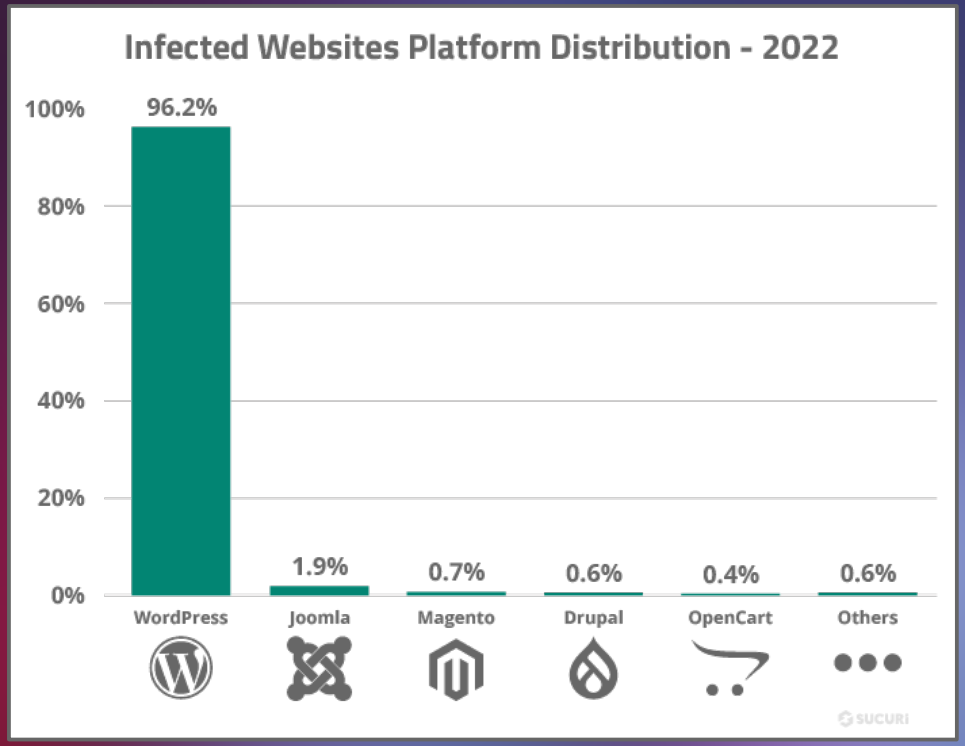
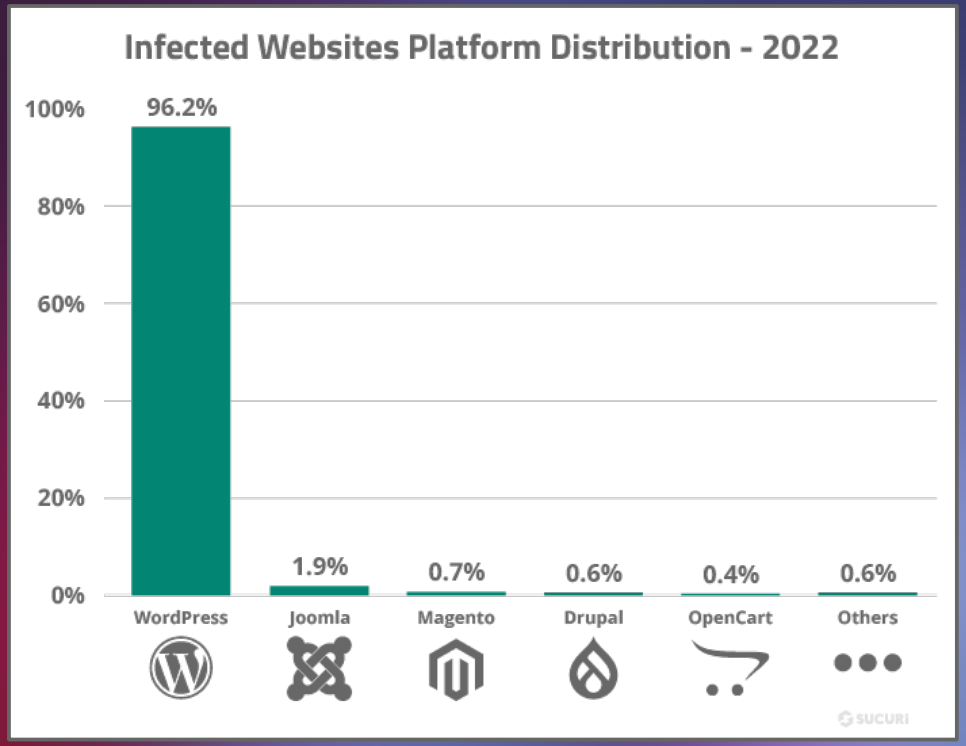
Repenser la sécurité des plateformes web

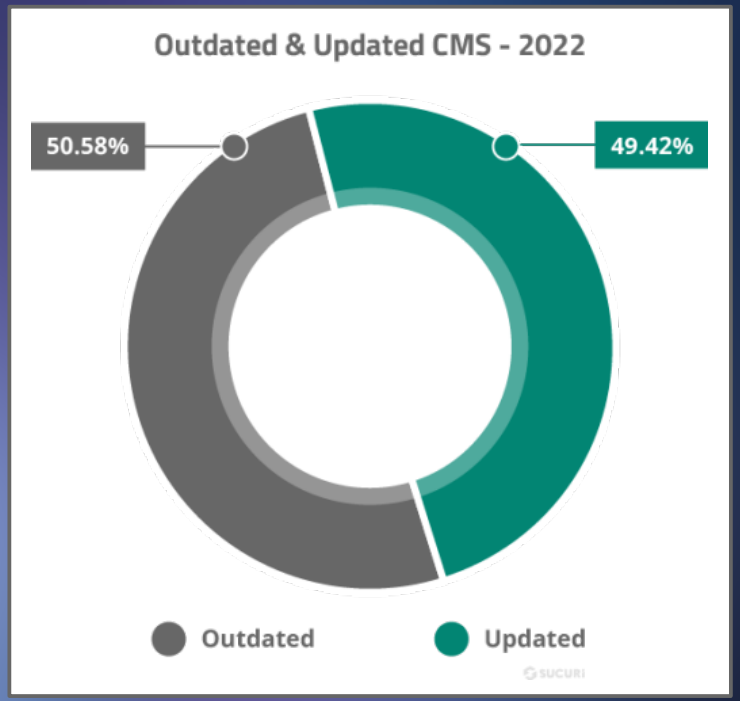
Pierre-Olivier Mercier

LRE Summer Week 2023

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE


Infected Websites Platform Distribution - 2022
100%
80%
60%
40%
20%
0%
96.2%
1.9%
0.7%
0.6%
0.4%
0.6%
WordPress
Joomla
Magento
Drupal
OpenCart
Others
SUCURI


Infected Websites Platform Distribution - 2022
100%
80%
60%
40%
20%
0%
96.2%
1.9%
0.7%
0.6%
0.4%
0.6%
WordPress
Joomla
Magento
Drupal
OpenCart
Others
SUCURI


Outdated & Updated CMS - 2022
50.58%
49.42%
Outdated
Updated
SUCURI

nginx security advisories

All nginx security issues should be reported to security-alert@nginx.org.

Patches are signed using one of the PGP public keys.

- Memory corruption in the ngx_http_mp4_module
  Severity: medium
  Advisory
  CVE-2022-41741
  Not vulnerable: 1.23.2+, 1.22.1+
  Vulnerable: 1.1.3-1.23.1, 1.0.7-1.0.15
  The patch pgp

- Memory disclosure in the ngx_http_mp4_module
  Severity: medium
  Advisory
  CVE-2022-41742
  Not vulnerable: 1.23.2+, 1.22.1+
  Vulnerable: 1.1.3-1.23.1, 1.0.7-1.0.15
  The patch pgp

- 1-byte memory overwrite in resolver
  Severity: medium
  Advisory
  CVE-2021-23017
  Not vulnerable: 1.21.0+, 1.20.1+
  Vulnerable: 0.6.18-1.20.0
  The patch pgp

NGINX

english
русский

news
about
download
security
documentation
faq
books
support

trac
twitter
blog

unit
njs

FIC EC2

66 : 31 : 28

Accueil | Scenarii | Tags | Aide

Station OxFF

Après l'utilisation de vos empreintes, de vos yeux ou de votre visage, SecureAuth a eu l'ingéniosité de développer un système d'identification avec... vos narines ! Cependant, cette startup prometteuse soupçonne d'être victime d'espionnage industriel.

Décontenancé

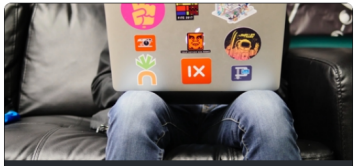
Devenez maître de la ligne de commande et entrez dans la matrice avec E-Shell! "I wish I had known E-Shell before starring in the Matrix trilogy. Now that could have been some method acting! #takethered pill #eshell" - Keanu Reeves.

La mort n'est pas une

Un meurtre ? Un crime p
enlèvement ? Une chute r
Un mystérieux inconnu ap
résoudre une énigme qui
enterrée et oubliée de
Seulement aujourd'hui
partout et n'efface rien.
FIC-tive !

Un pixel peut en cacher un autre...

Seddit l'entreprise ayant créé la plus affluente plateforme communautaire d'actualités fait face à un problème…



Bad Mood

ALERTE: InformaSup, une nouvelle école d'informatique en plein coeur de la technologie est victime d'une attaque. Elle demande l'aide d'une équipe experte dans le domaine de la cybersécurité pour les aider à sortir de cette situation.

We would li

Traulteq, une
vente en ligne
revente de p
main, a
cyberattaqu
marché.

Scandale / Whodunit / Whodunit 2 / Moonwalk / Loi de Murphy

Scandale

#Horodatage #Logs

La nouvelle circule partout sur la toile: des données confidentielles concernant l'hospitalisation du chef d'État ont fu
ou les auteurs de ce méfait.

Vous avez été contacté afin de comprendre comment l'information du président malade a pu être divulguée et retrou

Vous trouverez ci-joint une capture d'écran d'une annonce sans précédent diffusée à la télé hier soir, ainsi que des
qui vous seront surement utiles !

COTE
2.6 points
initialement 5 points

TENTÉ PAR
25 équipes (cumulant 120 tentatives)

RESOLU PAR
24 équipes

Téléchargements

Attention : puisqu'il s'agit de captures effectuées dans le but de découvrir si des actes malveillants ont été commis, les contenus qui sont téléchargeables peuvent contenir du contenu malveillant !

breaking_news.png
Taille : 219.32 kio
b2sum : 33da0ac849b443ebd17ca5ba911a4123410ab5f...

logs.txt
Taille : 31.89 kio
b2sum : 4ea7063c3ad24e360a5973154100fa1bee8340f...

patient_list.txt
Taille : 3.71 kio
b2sum : 862a97c22271f8474dec716eaaa3f764ae3a49f...

