# A3:2017-Sensitive Data Exposure

# Fuite d’informations sensibles dans la gestion de configuration

# Informations sensibles?

- Mot de passe
- Clé privée/Certificat

# Et c’est une problème?

## What Happened When I Leaked My Server Password on GitHub.com

June 10, 2020 By Craig Hays Leave a Comment

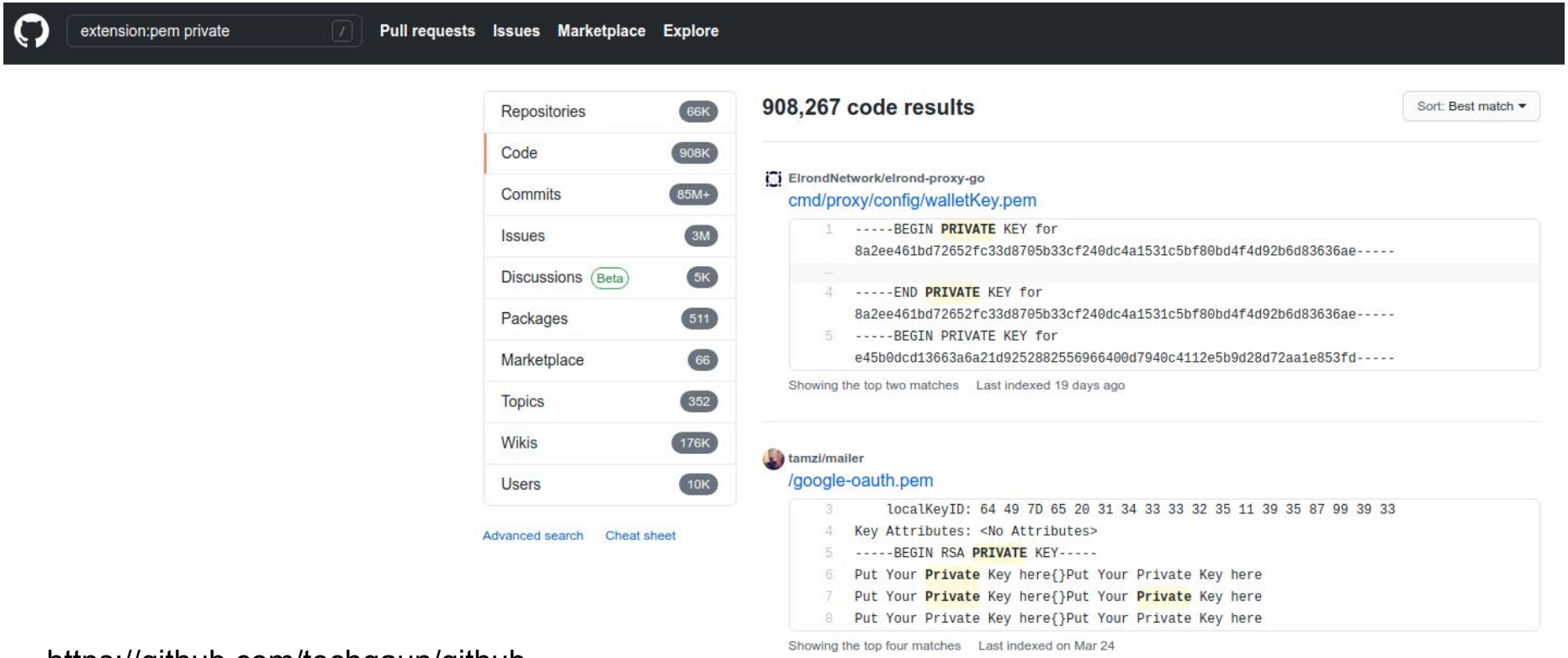
—

Reading Time: 7 minutes

*I deployed a honeypot and ‘accidentally’ leaked a valid SSH username and password into a GitHub repository. This is what happened over the next 24 hours.*

# Retrieving secrets

# Github dorks




https://github.com/techgaun/github-dorks

# API

Exemple avec l’API Gitlab:

Récupérer tous les id des projets disponibles: **GET /projects**

Récupérer tous les id des commits de chaque projet: **GET /projects/:id/repository/commits**

Récupérer le contenu du commit: **GET /projects/:id/repository/commits/:sha/diff**

**grep -i 'password|PRIVATE|...'**

# Comment s’en prémunir?

# gitleaks

```
yvan@yvan-XPS-13-9360:~/tmp/gitleaks$ ~/go/bin/gitleaks -v --debug --branch=master --path=. --config-path=gitleaks.toml
INFO[0000] opening .
{
        "line": "    - password: 3P]Rw*~?MT",
        "lineNumber": 3,
        "offender": "password: 3P]Rw*~?MT",
        "offenderEntropy": -1,
        "commit": "c65b09b125abedc039231bac92611fd651ab02b1",
        "repo": ".",
        "repoURL": "",
        "leakURL": "",
        "rule": "Env Var",
        "commitMessage": "Initial commit\n",
        "author": "Cotonne",
        "email": "cotonne@users.noreply.github.com",
        "file": "config.yml",
        "date": "2021-05-10T13:57:23+02:00",
        "tags": ""
}
INFO[0000] scan time: 1 millisecond 814 microseconds
INFO[0000] commits scanned: 2
WARN[0000] leaks found: 1
```

Peut être ajouté à git hooks pre-commit

# Génération de mot de passe à la volée

## Exemple avec Kubernetes

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: secret-env-pod
spec:
  containers:
  - name: mycontainer
    image: redis
    env:
      - name: SECRET_USERNAME
        valueFrom:
          secretKeyRef:
            name: mysecret
            key: username
      - name: SECRET_PASSWORD
        valueFrom:
          secretKeyRef:
            name: mysecret
            key: password
  restartPolicy: Never
```