tail -f app.log`

Configuration Example [1-4]

```
# Targets
# Note: [1] targets must be separated by "," without spaces
#       [2] if you have an individual IP address, just fill it
#       by appending "/32" as the following: "192.168.1.10/32"
TARGETS=192.168.0.0/24
```

Configuration Example [2-4]

```
# Operations after a server has been discovered
# Custom Operations can be set in this configuration file
# Let's suppose that we want to run the "ping" scanner
# First of all, it must be installed (check Dockerfile)
# After that, you can set a new operation just like below
#
# [
#   {
#    "name":"StartPing",
#    "operation":"StartScanner",
#    "data":
#      {
#         "scanner":"ping",
#         "params":["-c","1","%server%"]
#      }
#    }
# ]
#
# It will execute: $ ping -c 1 <server>
#
# After that, make sure to set it as an operation to be executed
#
CUSTOM_OPERATIONS=[{"name":"StartPing","operation":"StartScanner","data":{"scanner":"ping","params":["-c","1","%server%"]}}]
```

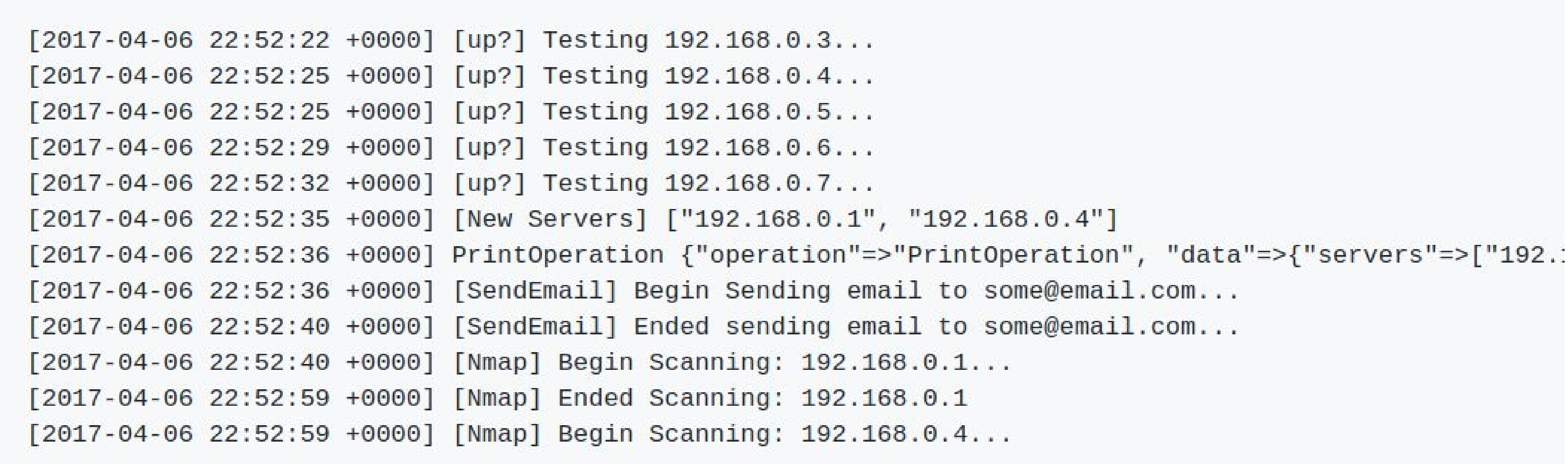
Configuration Example [3-4]

```
# Default Available: Print, SendEmail, StartNmap, SendWebhook, RegisterOnGauntlet
# Note: operations must be separated by "," without spaces
OPERATIONS=Print,SendEmail,StartNmap,StartPing


# Redis
# In case you want to use an external Redis
# Change the URL below
REDIS_URL=redis://localhost:6379/infosec


# WEBHOOK
# URL to send a POST
# Containing all newly discovered servers
WEBHOOK_URL=https://mydomain.com/some-uri
```

