# Git those passwords out your repos! Detecting leaked secrets at scale

Daniel Oates-Lee

# #> whoami

Daniel Oates-Lee

DevSecOps Engineer and director of Punk Security

- DevSecOps enthusiast
- Terraform
- Security guy
- Geek

# #> whoarewe

Punk Security

- DevSecOps consultancy
- 4 x Opensource tools


- Home of the DevSecOps CTF

# content

- What is the problem
- Secrets leak types
- What can go wrong
- How can we defend
- secretMagpie

# What is the problem?

A secret is publicly accessible

a. Should be, but too many permission

b. Shouldn’t be

# What is the problem?

A secret is not managed correctly and is then:

a. Written to a log or trace output
b. Used to elevate privilege
c. Used by an individual to gain access

# What is the problem?

Types of hardcoded secrets

- passwords
- api keys
- tokens
- private certificates/keys

# What is the problem?

- Where can it exist?
  - Files

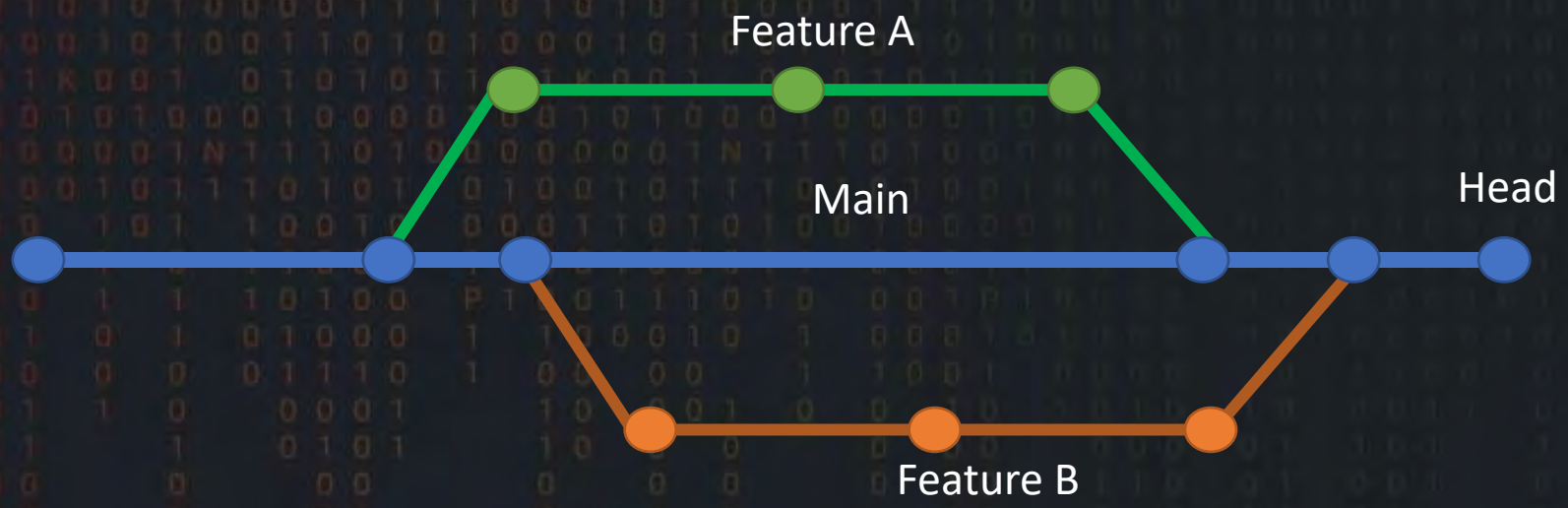
# What is the problem?

Where can it exist?