Indices

Astuce #1
Débloquer cet indice v

Faire son rapport

Horodatage de la requête récupérant les données du Président :
yyyy-mm-dd HH:MM:SS
Fuseau horaire UTC+2 (Europe/Paris)

Nom d'hôte du serveur dont les données ont fuité :
PC01

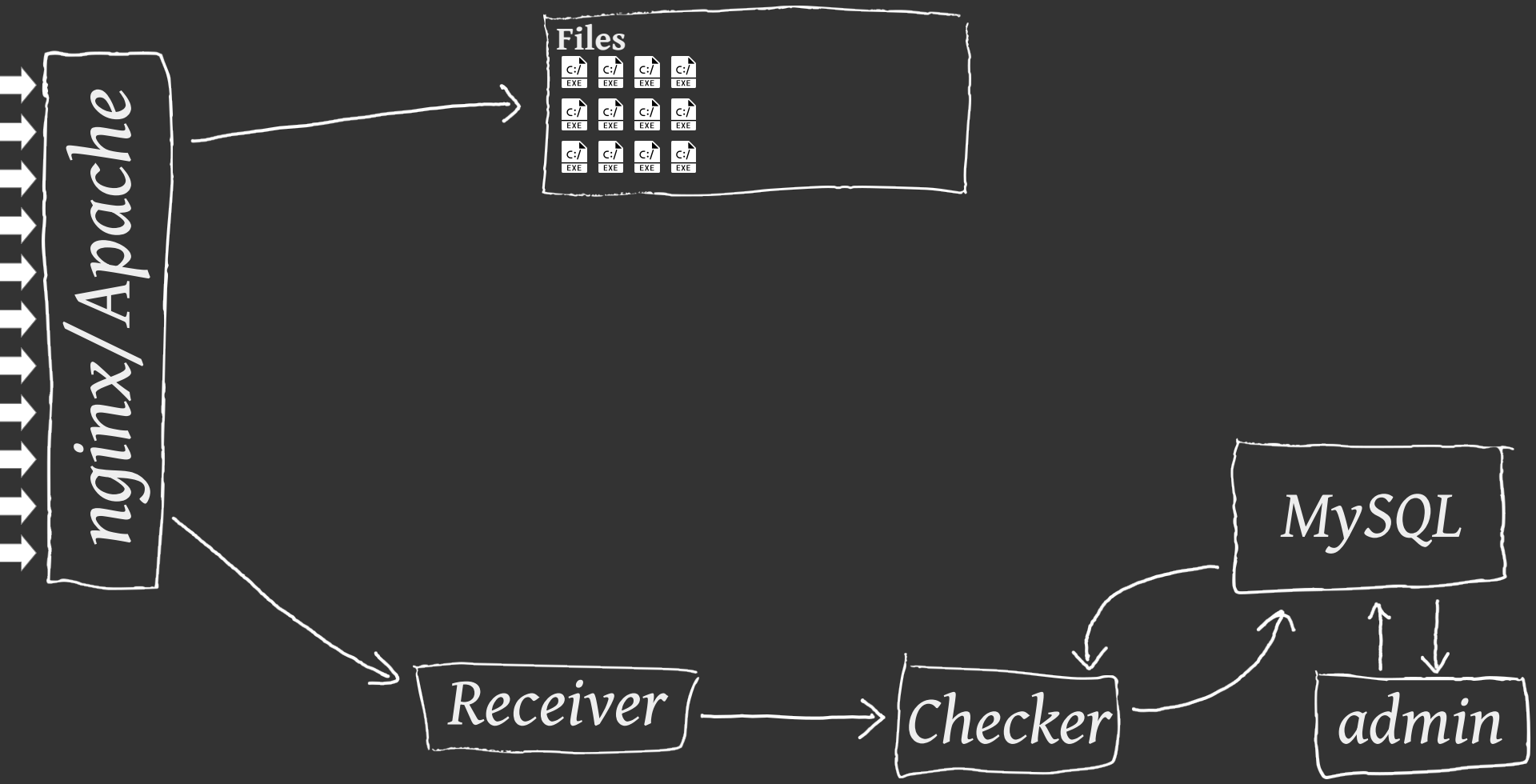
Poste depuis lequel l'attaquant est parvenu à récupérer les données médicales du chef d'État :
CHIR42

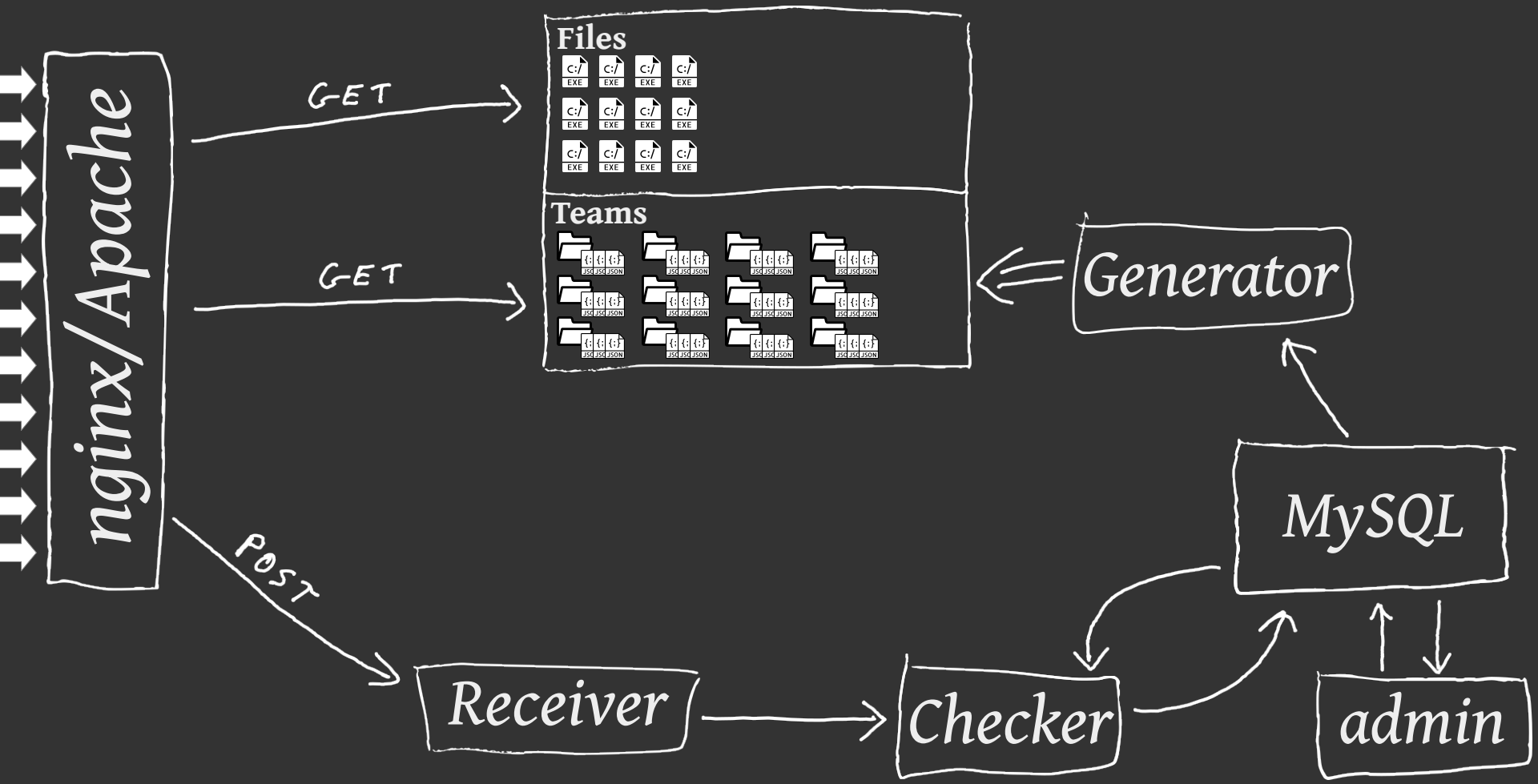
Soumettre

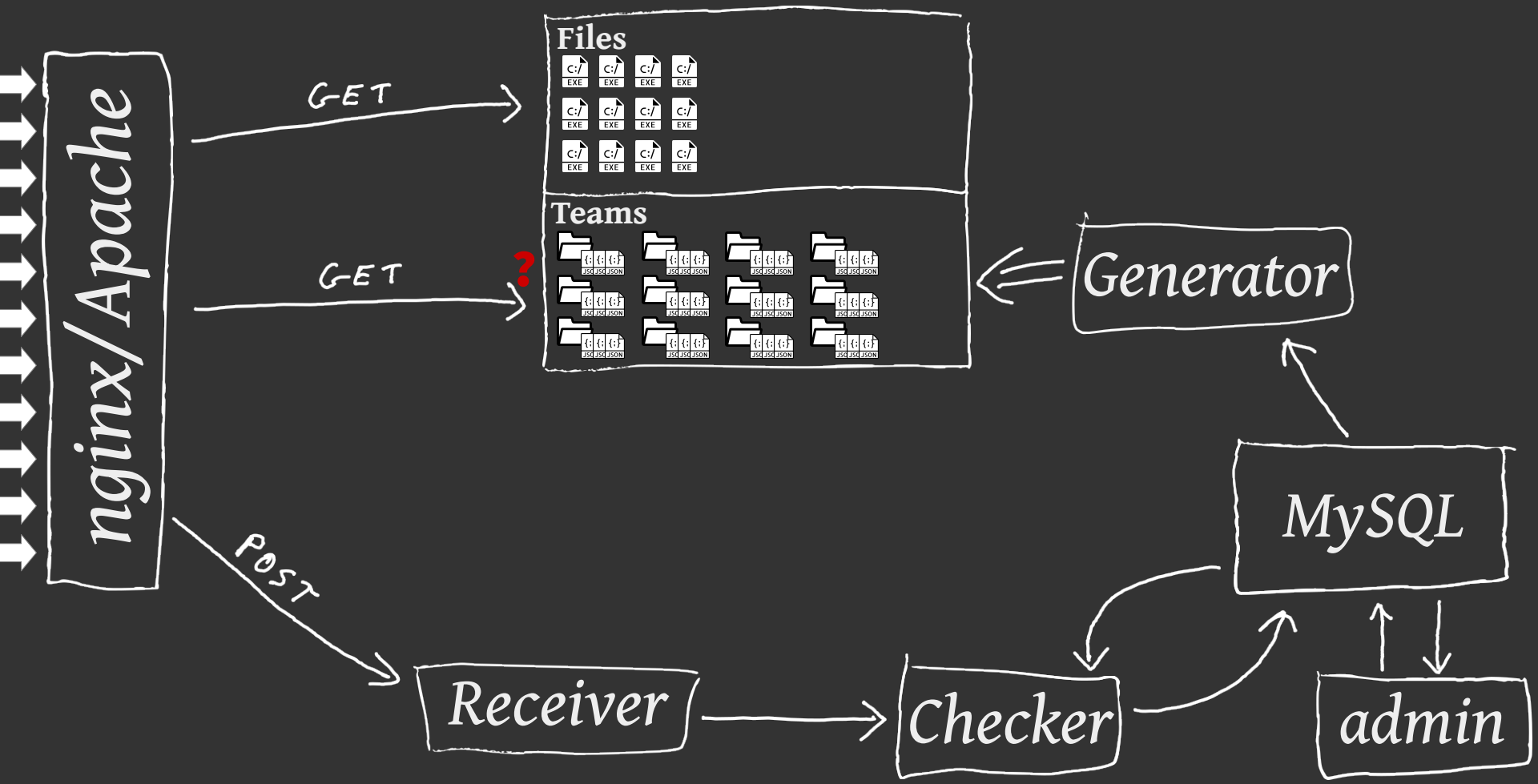

Comment avoir les avantages d’un site statique, mais avec des comptes utilisateurs ?

