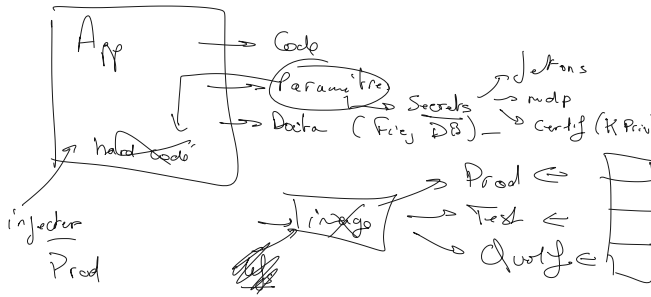
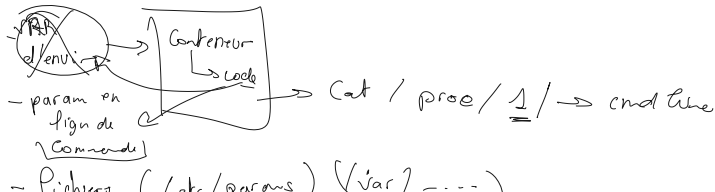
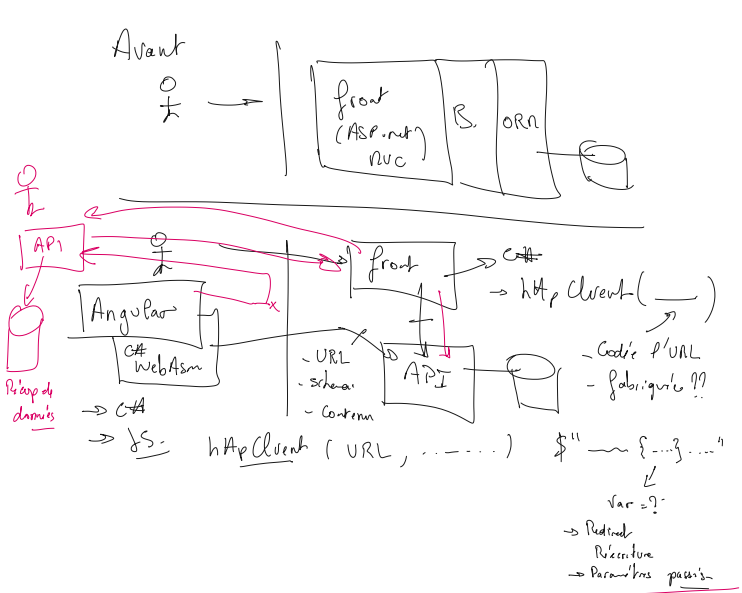
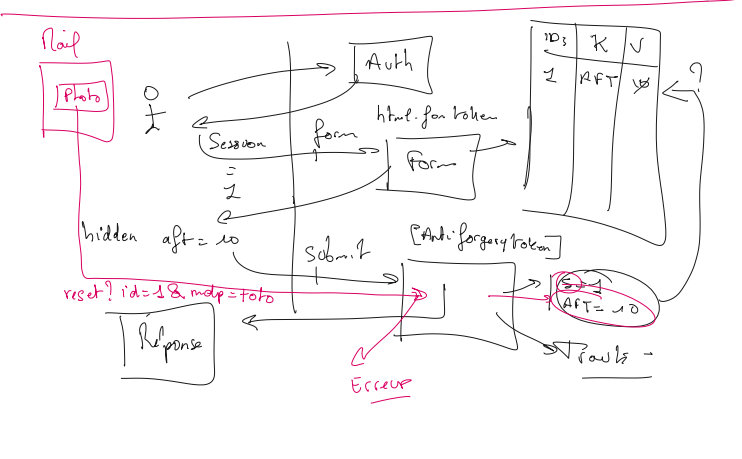

App
Code
Paramètre
Secrets
Jetons
mdp
Certif (K Priv)
Docker (Fic, DB)
Healthcheck
injecter
Prod
Jenkins
Prod
Test
Qualif