- Files
- GIT messages or history

# What can go wrong?

# What can go wrong?

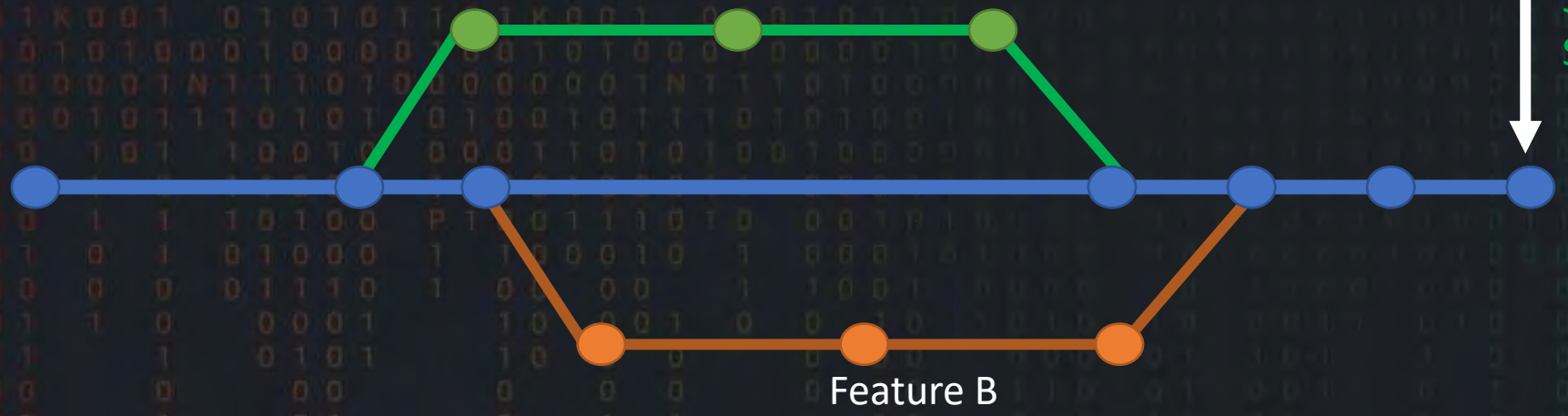


# What can go wrong?

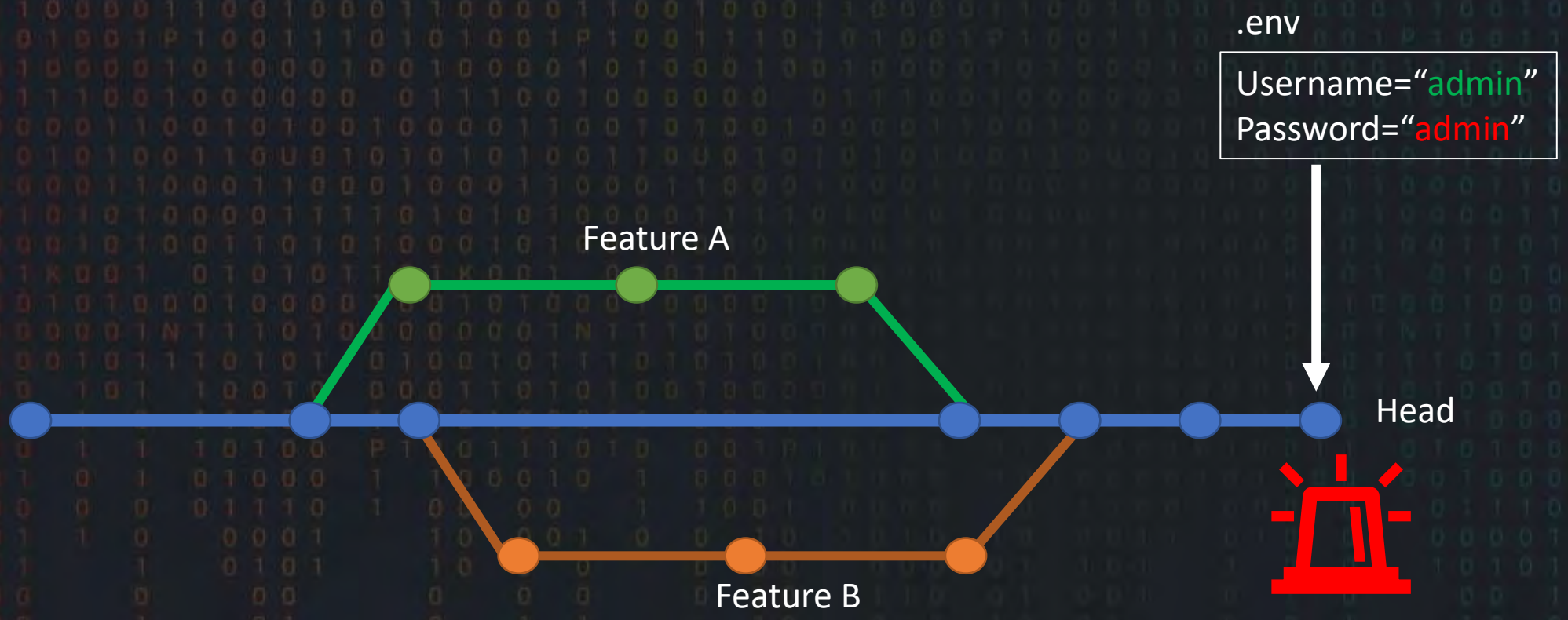
.env

```
Username="admin"
Password="admin"
```

```
$ git commit  -m "add creds"
$ git push
```