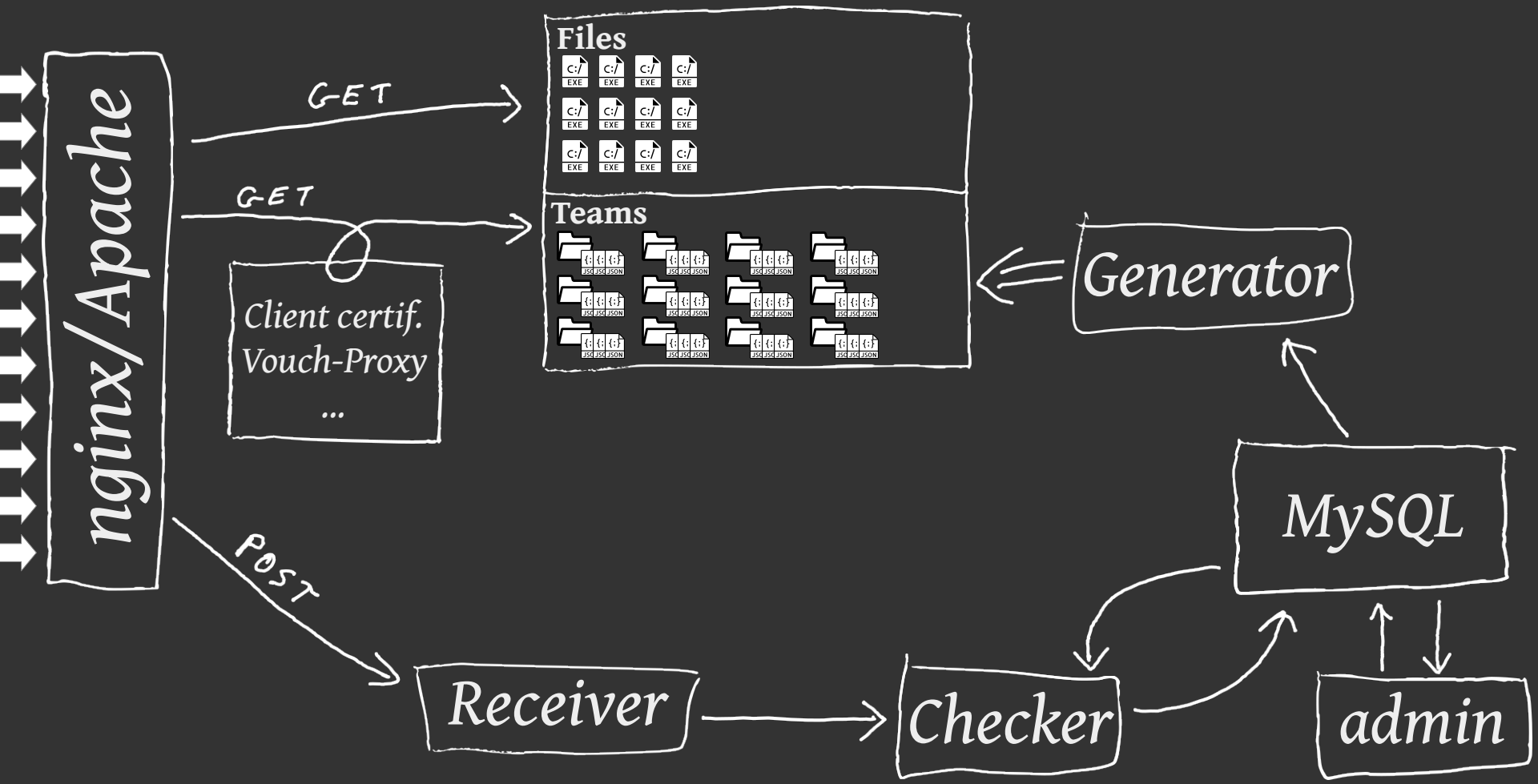

FTP
wordpress/
wp-admin/
wp-content/
wp-includes/
index.php
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
nginx/Apache
MySQL
PHP-FPM

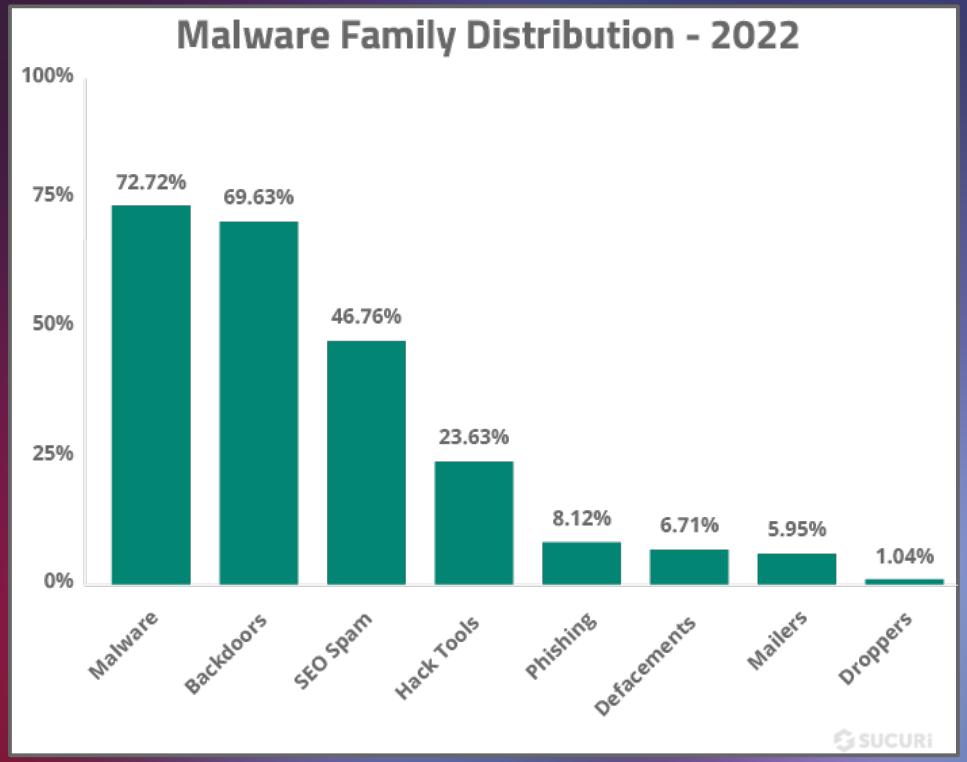

FTP
wordpress/
wp-admin/
wp-content/
wp-includes/
index.php
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
nginx/Apache
MySQL
/article
PHP-FPM
PHP-FPM
/wp-admin/

