LATERAL SECURITY

A Pentester's Guide to Automating Security

Benjamin Kearns – Technical Team Leader

www.lateralsecurity.com

Background

#whoami

WHO WE ARE

COMPANY

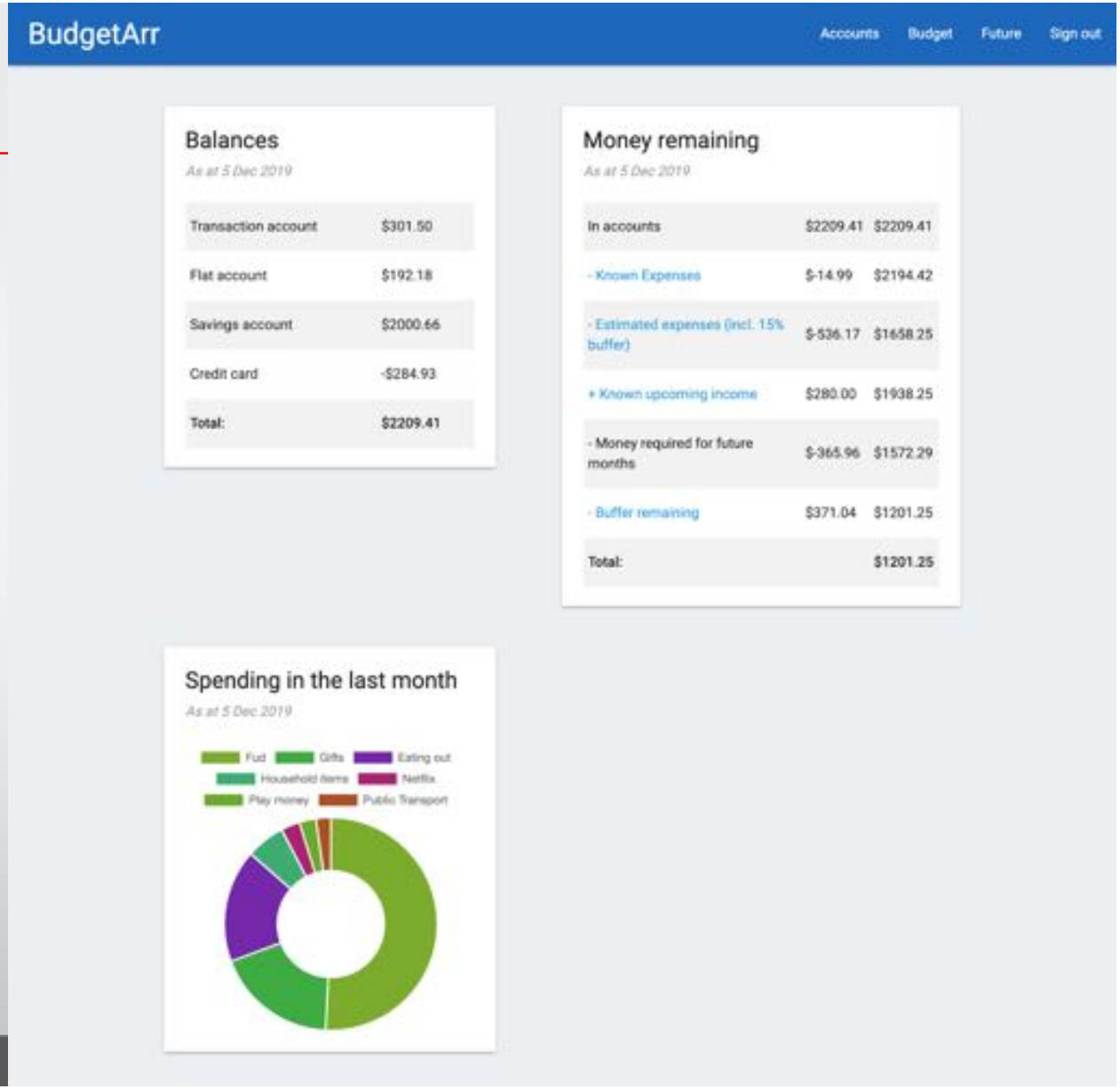
- Founded in 2008
- Directors – Nick von Dadelszen & Ratu Mason
- Offices – Wellington, Auckland, Christchurch
- Staff – 25