# What can go wrong?

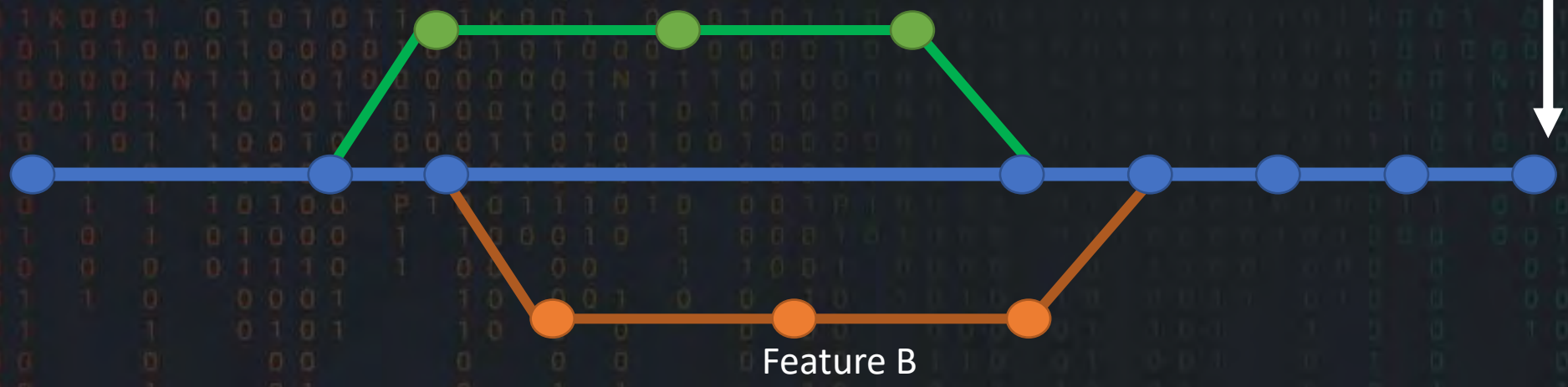


# What can go wrong?

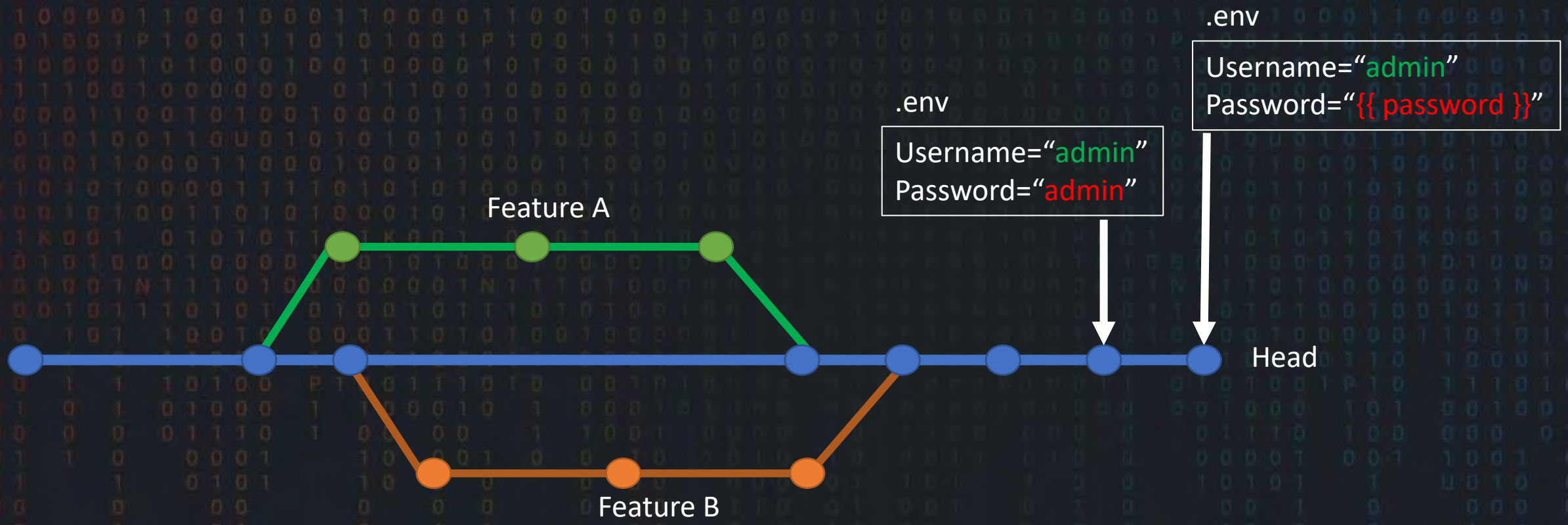
.env

```
Username="admin"
Password="{{ password }}"
```

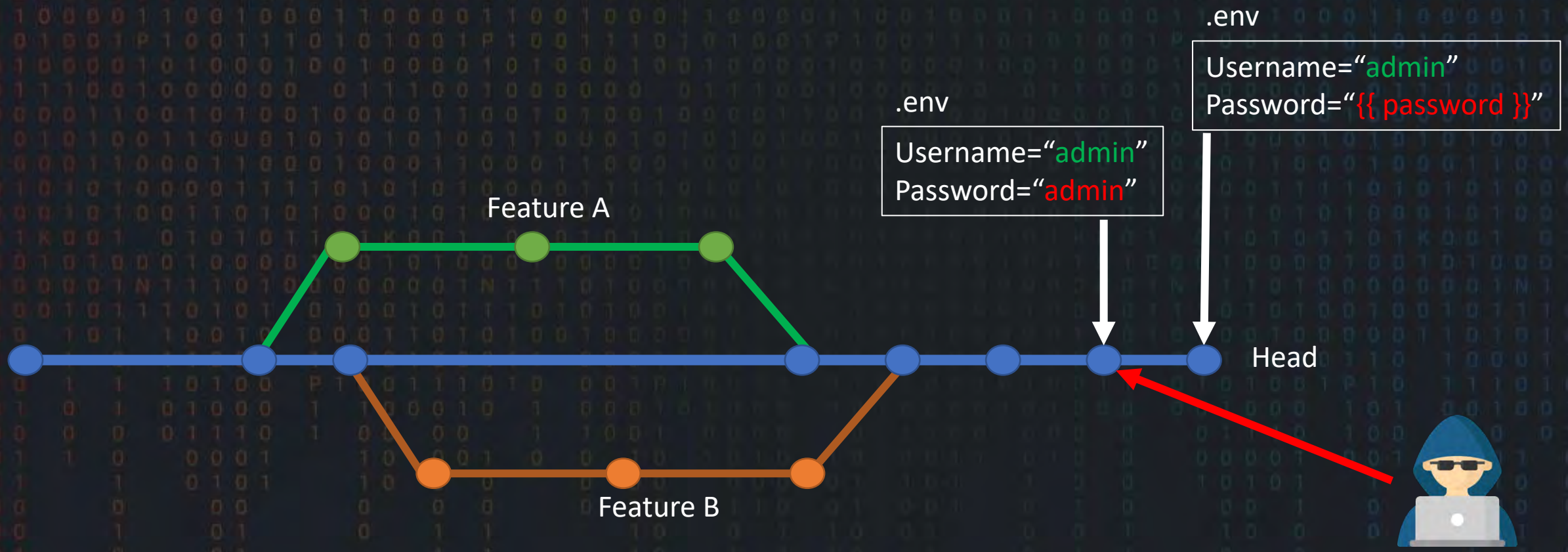
$ git commit -m "removed password"
$ git push