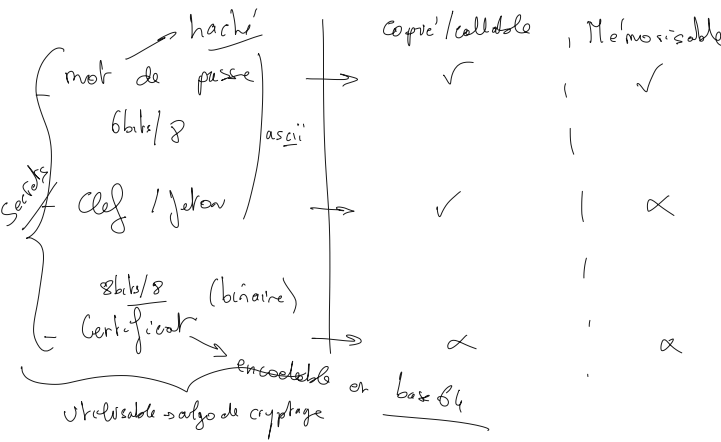

Conteneur
Code
Cat / proc / 1 / → cmd line
- param en ligne de commande
- fichiers (/etc/params) (/var/ ...)
↳ STDin ...


Mémoire

PS1
PS2
↳ "marcher"


Avant
front
(ASP.net)
MVC
B.
ORM
API
Angular
C# WebAsm
Paramètres du domaine
front
C#
→ HttpClient( )
- URL
- schéma
- Contenu
API
- Codé d'URL
- Fabrique ??
→ C#
→ JS
HttpClient (URL, ...)
$" ~~ {...} ..."
var = ?
→ Retrait
Réécriture
→ Paramètres passés


Naif
Photo
Auth
Session
=
1
form
html. for token
form
IDs
K
V
1
AFT
10
hidden aft = 10
Submit
[Anti-forgery token]
reset? id=18, mdp=foto
AFT = 10
Réponse
Erreur
Faults



Algos de Transformation

- Encodage (sans secret) → Exemples (Aucune sécurité)
  - UTF-8
  - ISO8859 = ascii étendu européen
  - base64
- Hachage (sans secret) → Transformation à Sens unique
- Cryptage
  - Symétrique (1 secret)
  - Asymétrique (paire de secrets)

Algos de hash → crc / checkSum

↳ Rapide / Suffisamment fiable
- Pas sécure

⇒ "Collision" Paquet ≠ hash identique

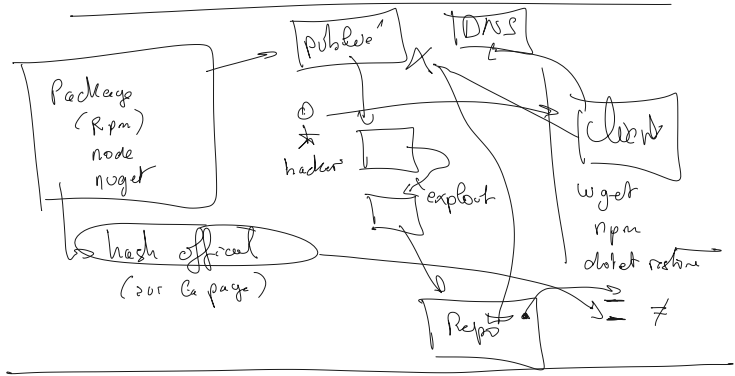
ABC BAC → 130

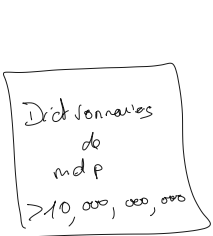
65+66+67 = 130

- md 5 → "bon compromis" → Très peu de collisions
→ utilisé pour - check non bidouillé
→ à partir des data en stockage, etc...

- sha
- sha1
  sha2 (56)
  (512)
- sha3

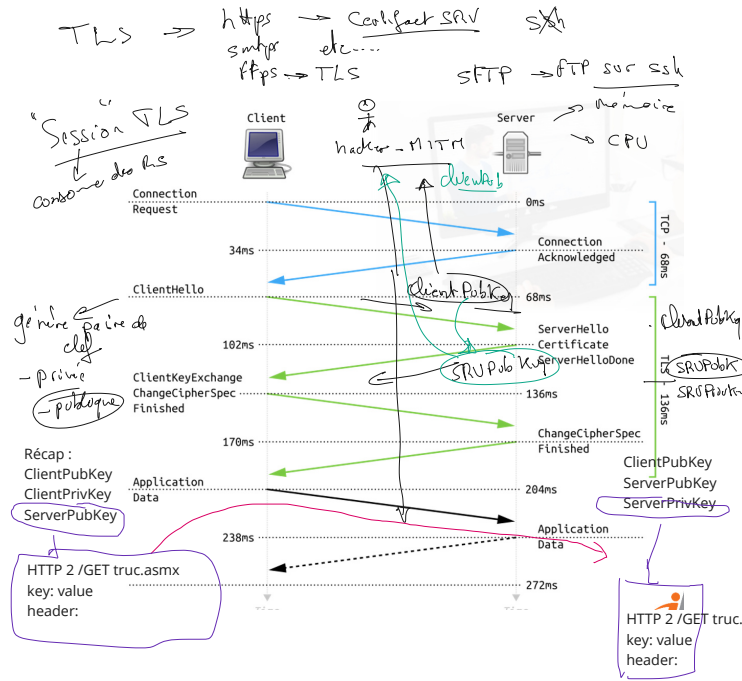
'sécurité'