Configuration Example [4-4]

```
# SCANNER
SCANNER_SEND_EMAIL=True
SCANNER_SEND_WEBHOOK=False
SCANNER_SAVE_TO_FILE=True


# SMTP
# Auth types: none, plain, login, cram_md5
# Note: SMTP_TO can be multiple emails
#       but they need to be separated by ","
#       without spaces
SMTP_TO=me@gmail.com
SMTP_FROM=noreply@mydomain.com
SMTP_SUBJECT=New servers were found!
SMTP_HOST=smtphost.com
SMTP_PORT=587
SMTP_ENABLE_STARTTLS_AUTO=True
SMTP_USER=aaa
SMTP_PASS=bbb
SMTP_DOMAIN=mydomain.com
SMTP_AUTH=plain
```

Example of output



```
[2017-04-06 22:52:22 +0000] [up?] Testing 192.168.0.3...
[2017-04-06 22:52:25 +0000] [up?] Testing 192.168.0.4...
[2017-04-06 22:52:25 +0000] [up?] Testing 192.168.0.5...
[2017-04-06 22:52:29 +0000] [up?] Testing 192.168.0.6...
[2017-04-06 22:52:32 +0000] [up?] Testing 192.168.0.7...
[2017-04-06 22:52:35 +0000] [New Servers] ["192.168.0.1", "192.168.0.4"]
[2017-04-06 22:52:36 +0000] PrintOperation {"operation"=>"PrintOperation", "data"=>{"servers"=>["192.1
[2017-04-06 22:52:36 +0000] [SendEmail] Begin Sending email to some@email.com...
[2017-04-06 22:52:40 +0000] [SendEmail] Ended sending email to some@email.com...
[2017-04-06 22:52:40 +0000] [Nmap] Begin Scanning: 192.168.0.1...
[2017-04-06 22:52:59 +0000] [Nmap] Ended Scanning: 192.168.0.1
[2017-04-06 22:52:59 +0000] [Nmap] Begin Scanning: 192.168.0.4...
```

But don’t you know Docker?
That’s a big problem.

Docker is a big part of automation

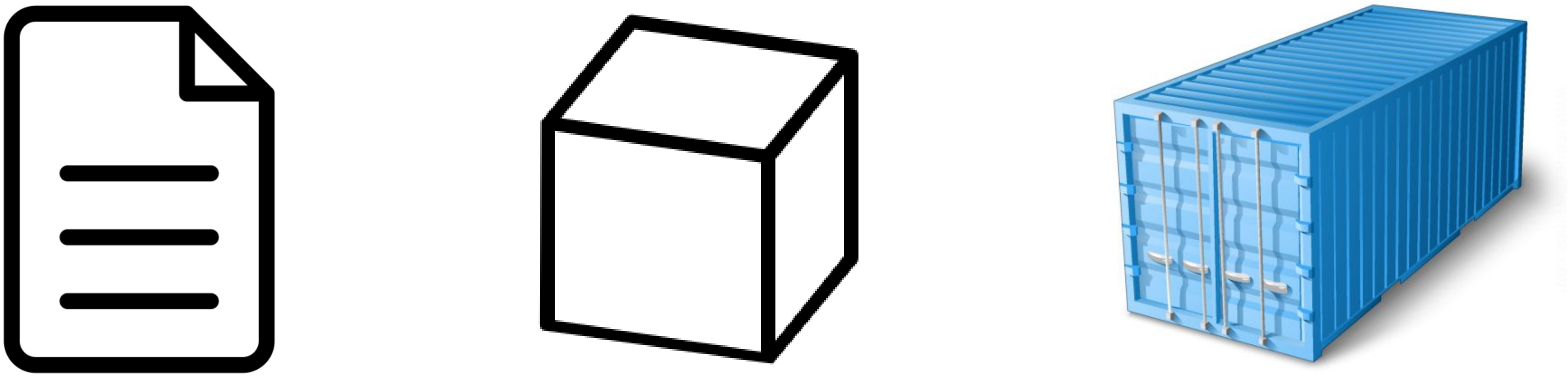
- It’s not only for developers who drunk the hype tech beer and want to ship applications in another way to do the same thing

- It’s a tool for any IT professional to save time by running self-contained tools with ease

You should know how to automate things.

Otherwise you’re failling to apply the Leverage Principle.