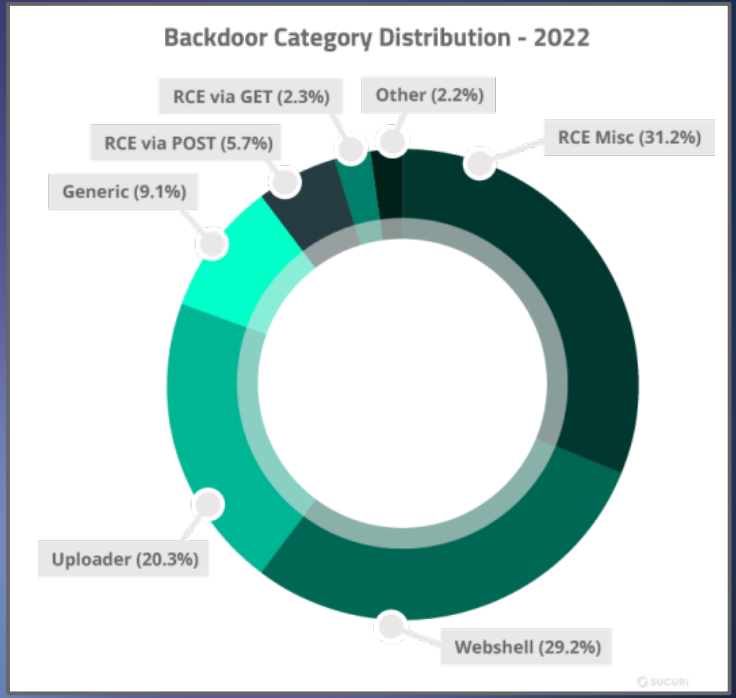

Files
nginx/Apache
Receiver
Checker
MySQL
admin

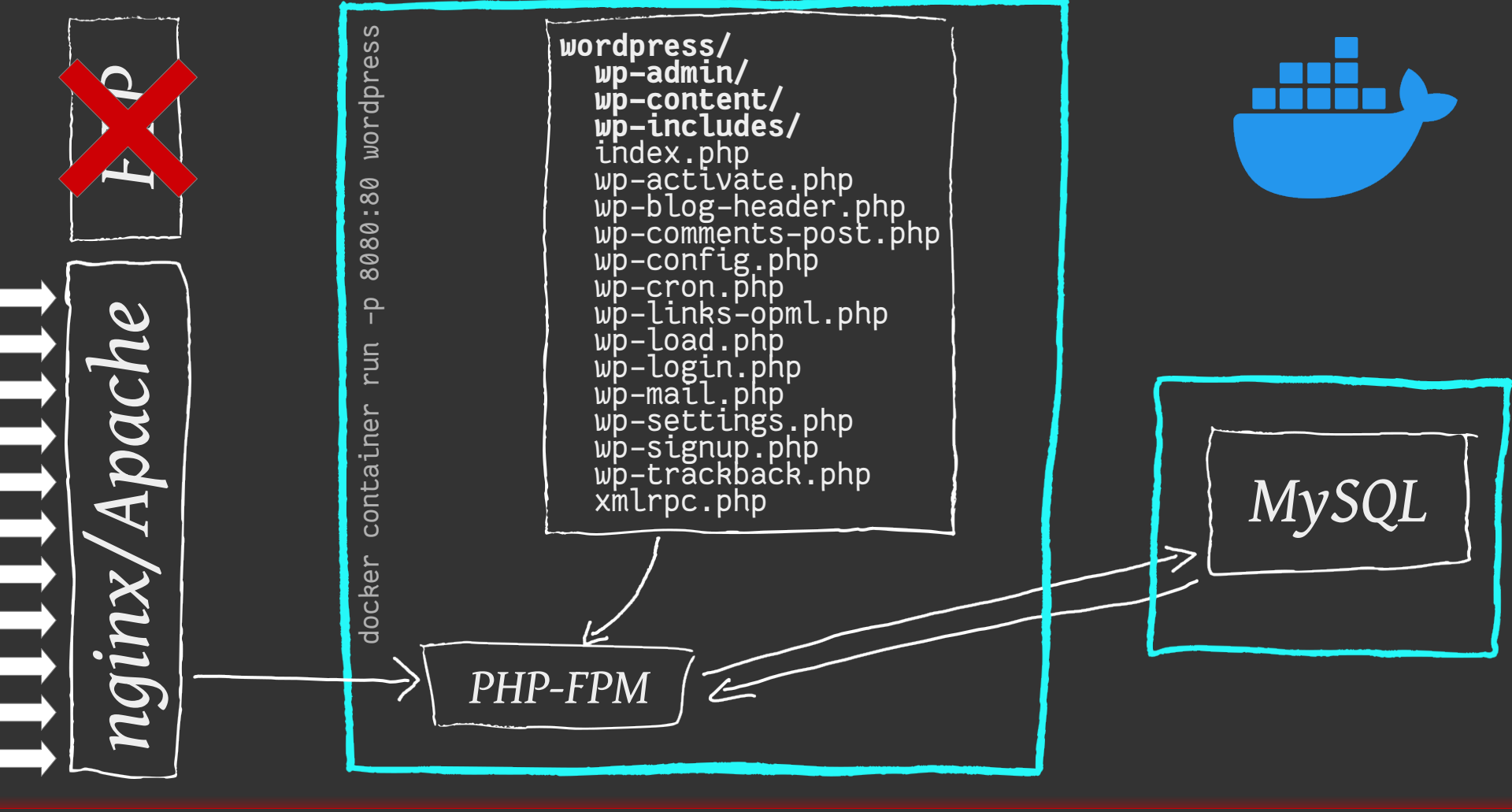

nginx/Apache
GET
GET
POST
Files
Teams
Generator
MySQL
Receiver
Checker
admin

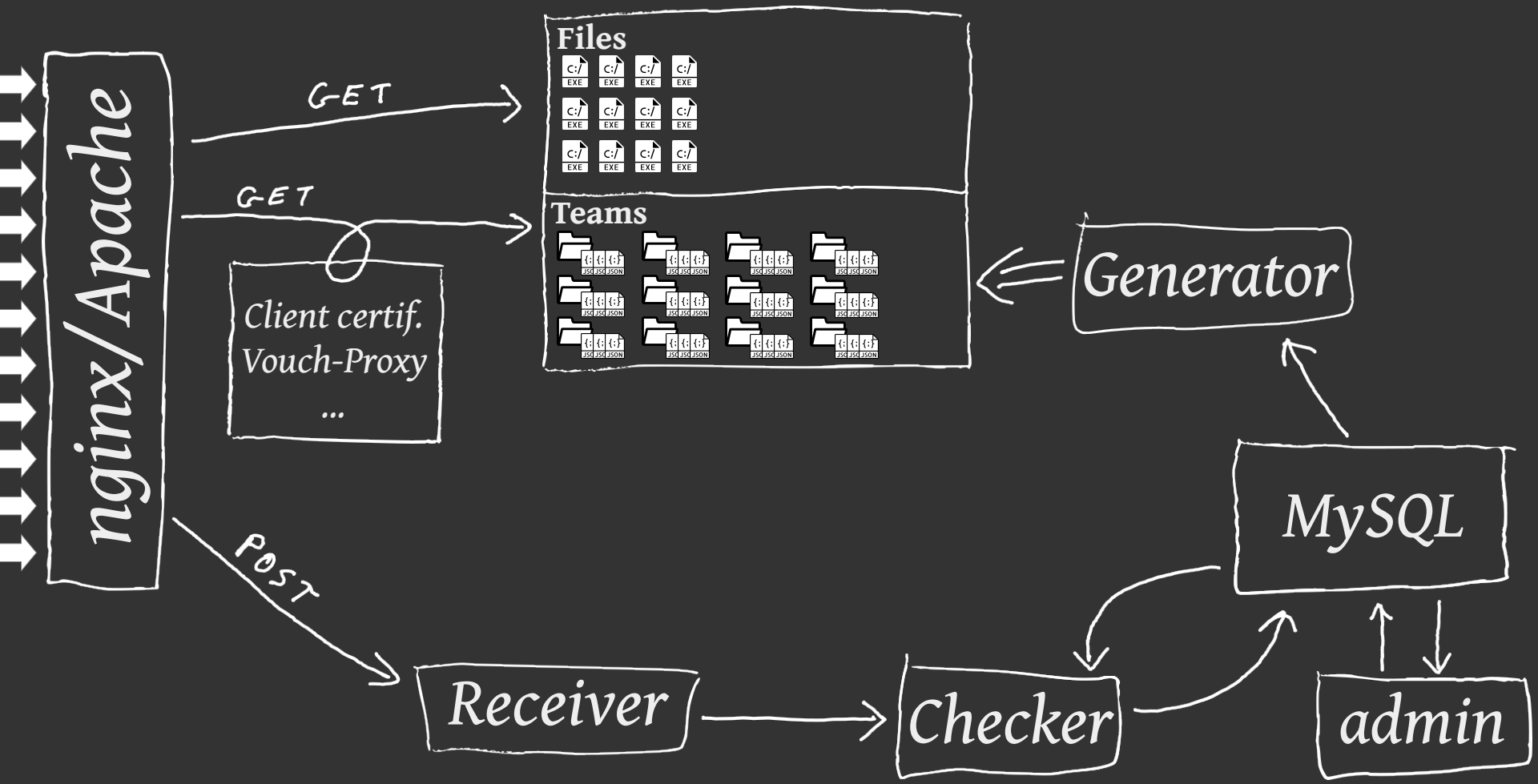

Files
Teams
GET
GET
?
POST
nginx/Apache
Generator
MySQL
Receiver
Checker
admin

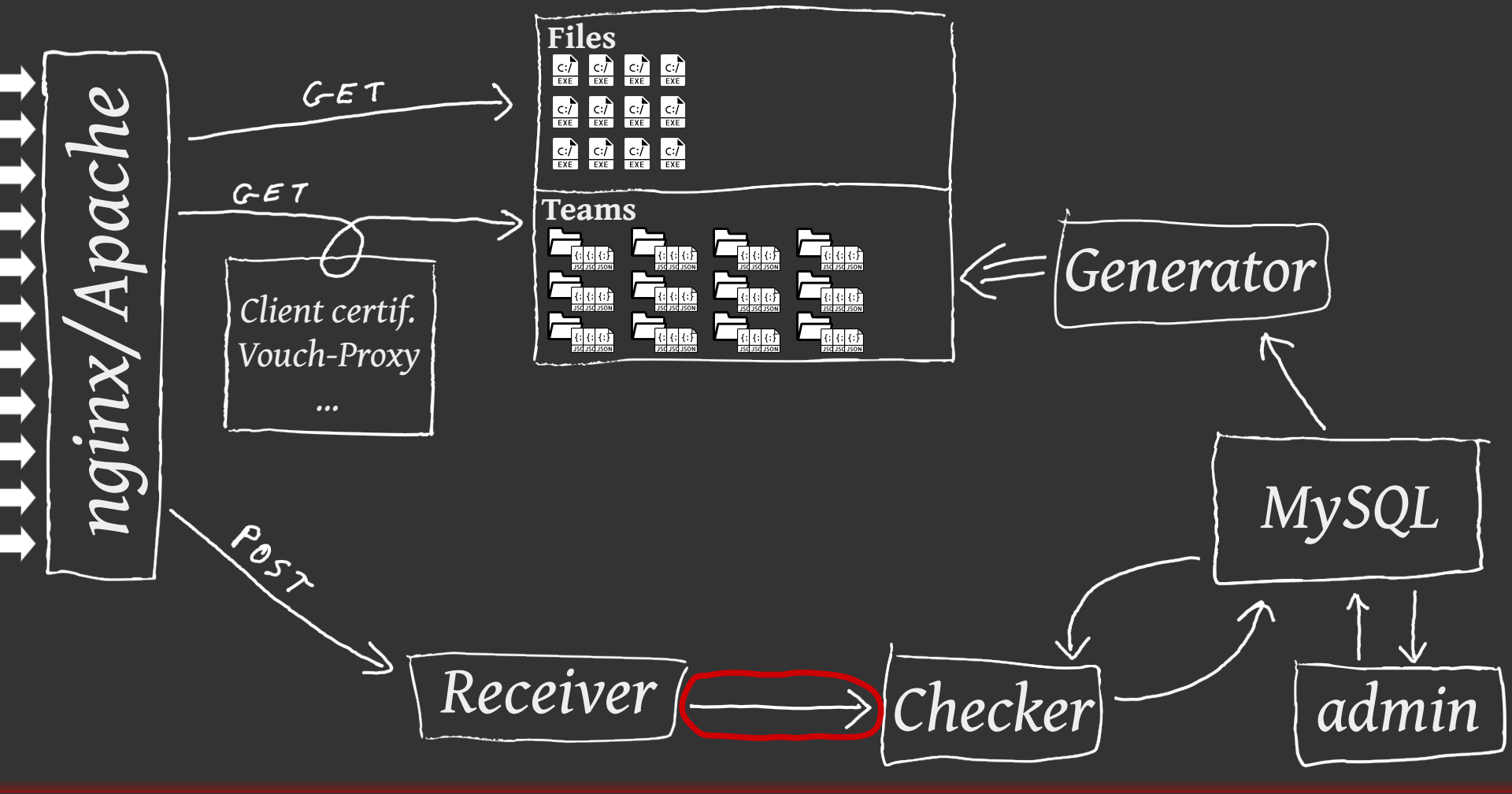

nginx/Apache
GET
GET
Client certif.
Vouch-Proxy
...
Files
Teams
Generator
MySQL
POST
Receiver
Checker
admin