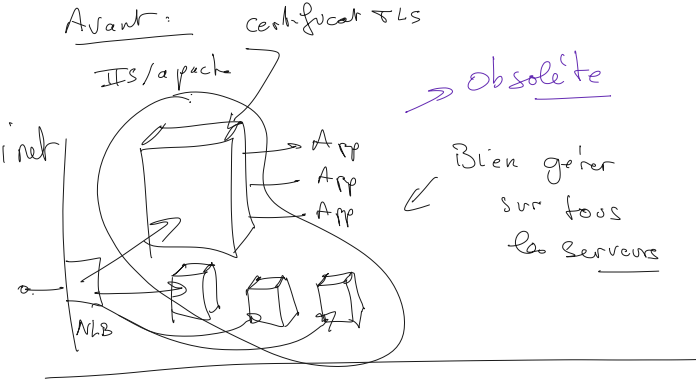


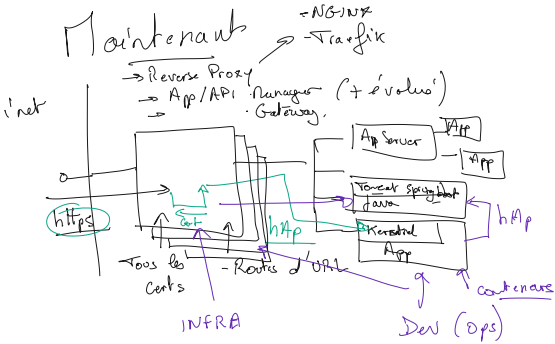


→ User
→ mdp encrypté
Hacker
→ sha2

Password
Azerty4 Pa$$w0rd

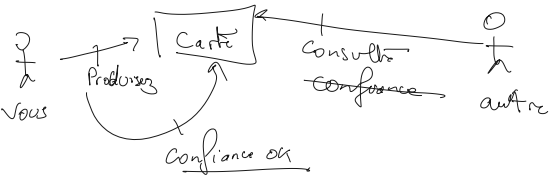

TLS
https → Certificat SRV
smtps etc....
ftps → TLS
SSH
SFTP → FTP sur ssh
« Session TLS »
Client
Server
hacker - MITM
mémoire
CPU
Connection Request
0ms
34ms
Connection Acknowledged
TCP - 68ms
ClientHello
68ms
ClientKeyExchange
ChangeCipherSpec
Finished
102ms
ServerHello
Certificate
ServerHelloDone
136ms
TLS - 136ms
170ms
ChangeCipherSpec
Finished
Application Data
204ms
238ms
Application Data
272ms
Récap :
ClientPubKey
ClientPrivKey
ServerPubKey
HTTP 2 /GET truc.asmx
key: value
header:
ClientPubKey
ServerPubKey
ServerPrivKey
HTTP 2 /GET truc.
key: value
header:


Avant :
Certificat TLS
IIS / apache
App
App
App
inet
NLB
Obsolète
Bien gérer
sur tous
les serveurs


Maintenant
- NGINX
- Traefik
Reverse Proxy
App / API Manager (+ évolué)
Gateway.
inet
App Server
App
Tomcat Spring Boot
Java
Kestrel
App
https
http
hMp
Tous les
Certs
- Routes d'URL
INFRA
Dev (Ops)
containers

Certificat → Carte (Métaphore)

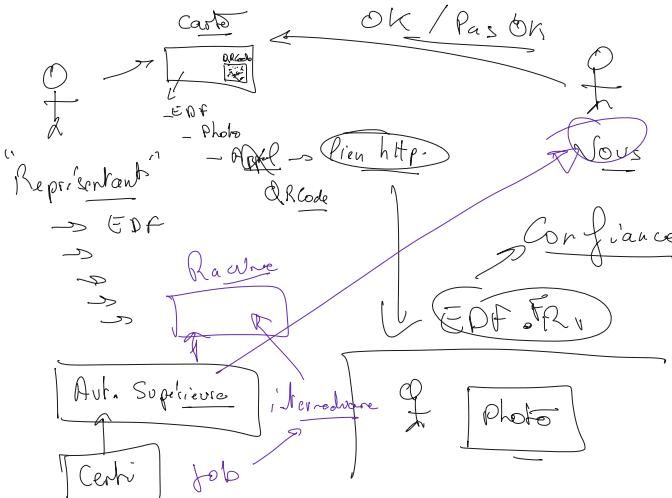
→ Quelle confiance ?