How Docker Works



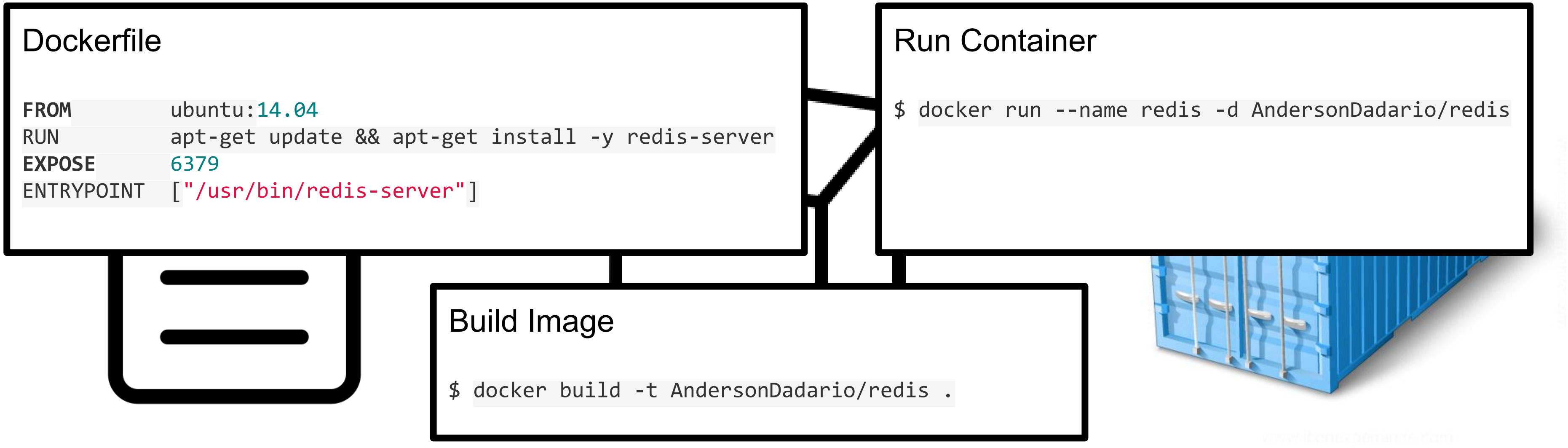
Dockerfile

Docker Image

Docker Containers

I’ve made a free docker security course [in pt-br and en-us]:
https://dadario.com.br/courses/

How Docker Works



Dockerfile

```
FROM        ubuntu:14.04
RUN         apt-get update && apt-get install -y redis-server
EXPOSE      6379
ENTRYPOINT  ["/usr/bin/redis-server"]
```

Run Container

```
$ docker run --name redis -d AndersonDadario/redis
```

Build Image

```
$ docker build -t AndersonDadario/redis .
```

Dockerfile

Docker Image

Docker Containers

I’ve made a free docker security course [in pt-br and en-us]:
https://dadario.com.br/courses/

Great, so automation is about docker, right? Wrong! There are more to it

Main automation tools

- Docker
  - Rationale: easily ship and run apps
- Cloud Computing
  - Rationale: should be easy to deploy and maintain servers, databases and other services

- Programming
  - Rationale: you need to perform customizations or create specific programs all the time

But you don’t know how to program? Can’t create a web app? Holy s...

Look, the current scenario is ugly

- Open Source solutions are few, complex and hard to maintain. Even @w3af said that you should contribute to an existing scanner instead of rolling out your own;

- Commercial products aren’t a one-size-fits-all solution either.

Know how to program is a must

- The community needs more information security guys who know how to code to build or maintain more open source solutions;

- Your environment will require custom tweaks all the time. Be ready to do them. Your users are awaiting.

But you came from a network security background?

Hum, here’s the summary

- Network security tend to rely heavily on vendor products. Your resumé is as good as your concepts, certifications and products that you’ve worked with.

- But it doesn’t work for application security. Applications are extremely customized, so is their security.

Please, don’t skip learning how to code

Don’t understimate it

- You need to know how to “talk dev”, thus learning to code is mandatory;

- It’s mandatory for automation as well. At least for fixing bugs or implementing new features.

Remember why automation

- It saves time

- It enforces security policies

- It protect apps and your organization

Remember that it ain’t easy

- The environment is not mature
  - e.g., few security answers / guides on AES GCM implementation

- You need to know how to code to contribute

- The cavalry is NOT coming

And don’t expect a reward

- It’s ingrateful to secure things
- But that’s our duty
- So let’s become the cavalry and build a security that we’d be proud of

Muchas Gracias!

Anderson Dadario
@andersonmvd
https://dadario.com.br