

# ABC CICD

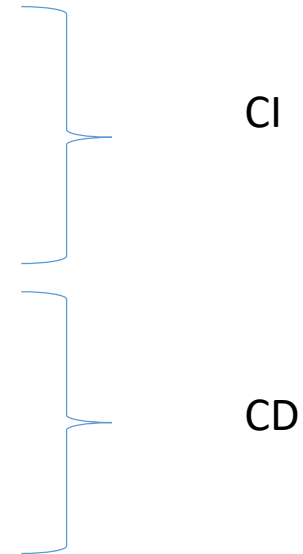
Principes de base

[github.com/gquere](https://github.com/gquere) + [gists](#)  
[errno.fr](http://errno.fr)

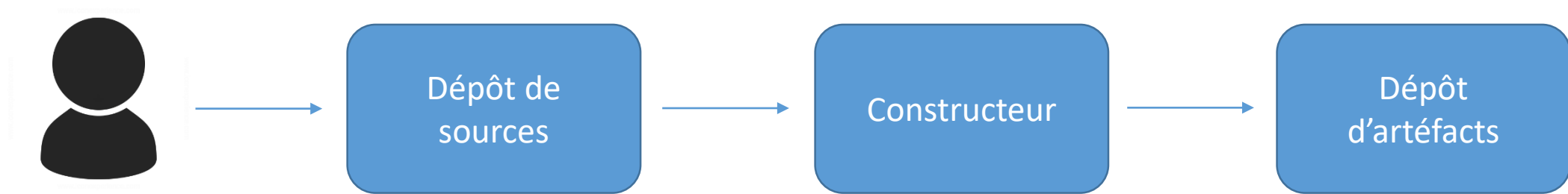


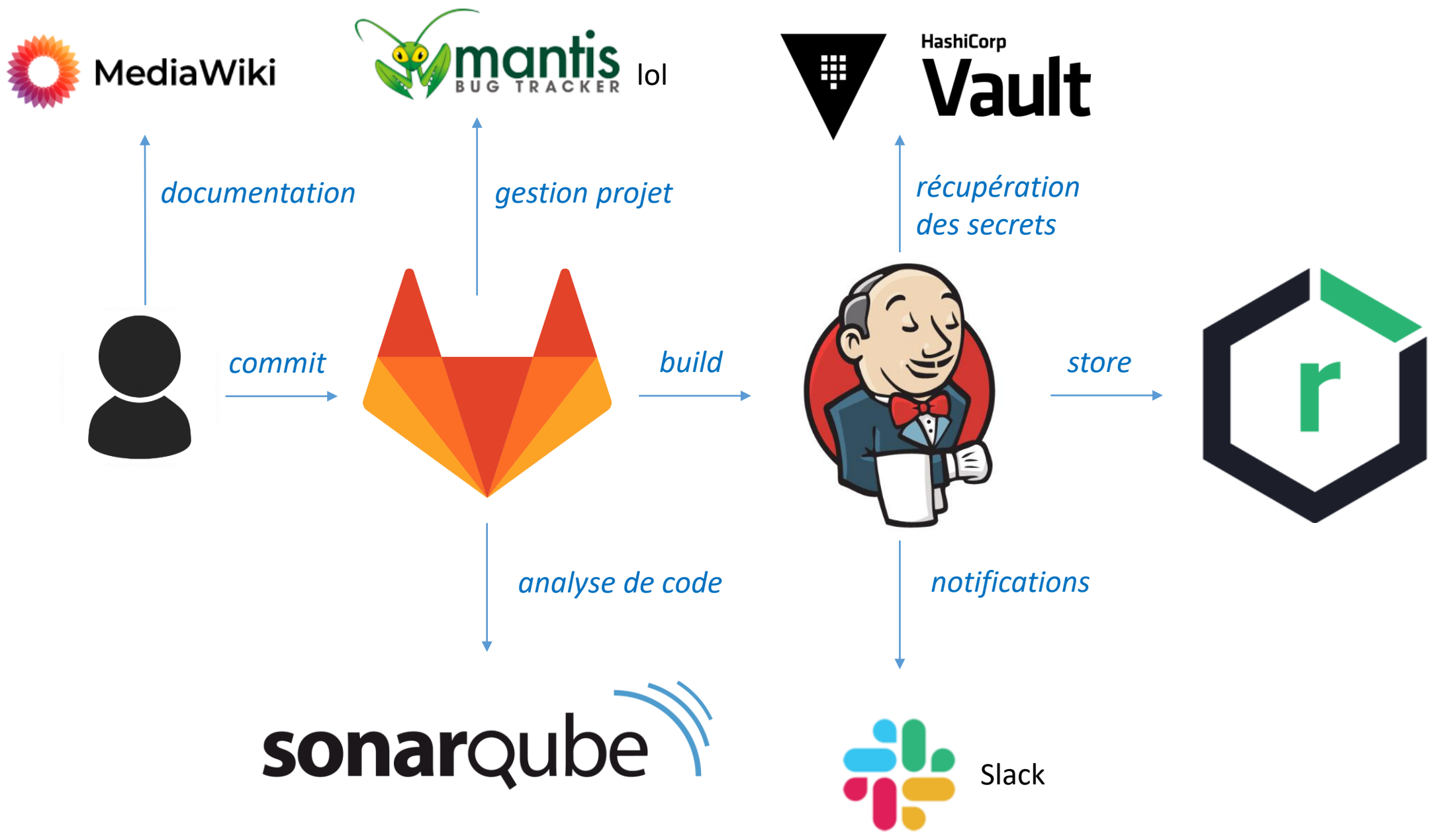
# CICD CEKOI

- Gestion des sources
  - GitHub, BitBucket, GitLab ...
- Gestion des builds
  - Jenkins, Travis, runners GitLab
- Gestion des artéfacts
  - Nexus, Artifactory