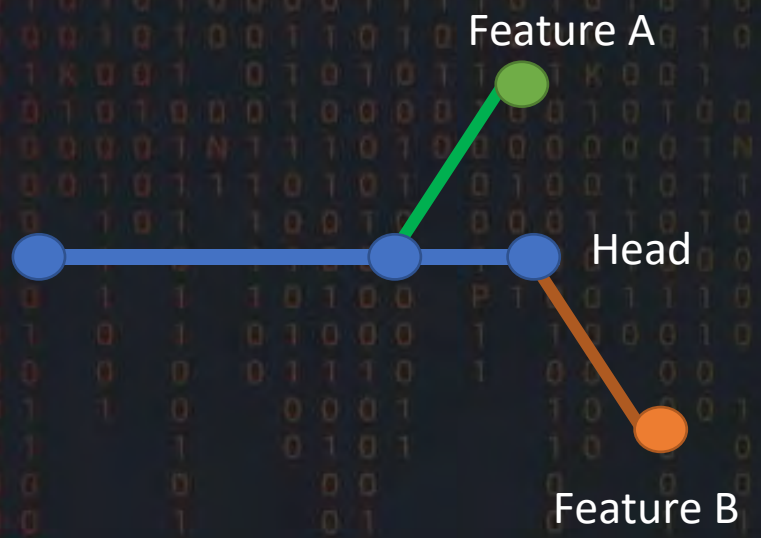
# What can go wrong?



# What can go wrong?



# What can go wrong?

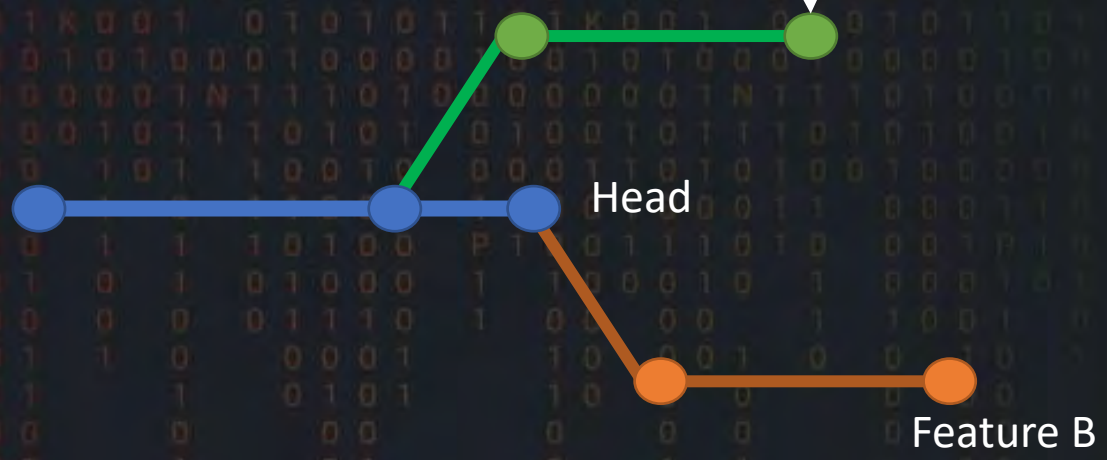


# What can go wrong?

.env

```
Username="admin"
Password="admin"
```

$ git commit -m "add creds"
$ git push

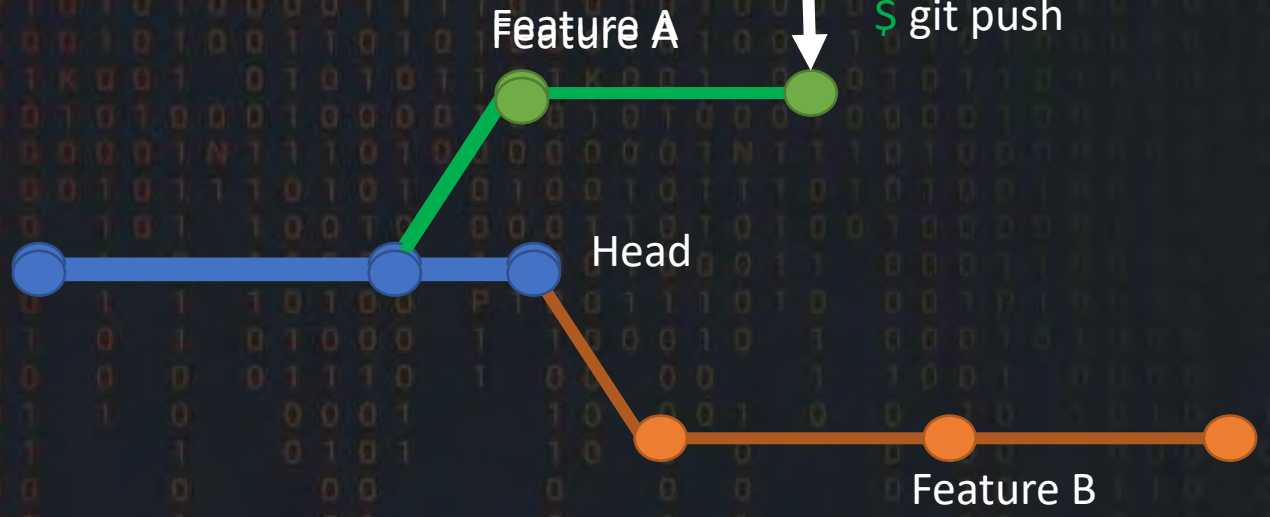


# What can go wrong?

.env

```
Username="admin"
Password="admin"
```

```
$ git commit  -m "add creds"
$ git push
```