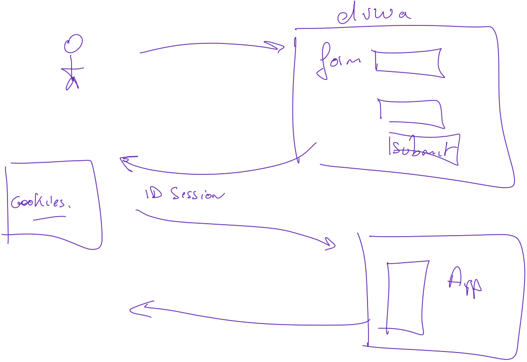


→ Certificats auto signés -

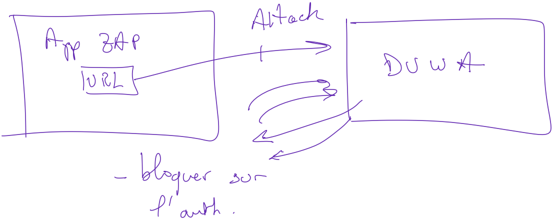
→ a 1 niveau

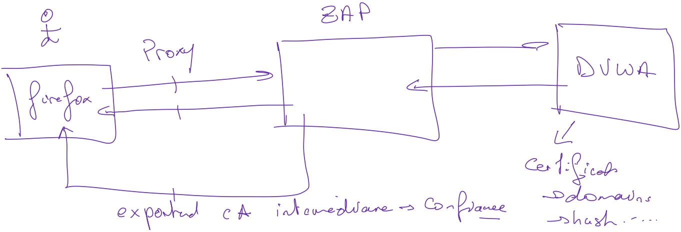
Exo

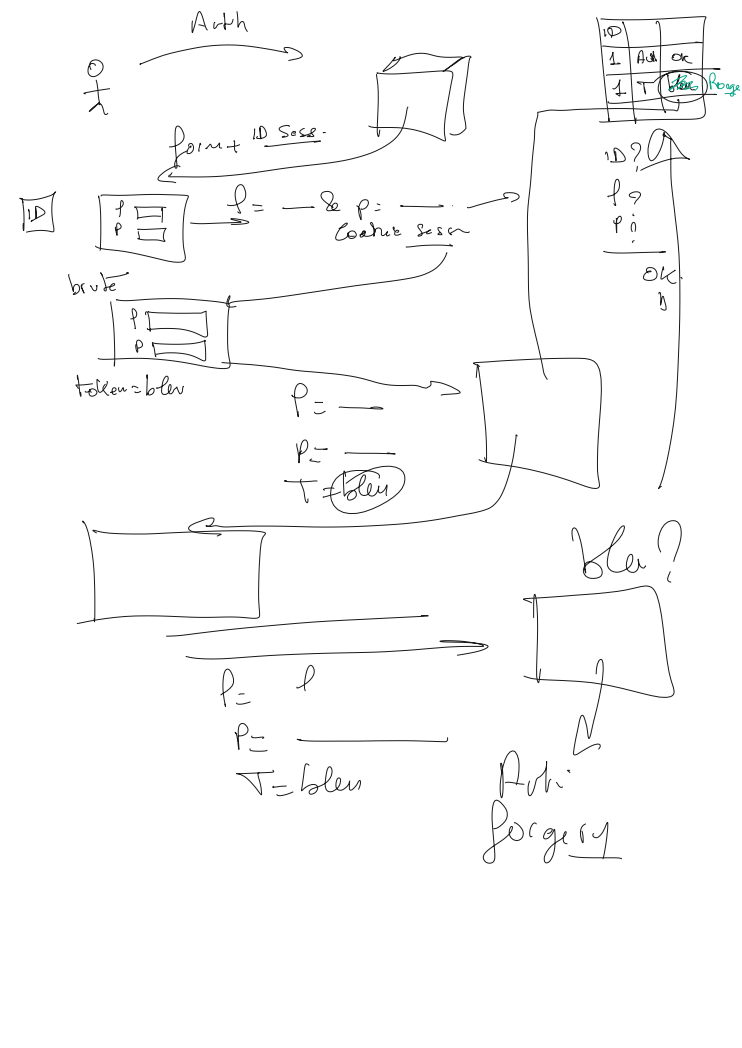


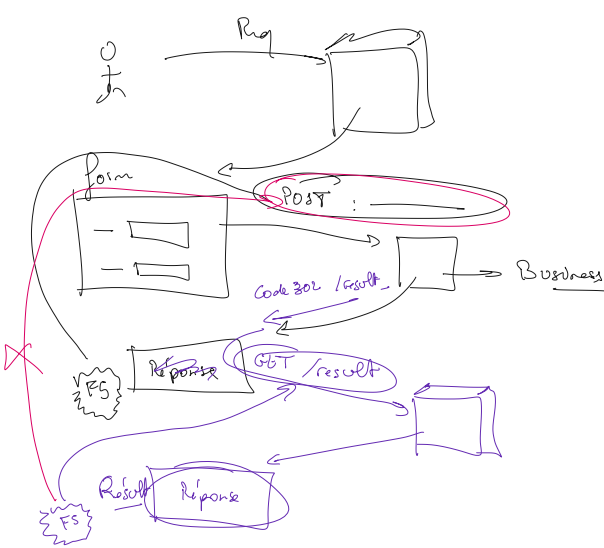

dvwa
form
Submit
Cookies.
ID Session
App

ZAP (client)


App ZAP
URL
Attack
DVWA
- bloquer sur l'auth.


ZAP
Proxy
firefox
DVWA
Certificats
domains
hash . . . .
exported CA intermediaire → confiance


Auth
ID
Auth
OK
1
T
bleu
Forge
point ID Sess.
ID
f
p
f =
& p =
Coeur Sess
ID ?
f ?
p ?
OK
brute
f
p
token = bleu
p =
p =
T = bleu
bleu ?
f =
p =
T = bleu
Auth
forgery


Req
form
POST :
Business