# CICD CEKOI



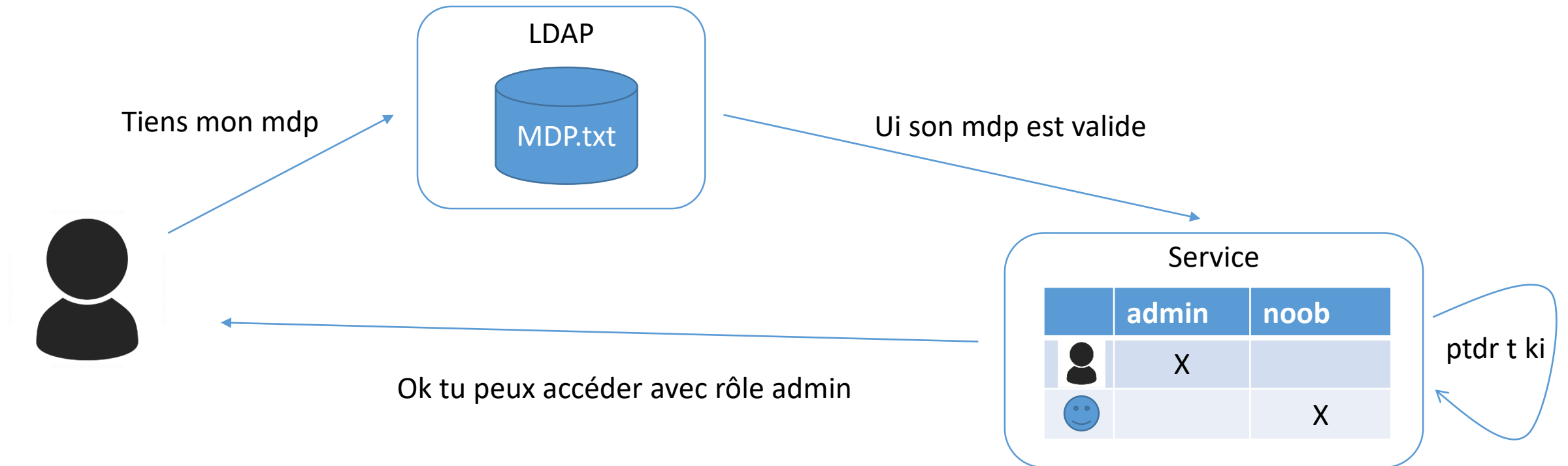


# Pourquoi ?

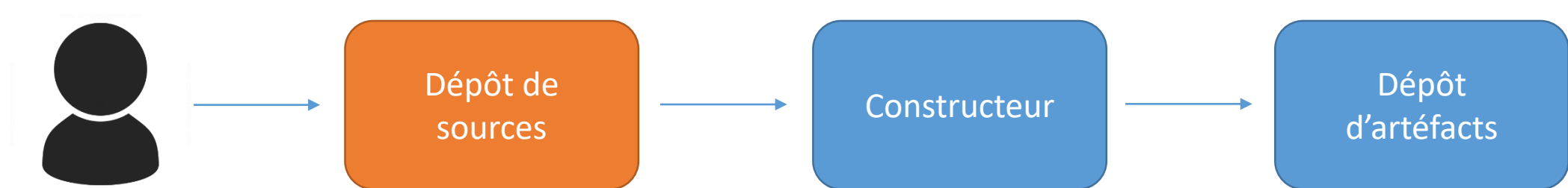
- Incontournable en entreprise
  - Editeur
  - Outils internes
- Audit
- ~~Pentest~~

# Authentication, habilitation

- Authentication = preuve d'identité
- Habilitation = accès conditionnel



# Dépôts de sources



# Vulnérabilités classiques : GitLab



- Dépôts publics
  - Dump de code, recherche de secrets
- Ajout d'utilisateur
- Absence de revue de code
- Absence de signature des commits

**Tip:** rechercher des secrets dans un historique avec `yar`

**Tip:** suivre les travaux de `@vakzz` sur `hackerone`, une RCE GitLab par an



# Exemple de pentest 1h



## GitLab Enterprise Edition

### Open source software to collaborate on code

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