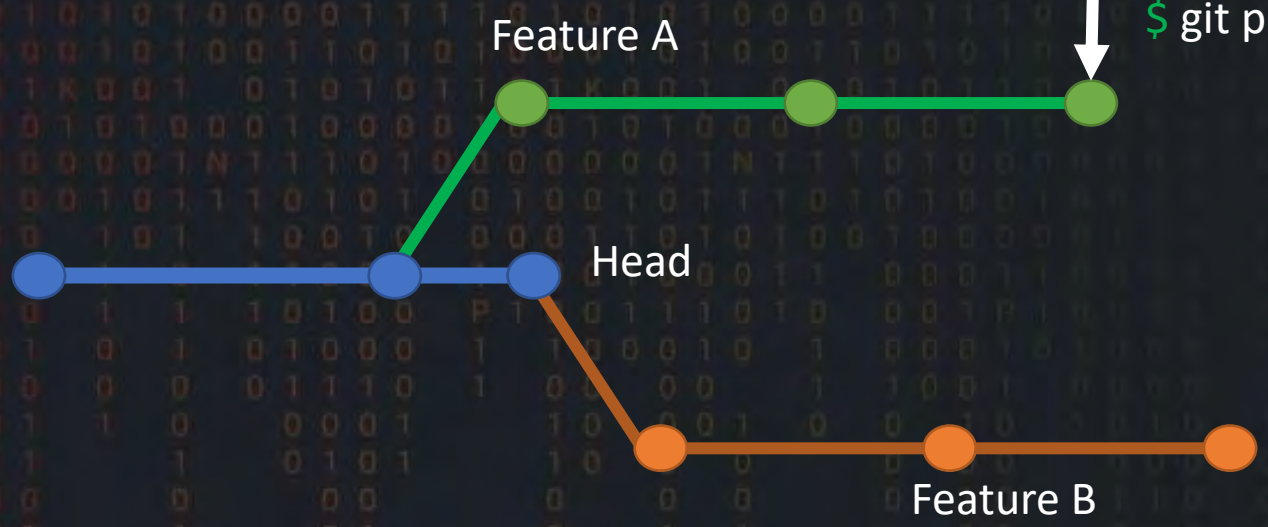


# What can go wrong?

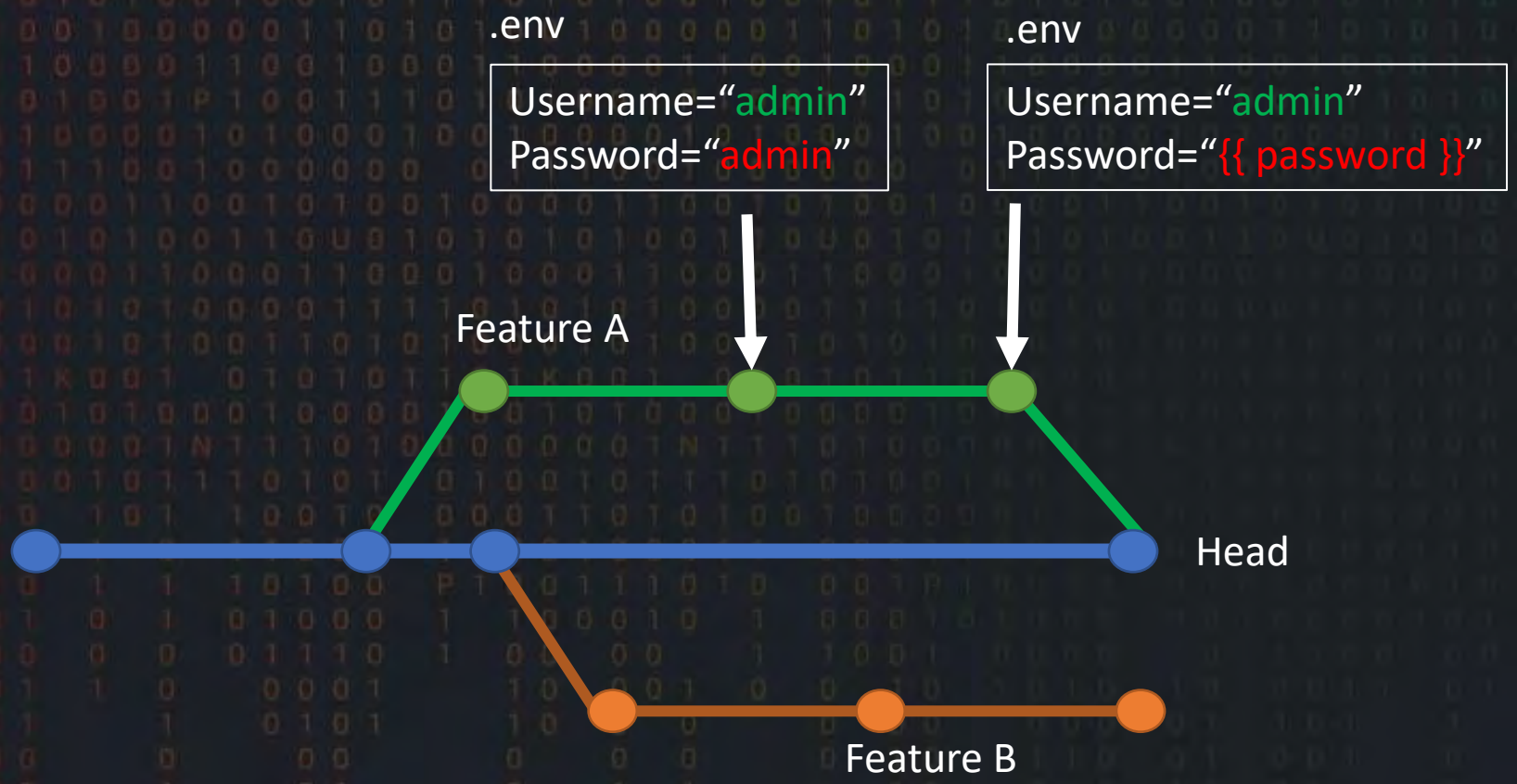
.env

```
Username="admin"
Password="{{ password }}"
```