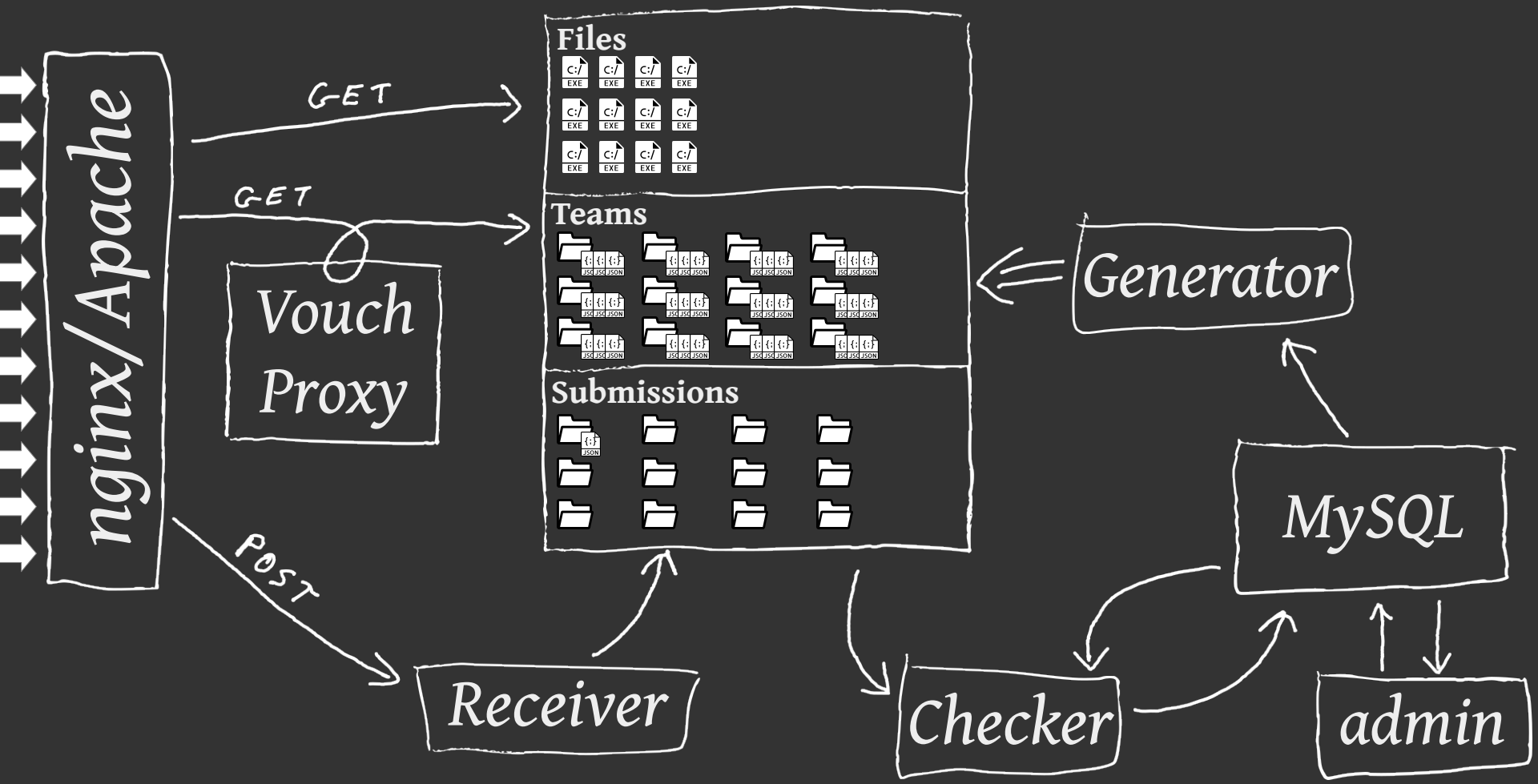

Malware Family Distribution - 2022
100%
75%
50%
25%
0%
72.72%
69.63%
46.76%
23.63%
8.12%
6.71%
5.95%
1.04%
Malware
Backdoors
SEO Spam
Hack Tools
Phishing
Defacements
Mailers
Droppers
SUCURI

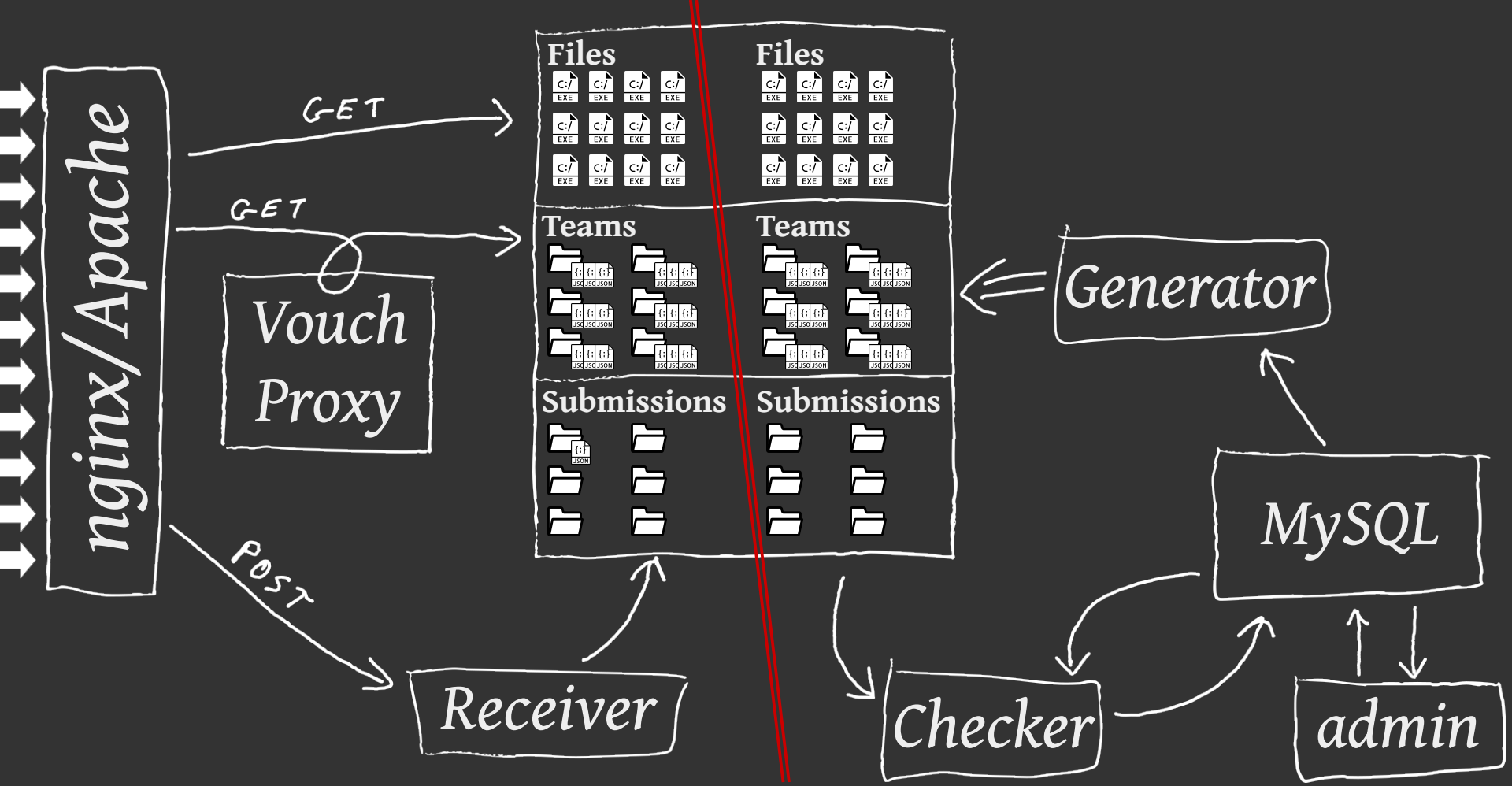

Backdoor Category Distribution - 2022
RCE via GET (2.3%)
Other (2.2%)
RCE via POST (5.7%)
RCE Misc (31.2%)
Generic (9.1%)
Uploader (20.3%)
Webshell (29.2%)

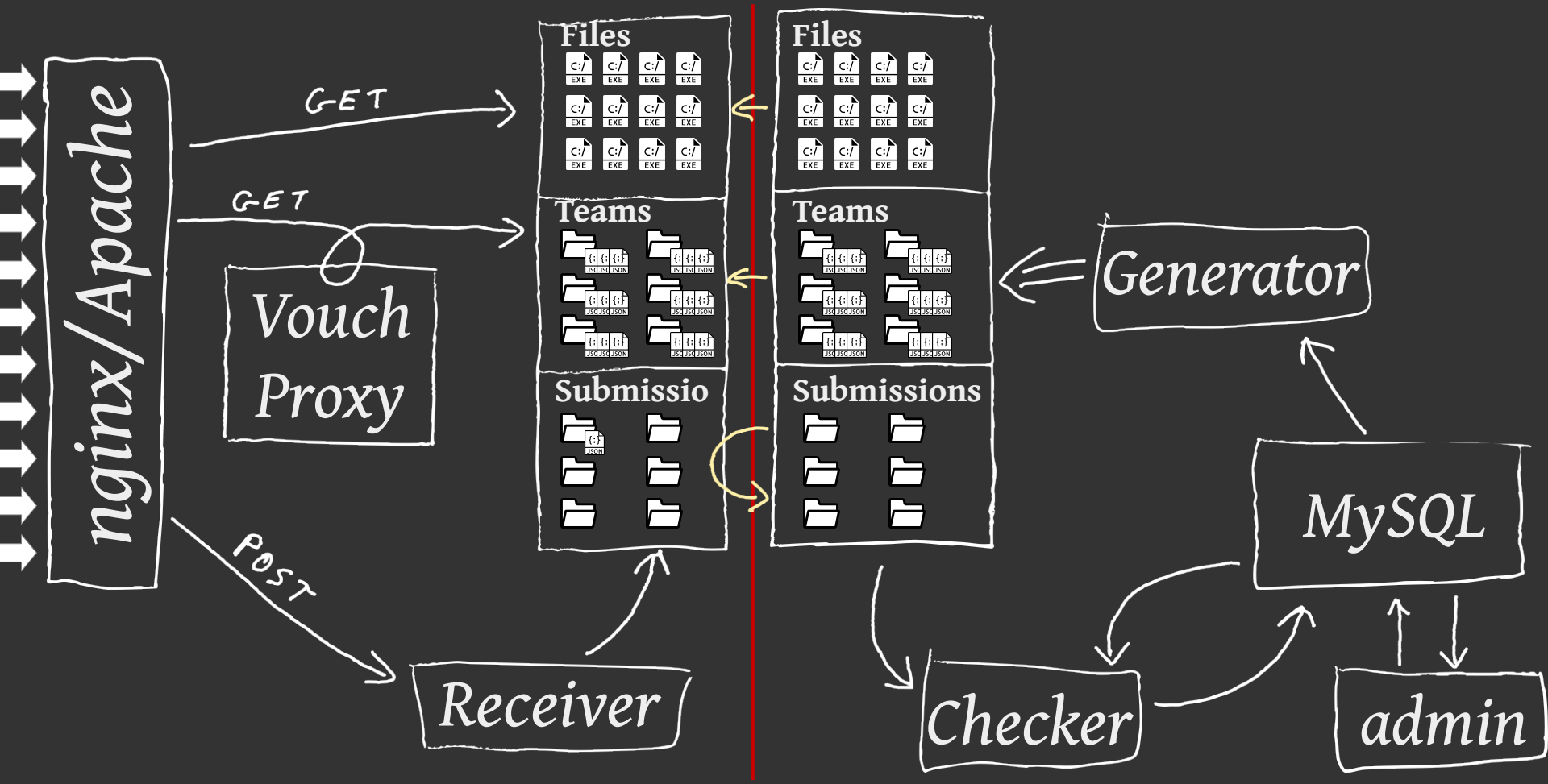

FTP
nginx/Apache
docker container run -p 8080:80 wordpress
wordpress/
wp-admin/
wp-content/
wp-includes/
index.php
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
PHP-FPM
MySQL