LDAP	Standard	<b>Register</b>
------	----------	-----------------

Full name

Username

Username is available.

Email

Email confirmation

Password

Minimum length is 8 characters

**Register**

# Recherche de secrets

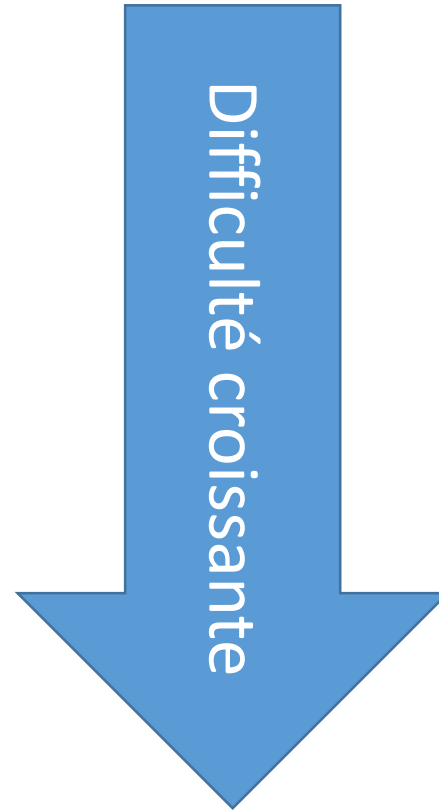
```
://[a-zA-Z0-9_ - ]\+:[^/@]\+@|curl .*-u|wget .*--  
password|wget .*--http-password|wget .*--ftp-  
password|wget .*--proxy-password|echo  
.*|\s*passwd|echo  
.*|\s*chpasswd|Authorization.*:.*Basic|Authorization.*:  
.*Bearer|docker login .*-  
p|<password>[^<]\+</password>|mysql .*-p|mysql .*--  
password|PGPASSWORD|RSYNC_PASSWORD|BEGIN  
.*PRIVATE|[a-zA-Z0-9]7z[ _r].*-p[^ ]|unzip .*-P|mount  
.*-o.*password=|jfrog .*--password=|jfrog .*--  
apiKey=|mongo .*-p|cqlsh .*-p|ldapsearch .*-  
w|ldapsearch .*-y|sshpass|X-Vault-  
Token|secret_id|VAULT_TOKEN|vault login
```