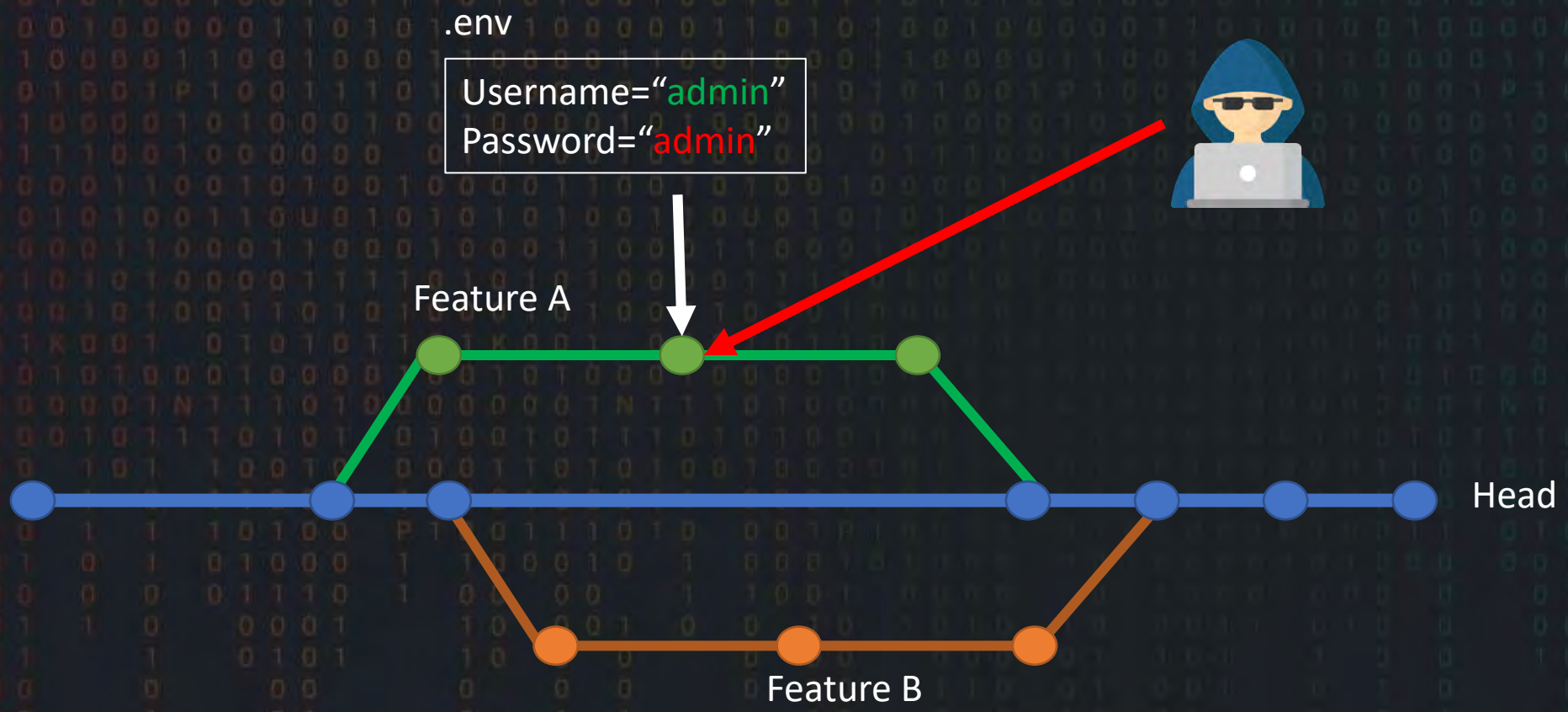
$ git commit  -m "removed password"
$ git push



# What can go wrong?



# What can go wrong?



# How do we defend?

- DevSecOps
  - Secret Scanning tools

# How do we defend?

- DevSecOps
- Findings and rotation
  - Record/ticket
  - Rotation of secret
  - Training
  - RED team Manual verification checks

# How do we defend?

- DevSecOps
  - Secret management
    - Secrets Vaults
    - Log access to secrets
    - Rotate regularly
    - Encryption

# secretMagpie?

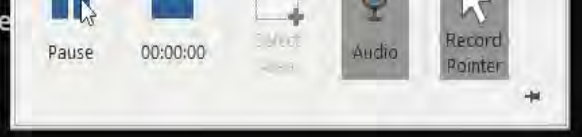
- Pre-secret scanning
- CI pipeline or manual tool
- Two secret scanners
- Easy to read output

https://github.com/punk-security/secret-magpie-cli

# secretMagpie?


https://github.com/punk-security/secret-magpie-cli

```
PS C:\Users\DanielOates-Lee> docker run -it punksecurity/secre
```



Import statuses from CSV: Browse...