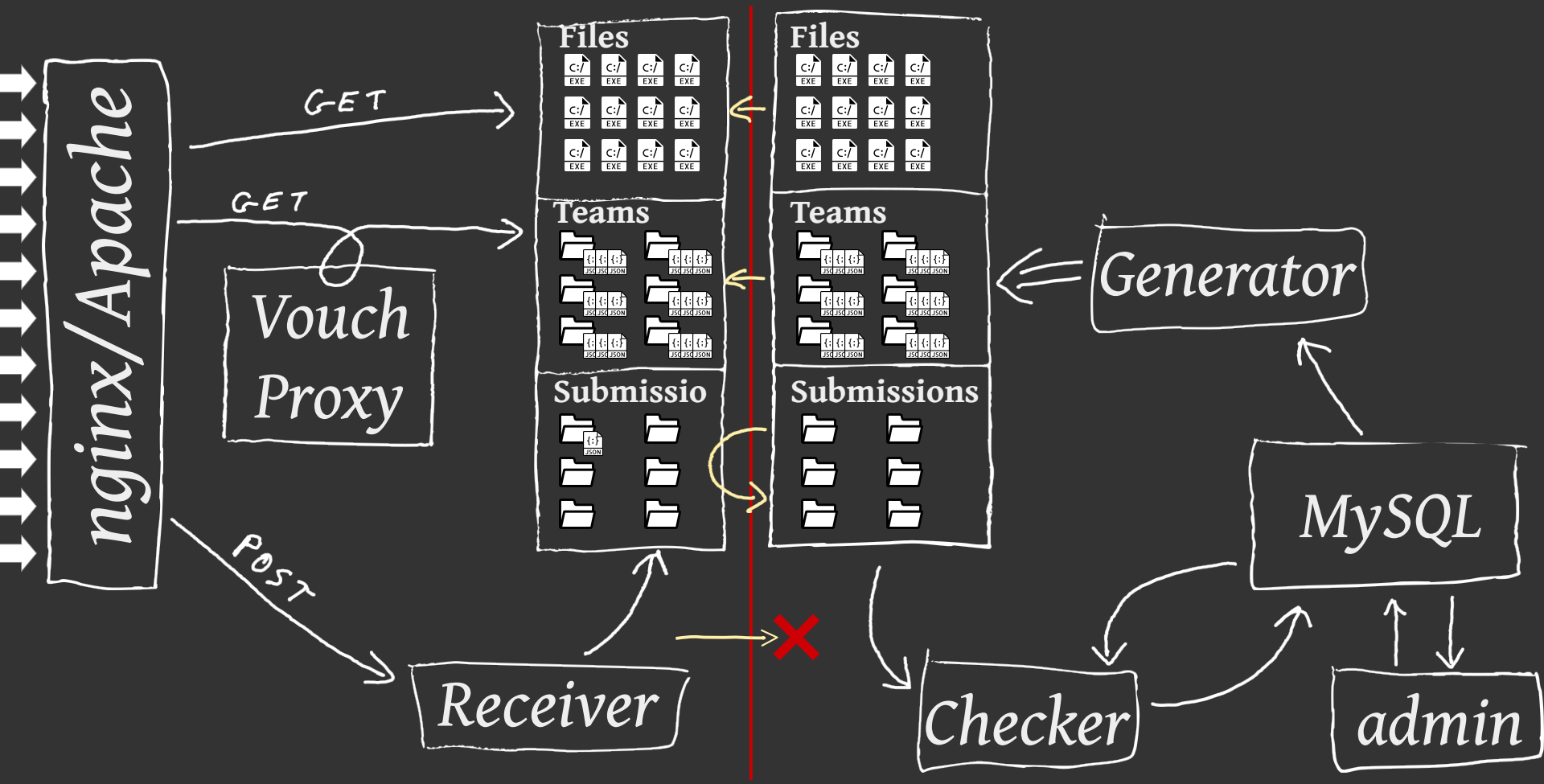

nginx/Apache
GET
GET
Client certif.
Vouch-Proxy
...
Files
Teams
Generator
MySQL
POST
Receiver
Checker
admin


Files
Teams
GET
GET
nginx/Apache
Client certif.
Vouch-Proxy
...
Generator
MySQL
POST
Receiver
Checker
admin


nginx/Apache
GET
GET
Vouch Proxy
POST
Files
Teams
Submissions
Generator
MySQL
Receiver
Checker
admin

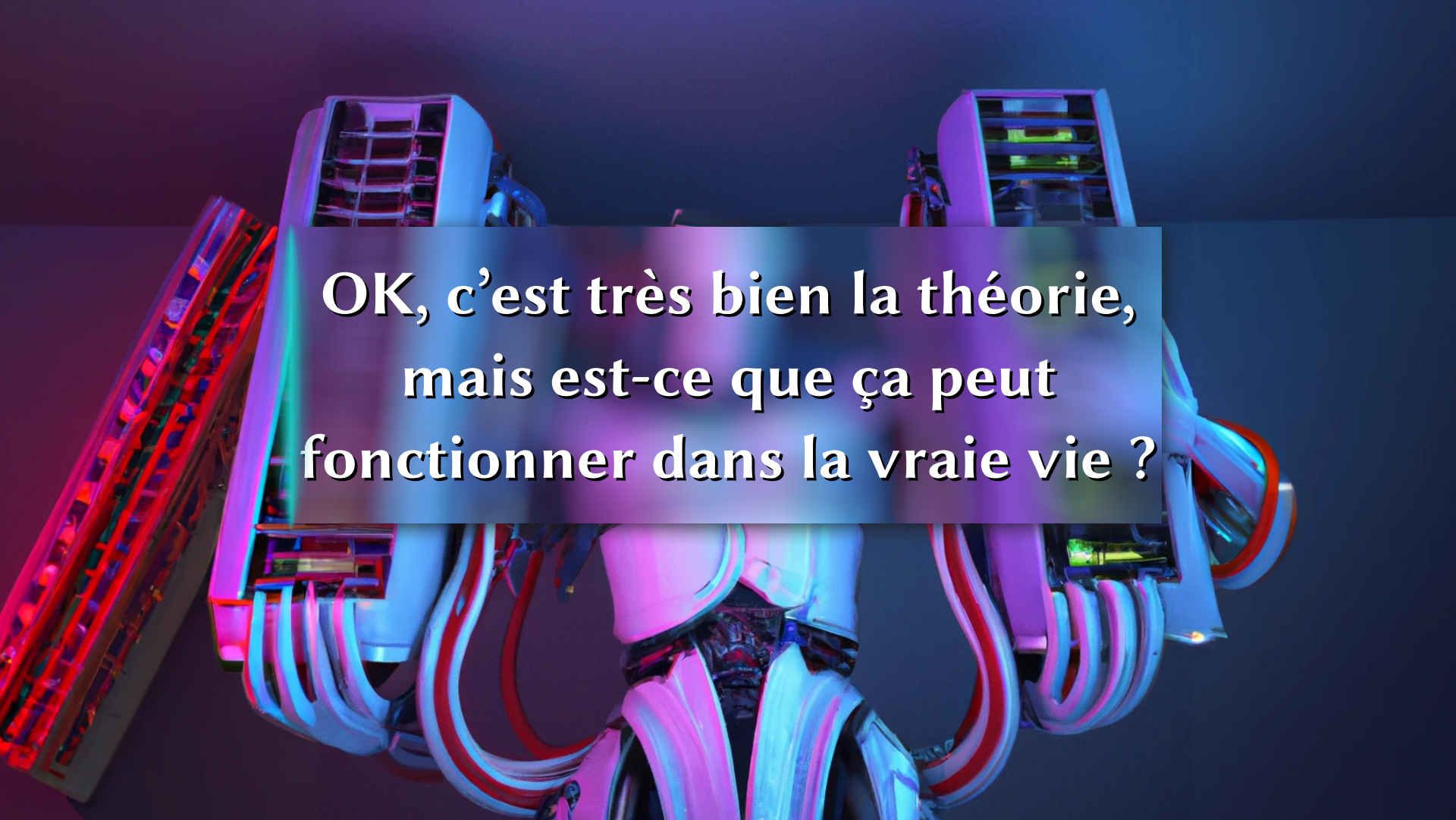

nginx/Apache
GET
GET
Vouch Proxy
POST
Files
Files
Teams
Teams
Submissions
Submissions
Generator
MySQL
Receiver
Checker
admin


nginx/Apache
GET
GET
Vouch Proxy
POST
Receiver
Files
Teams
Submissio
Files
Teams
Submissions
Generator
MySQL
Checker
admin

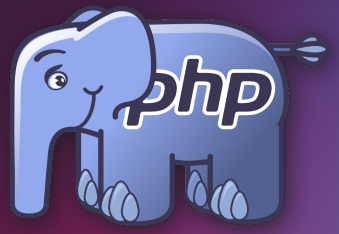


Défense en profondeur : isolation par machines

Pierre-Olivier Mercier


OK, c’est très bien la théorie,
mais est-ce que ça peut
fonctionner dans la vraie vie ?

2013



Challenge forensic

FIC CHALLENGE

EPITA ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

- Dotnet 3
- Dump mémoire 5
- Flash 4
- Images 1 5
- Images 2 5
- Java 4
- PDF 1 5
- PDF 2 4
- Réseau 1 5
- Réseau 2 5
- Réseau 3 4
- Social Engineering 5

Images 2

Exercice 1 | Exercice 2 | Exercice 3 | Exercice 4 | Exercice 5

Exercice 5

0 équipe a résolu cet exercice

- **Gain :** 80
- **Description :** La vidéo au format mkv est filmée dans le style d'un film muet. Vous cherchez des informations supplémentaires.