# Recherche de secrets

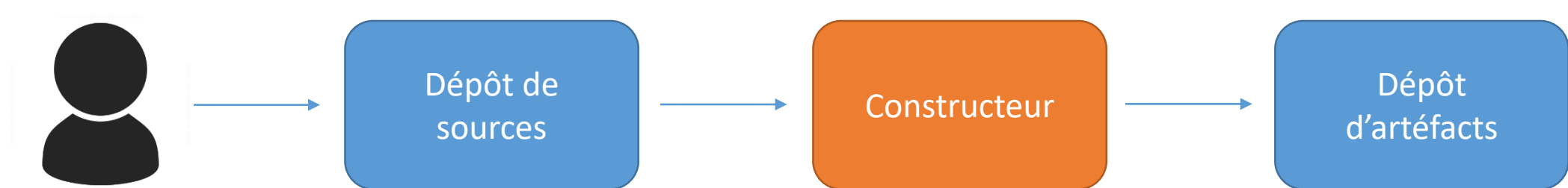


# Défense

- Pas de projets publics
- Habilitations fines
- Hooks pour pas pousser des secrets
- Peer Review systématique
- Signature de commits



# Constructions



# Vulnérabilités classiques : Jenkins

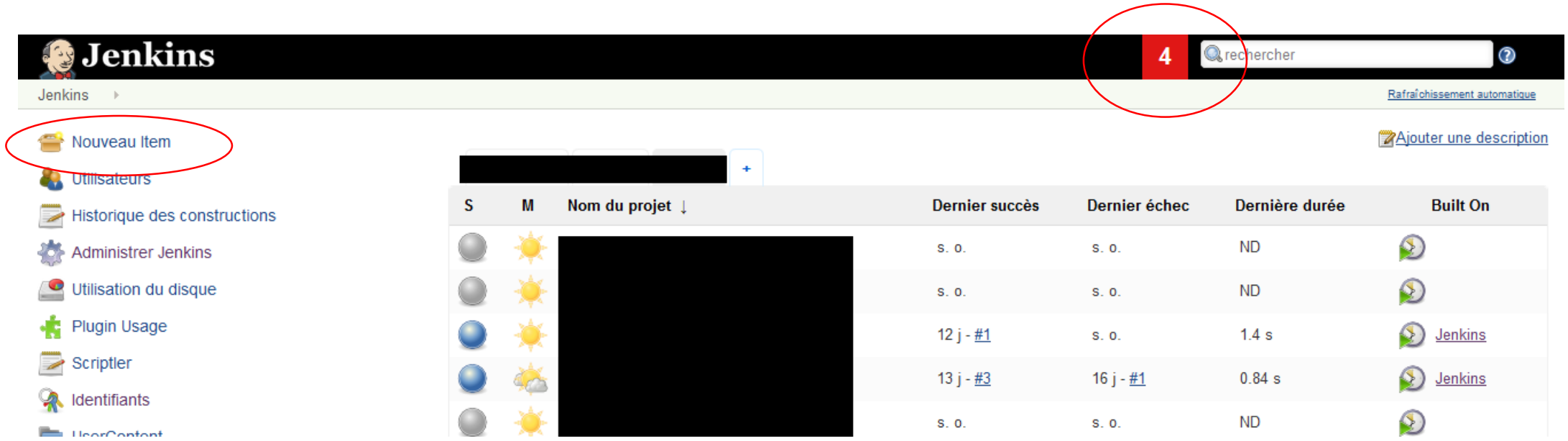


- Absence d'authent
- Absence d'habilitation (create new element, configure job)
- Contient des secrets de build et de déploiement
- Secrets se retrouvent dans les logs de build
  - Dump de logs, recherche de secrets