Download as: CSV

Search...

*Made by Punk Security*

Action: Confirmed as Rotated Go 0 out of 455 selected

Reset False Positive List

| Repository | Commit | File | Short Secret | Hashed Secret | Status |
|---|---|---|---|---|---|
| wrongsecrets | 42e63b0756f... | Dockerfile.web | 1.6.5-no-vault | 58faad65fe965a0ae5bc0... | New |
| wrongsecrets | 42e63b0756f... | azure/k8s/secret-challenge-v | 1.6.5-k8s-vault | 00290866979a4c0a13d1... | New |
| wrongsecrets | 42e63b0756f... | aws/k8s/secret-challenge-vau | 1.6.5-k8s-vault | 00290866979a4c0a13d1... | New |
| wrongsecrets | 42e63b0756f... | k8s/secret-challenge-deployr | 1.6.5-no-vault | 58faad65fe965a0ae5bc0... | New |
| wrongsecrets | 42e63b0756f... | gcp/k8s/secret-challenge-vau | 1.6.5-k8s-vault | 00290866979a4c0a13d1... | New |
| wrongsecrets | 42e63b0756f... | k8s/secret-challenge-vault-de | 1.6.5-k8s-vault | 00290866979a4c0a13d1... | New |
| wrongsecrets | 42e63b0756f... | okteto/k8s/secret-challenge- | 1.6.5-no-vault | 58faad65fe965a0ae5bc0... | New |
| wrongsecrets | 42e63b0756f... | okteto/k8s/secret-challenge- | 1.6.5-no-vault | 58faad65fe965a0ae5bc0... | New |
| wrongsecrets | e1933c82f8f1... | aws/k8s/secret-challenge-vau | 1.6.5RC2-k8s-vault | ef27dafceed6ada042872... | New |
| wrongsecrets | e1933c82f8f1... | Dockerfile.web | 1.6.5RC2-no-vault | a8037015554e3a3ca4c1... | New |
| wrongsecrets | e1933c82f8f1... | gcp/k8s/secret-challenge-vau | 1.6.5RC2-k8s-vault | ef27dafceed6ada042872... | New |
| wrongsecrets | e1933c82f8f1... | k8s/secret-challenge-vault-de | 1.6.5RC2-k8s-vault | ef27dafceed6ada042872... | New |
| wrongsecrets | e1933c82f8f1... | azure/k8s/secret-challenge-v | 1.6.5RC2-k8s-vault | ef27dafceed6ada042872... | New |
| wrongsecrets | e1933c82f8f1... | k8s/secret-challenge-deployr | 1.6.5RC2-no-vault | a8037015554e3a3ca4c1... | New |
| wrongsecrets | e1933c82f8f1... | okteto/k8s/secret-challenge- | 1.6.5RC2-no-vault | a8037015554e3a3ca4c1... | New |

## Filter

Clear All Filters

### By Status

All

New (455)

### By Repository

All

wrongsecrets (455)

### By Type

All

generic-api-key (442)

AWS (5)

private-key (4)

aws-access-token (3)

PrivateKey (1)

### By Filename

All

secret-challenge-vault-deployment.yml (128)

secret-challenge-vault-deployment.yml.tpl (111)

Dockerfile.web (83)

secret-challenge-deployment.yml (74)

README.md (23)

secret-challenge-ctf-deployment.yml (11)

Challenge15.java (7)

Import statuses from CSV: Browse...

Download as: CSV

Search...

*Made by Punk Security*

Action: Confirmed as Rotated Go 0 out of 5 selected

Reset False Positive List

| Repository | Commit | File | Short Secret | Hashed Secret | Stat |
|---|---|---|---|---|---|
| wrongsecrets | 43d6429098e... | src/main/resources/explanati | AKIASP2TPHJS6R72AFU2 | 71fdf4b5a3451558e3de0... | Nev |
| wrongsecrets | 43d6429098e... | src/main/resources/explanati | AKIASP2TPHJS4XUU3EPJ | 50185f7cd3f434fd2bdeb... | Nev |
| wrongsecrets | 2c2c0b12312... | src/main/java/org/owasp/wrc | AKIAYVP4CIPPEMEC27B2 | 438ecefcc3955931f3171f... | Nev |
| wrongsecrets | 2c2c0b12312... | src/main/java/org/owasp/wrc | AKIAYVP4CIPPJCJOPJWL | 8503ffb1bd3e5eb7bd5c... | Nev |
| wrongsecrets | 2c2c0b12312... | src/main/java/org/owasp/wrc | AKIAYVP4CIPPCXOWVNMW | ad3df8eb9fffa8cb0b84af... | Nev |

## Filter

Clear All Filters

### By Status

All

New (5)

### By Repository

All

wrongsecrets (5)

### By Type

All

AWS (5)

### By Filename

All

Challenge15.java (3)

challenge15.adoc (2)

### By Extension

All

java (3)

adoc (2)

### By Hashed Secret

All

ad3df8eb9fffa8cb0b84afae7f82f10b47078199913cc4679ef6741a8f46f496 (1)

8503ffb1bd3e5eb7bd5cd7282cf645aa8d273ba4188e4198ac7b31d3bdf64f66 (1)

438ecefcc3955931f3171f1072a27809b22684c

## Git history

One of the mistakes we often make when we do commit secrets to Git, is trying to get rid of them without rotating the secret. What makes it worse, is that without properly overriding the commit with the secret and/or removing the commit, it will remain in history forever.