Téléchargements

	Nom	SHA1	Taille
	exo5.mkv	9112e43a9984eadf1d90416e08054db574862244	32640375

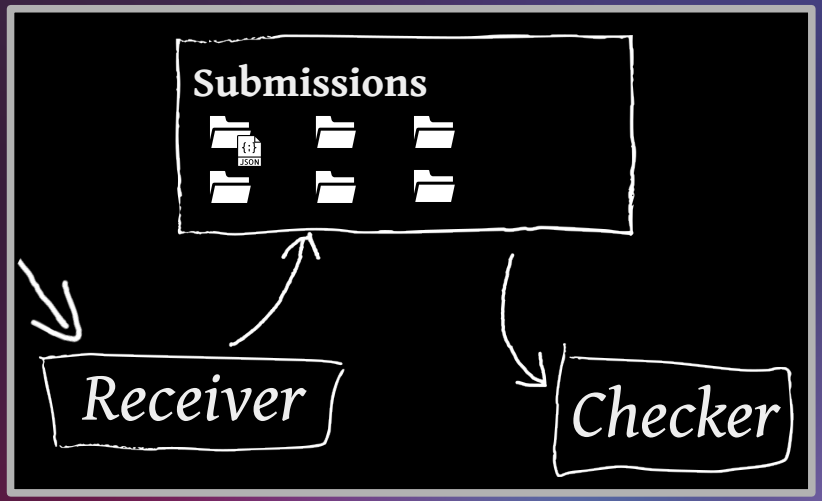
Solutions

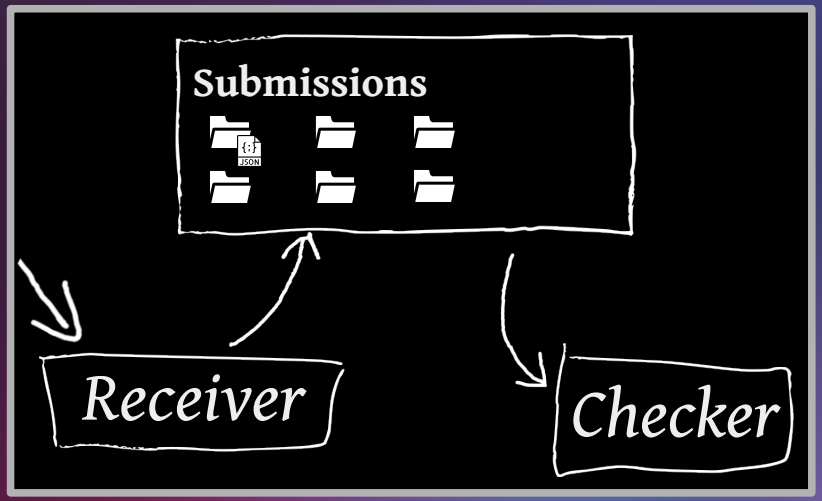
Vérifiez votre solution parmi les algorithmes suivants :

sha256	a88b0258c23902bbc4101be31a164a7e753a8bf5ed1d34ffebef579246fff7a8
sha512	a39d6dfdb8cdb588f92dd197ab83d3ce1142aa79607a7c585ea15e09c7746103999a8e8ace744687affb4d…
whirlpool	713471898f2ed77711b78ecc6471f16a03a53e5046b8d69188f5c992e03c61f1d9e3aa3d0aa1dd72e911a0…

Première implémentation pour le FIC 2014

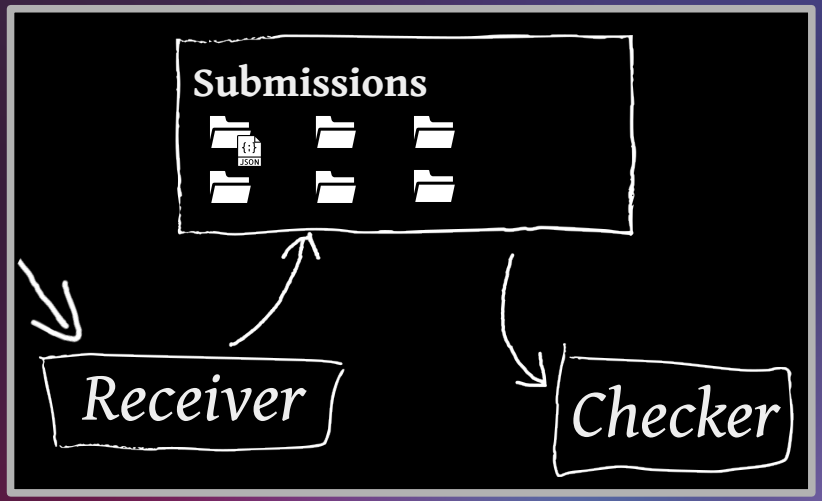
Pierre-Olivier Mercier


Submissions
JSON
Receiver
Checker




```
42sh$ crontab -e
* * * * * php check-submissions.php /submissions
```

```
While true; do
    php check-submissions.php /submissions
    sleep .5
done
```



Ou inotify // incrond
(kqueue sous BSD) 👍

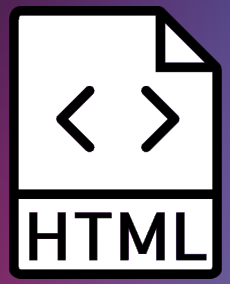
```
42sh$ crontab -e
* * * * * php check-submissions.php /submissions
```

```
While true; do
    php check-submissions.php /submissions
    sleep .5
done
```

```
find /submissions -type f | while read f; do
    mkdir -p /submissions/.tmp/$(basedir "${f}")
    mv "${f}" /submissions/.tmp/$(basedir "${f}")
done
rsync -av /submissions ...
rm -r /submissions/.tmp
```

```
find /submissions -type f | while read f; do
    mkdir -p /submissions/.tmp/$(basedir "${f}")
    mv "${f}" /submissions/.tmp/$(basedir "${f}")
done
rsync -av /submissions ...
rm -r /submissions/.tmp
```

```
rsync --remove-source-files -av /submissions ...
```



Par équipe :

```
4 + $nb_exercice
```

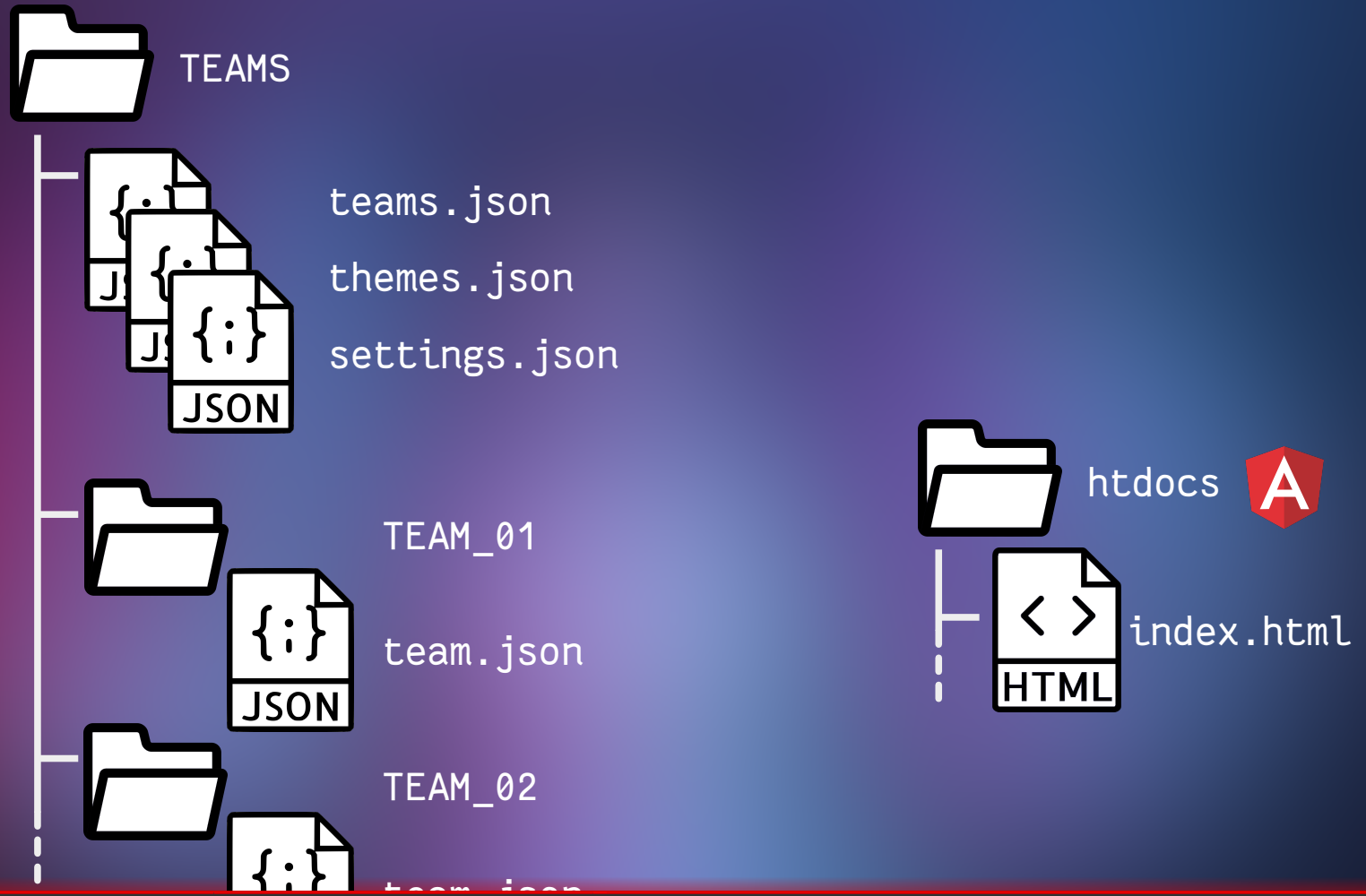
Par équipe :