**Tip** : même sur un Jenkins protégé on peut récupérer la version sur le endpoint /oops

**Tip** : les tokens Jenkins au format `11[0-9a-f]{32}` s'utilisent avec Jenkins-CLI

# Exemple de pentest 1h

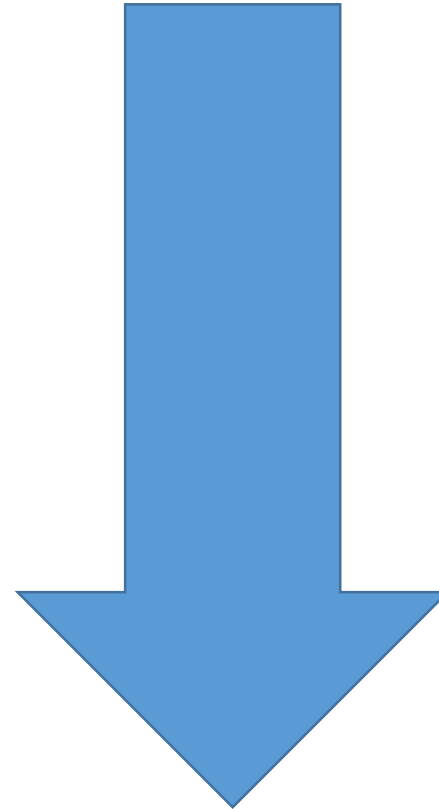


The screenshot shows the Jenkins web interface. At the top, there is a search bar with the text "rechercher" and a red circle around the number "4". Below the search bar, there is a sidebar with several menu items, including "Nouveau Item" which is circled in red. The main content area displays a table of build jobs. The table has columns for "S", "M", "Nom du projet", "Dernier succès", "Dernier échec", "Dernière durée", and "Built On". The "Nom du projet" column is redacted with a black box.

S	M	Nom du projet ↓	Dernier succès	Dernier échec	Dernière durée	Built On
☐	☀	[Redacted]	s. o.	s. o.	ND	
☐	☀	[Redacted]	s. o.	s. o.	ND	
☐	☀	[Redacted]	12 j - #1	s. o.	1.4 s	<a href="#">Jenkins</a>
☐	☀	[Redacted]	13 j - #3	16 j - #1	0.84 s	<a href="#">Jenkins</a>
☐	☀	[Redacted]	s. o.	s. o.	ND	

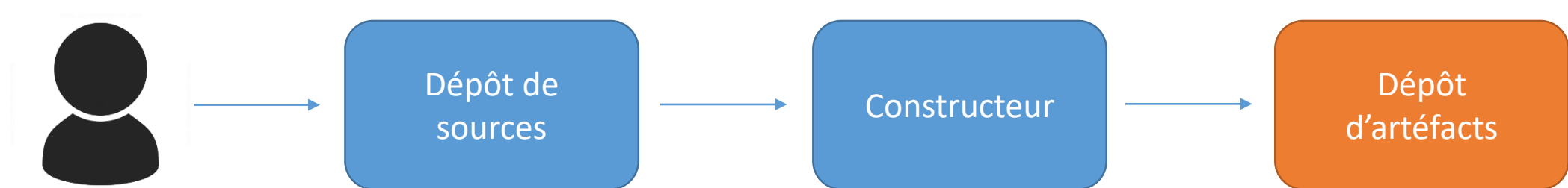
# Défense

- Authentification systématique
- Droits fins
- Plugins de protection
- Durée de vie courte des secrets
- Découplage master/slave
- Configurations stockées dans le git





# Dépôts d'artéfacts



# Vulnérabilités classiques : Artifactory

- Souvent pas d'authent
- Récupérer des artéfacts = récupérer le code
  - Parfois récupérer des secrets
- Ecraser des artéfacts
- Dependency Confusion



**Tip:** il est parfois possible de déployer avec l'utilisateur anonyme

**Tip:** le mot de passe de access-admin est gardé sur disque après un déploiement

# Défense

- Authentification systématique
- Habilitation
  - Comptes d'écriture
  - Comptes de lecture
- Envoi des logs au SIEM
  - Accès des comptes techniques à l'IHM
  - Téléchargement en masse d'artéfacts
  - Artéfact écrasé
- Bien lire la doc
  - Options pour se protéger des confusions
- Signer les paquets