So, we kept some AWS access-keys in git as a "mistake", can you find them?

Note: the answer contains one of the 3 aws credential profiles you find in a commit its java comments, but then without the java comment markup as a single line. Alternatively you can just provide the secret access key with we are looking for.

Note-2: Did you know that these are working access keys[1]?! Go to stats when you tried them to find out more!

aws_access_key_id=AKIASP2TPHJS6R72AFU2 aws_secret_access_key=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 region=us-east-2 output=json

#https://canarytokens.org/manage?token=cs07k832u9t1u4npowbvsw4mb&auth=7f75f2b2a4207c91fbc1ea59f7a495eb

aws_access_key_id=AKIASP2TPHJS6R72AFU2aws_secret_access_key=tpRLTDr0/PTZtUkS1rCUeWzQvknekDIpe4U3cxbv

aws_access_key_id=AKIASP2TPHJS4XUU3EPJ aws_secret_access_key=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 region=us-east-2 output=json

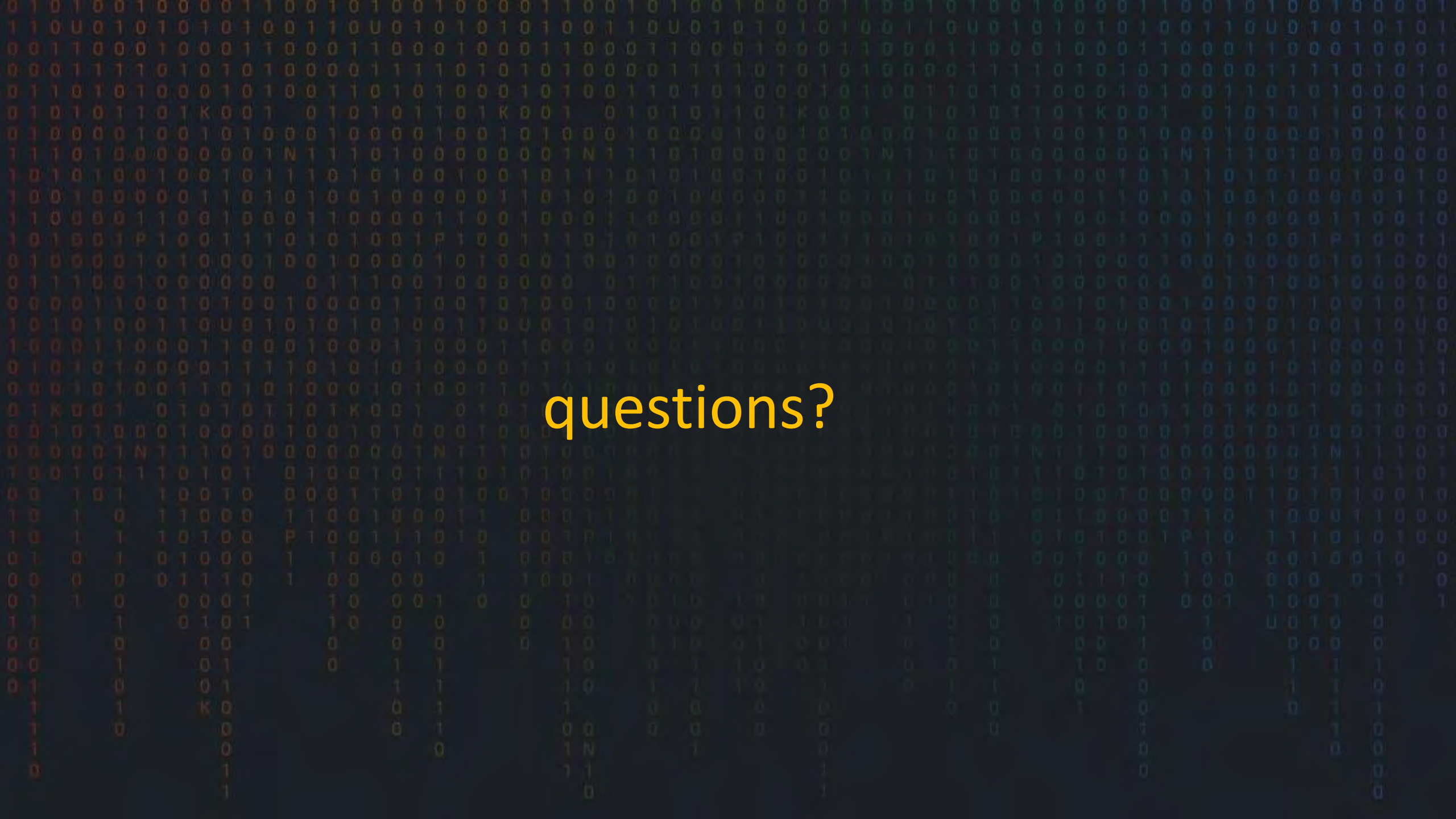
#https://canarytokens.org/manage?token=n0cnd92mavmv1m61tjmyj9of5&auth=6519be82ef910868529091527c3edb3f

aws_access_key_id=AKIASP2TPHJS4XUU3EPJaws_secret_access_key=CU0oKt4Gt1lHDtJjnRLfdBUZWadmYIHevq/TyUz/

https://wrongsecrets-commjoen.cloud.okteto.net/canaries/tokencallbackdebug

---

1. They are not "normal" AWS access keys: they are canary tokens! Though you can do `aws sts get-caller-identity` with them. When you use them, some of your data (IP/agent) is being logged.


questions?

# Punk Security

Automating quality and security checks