Code 302 /result
GET /result
F5
Réponse
Résult
Réponse
F5

SRC
- php
- dotnet
- java

→ Runtime
- php
- dotnet
- JRE

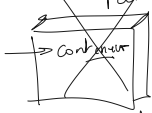
→ 1 Exec. qui embarque le Serveur

image :
- Alpine
- → dotnet (8)
- → App

→ l'image de Votre App

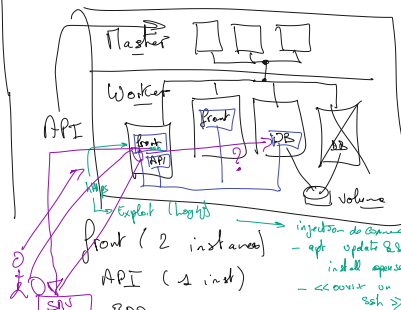
Lancement dotnet run ...

docker / Podman

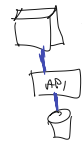


→ DEV ok
→ ! ok Prod

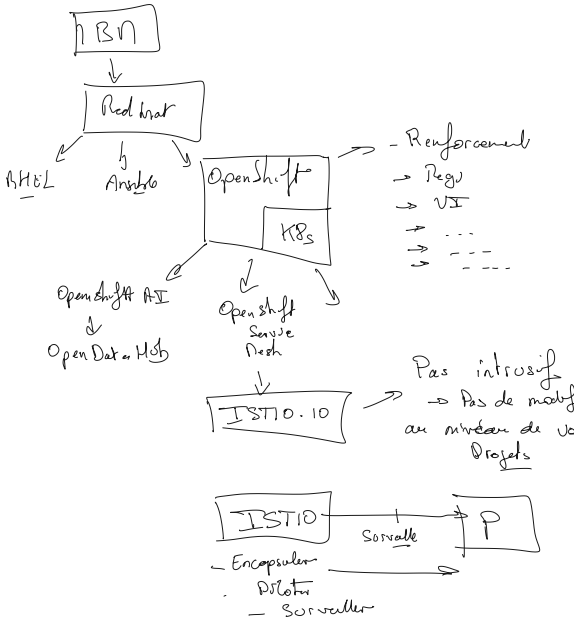
Kubernetes



-ssh> shell



RF = 2
RF = 2
RF = 1



Film Youtube OWASP ZAP : https://www.youtube.com/watch?v=RLIC1Yp5O8Y
Implémentation de OpenShift Service Mesh (istio) : https://www.youtube.com/watch?v=Uo8LEcUMVxg