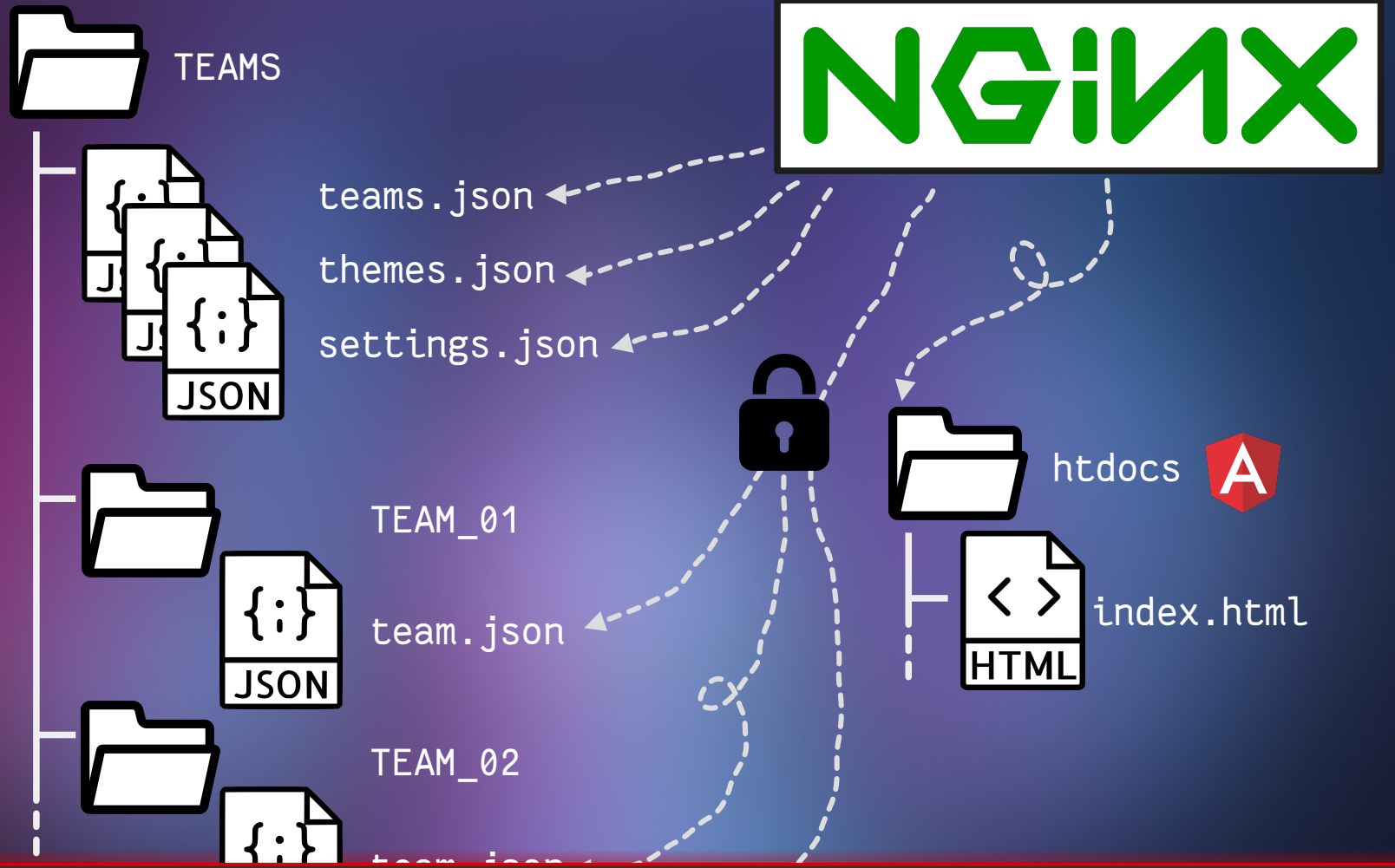
`4 + $nb_exercice`

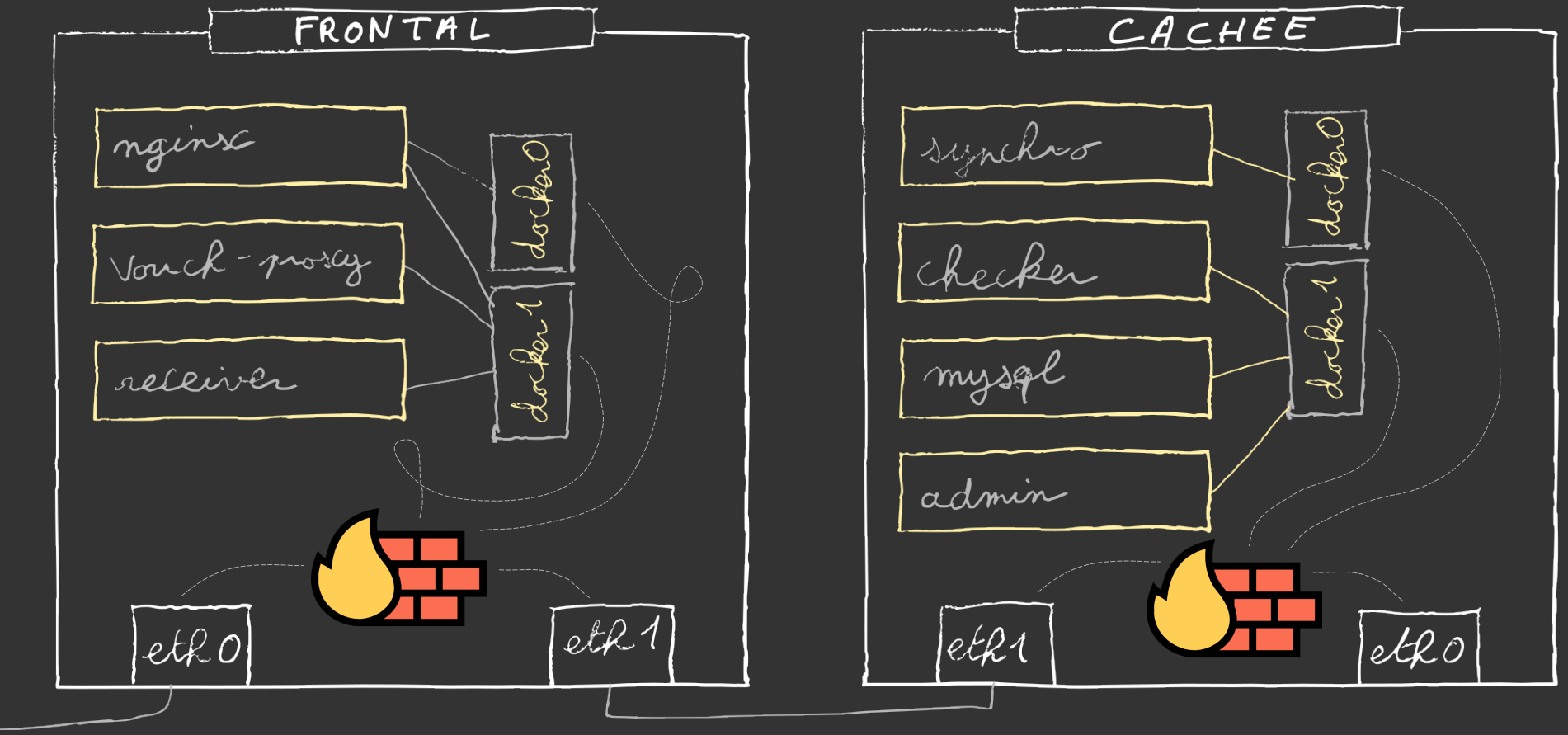
1 fichier par équipe

3 fichiers globaux

Seconde implémentation


TEAMS
teams.json
themes.json
settings.json
JSON
TEAM_01
team.json
JSON
TEAM_02
htdocs
index.html
HTML


TEAMS
JSON
teams.json
themes.json
settings.json
NGINX
htdocs
TEAM_01
team.json
JSON
HTML
index.html
TEAM_02

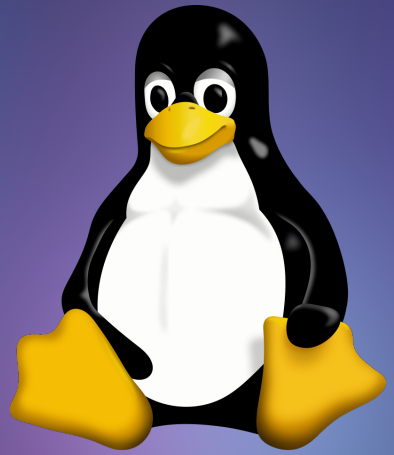

FRONTAL
nginxc
vouch-proxy
receiver
docker0
docker1
eth0
eth1
CACHEE
sync.ro
checker
mysql
admin
docker0
docker1
eth1
eth0


LinuxKit à la rescousse
linuxkit
RC

IPC

PID

UTS



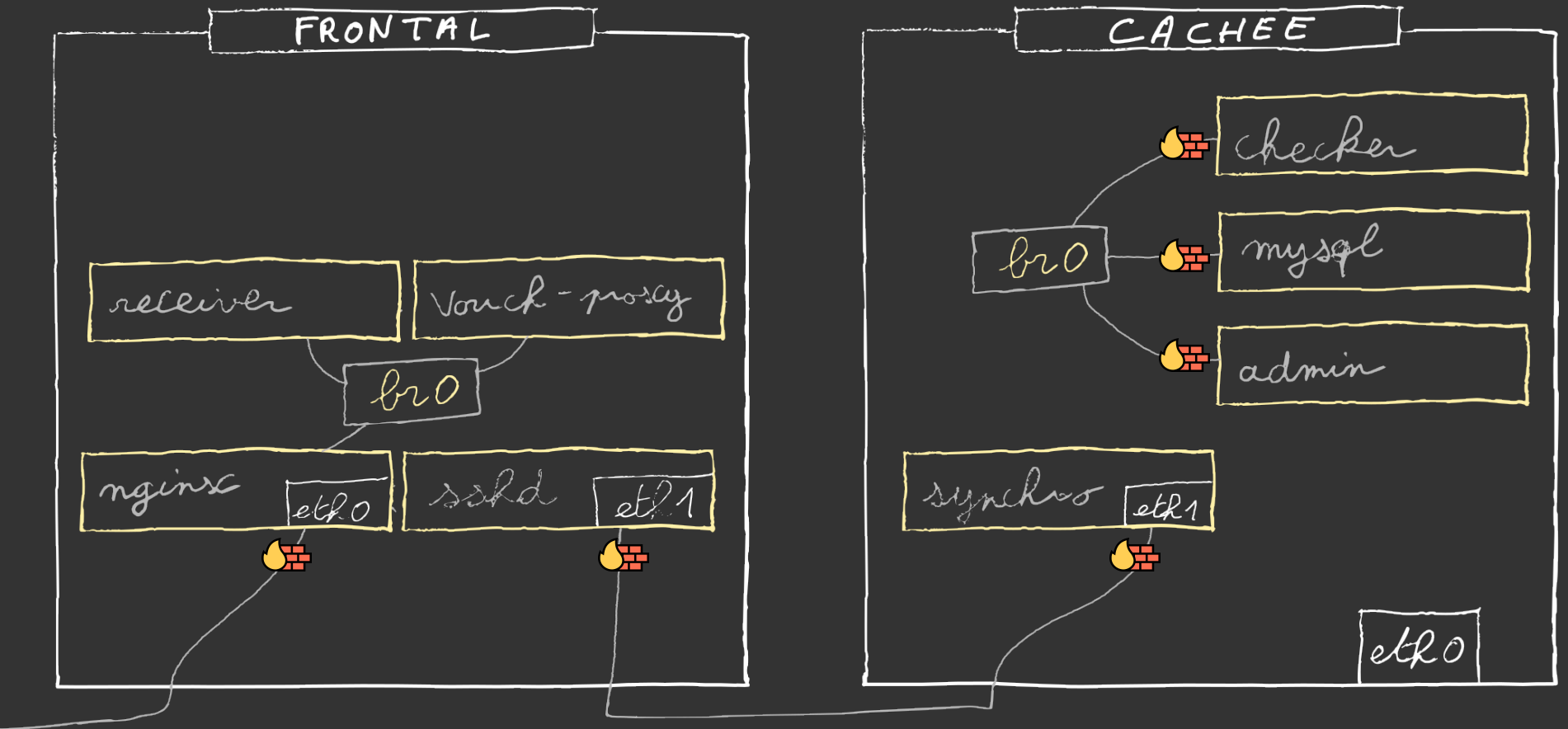
network

mount

user

time

cgroup


FRONTAL
receiver
Vouch-proxy
br0
nginxc
eth0
sshd
eth1
CACHEE
checker
br0
mysql
admin
synchro
eth1
eth0


Est-ce plus complexe ?

Dépôt git :

https://git.nemunai.re/fic/server

Pierre-Olivier Mercier
https://nemunai.re/