SERVICES

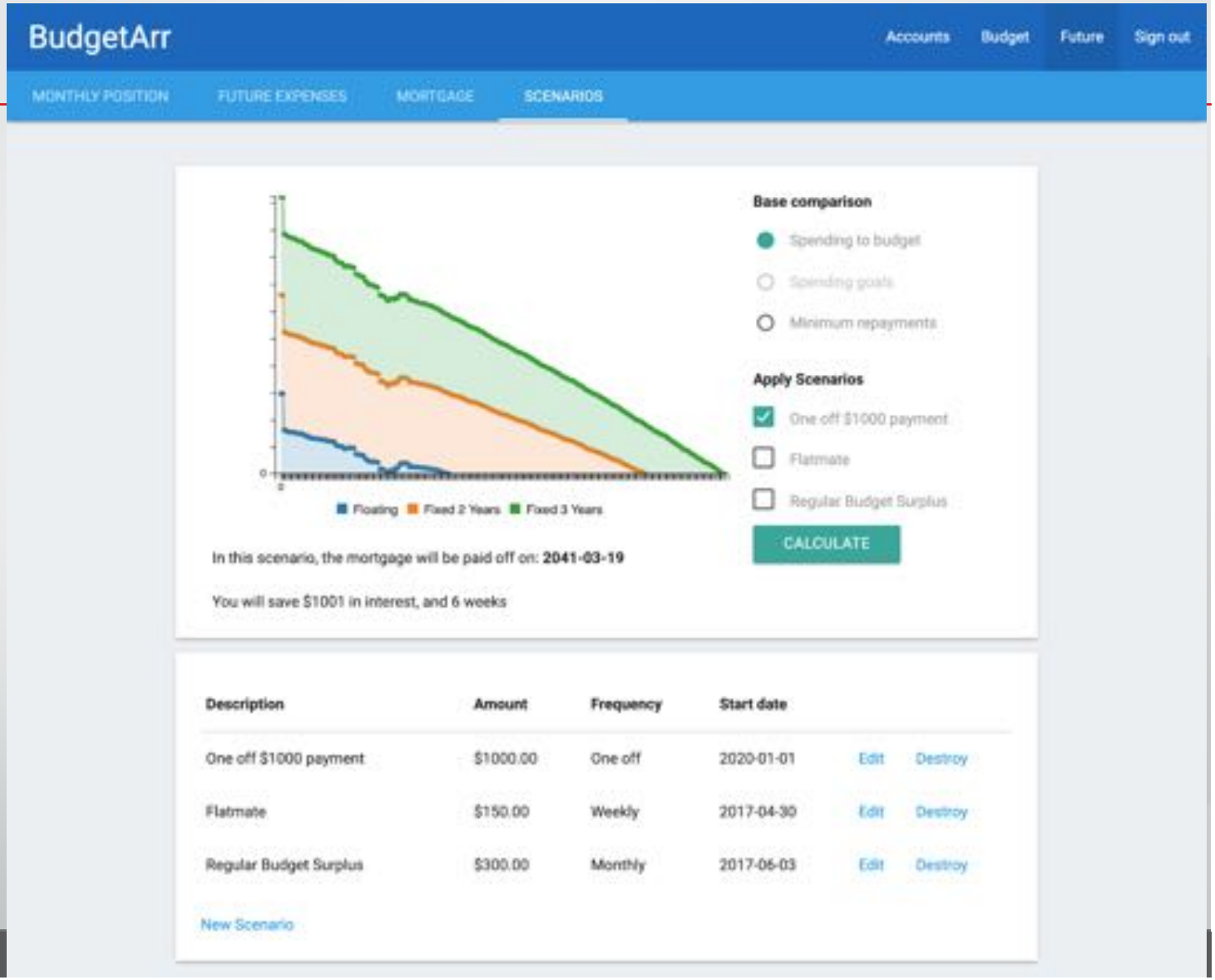
- Advisory Consulting
- Security Testing
- Managed Services
- Incident Response & Forensics
- Training Services

More details @ www.lateralsecurity.com/services

Starting State



Starting State



This Talk

STATIC ANALYSIS

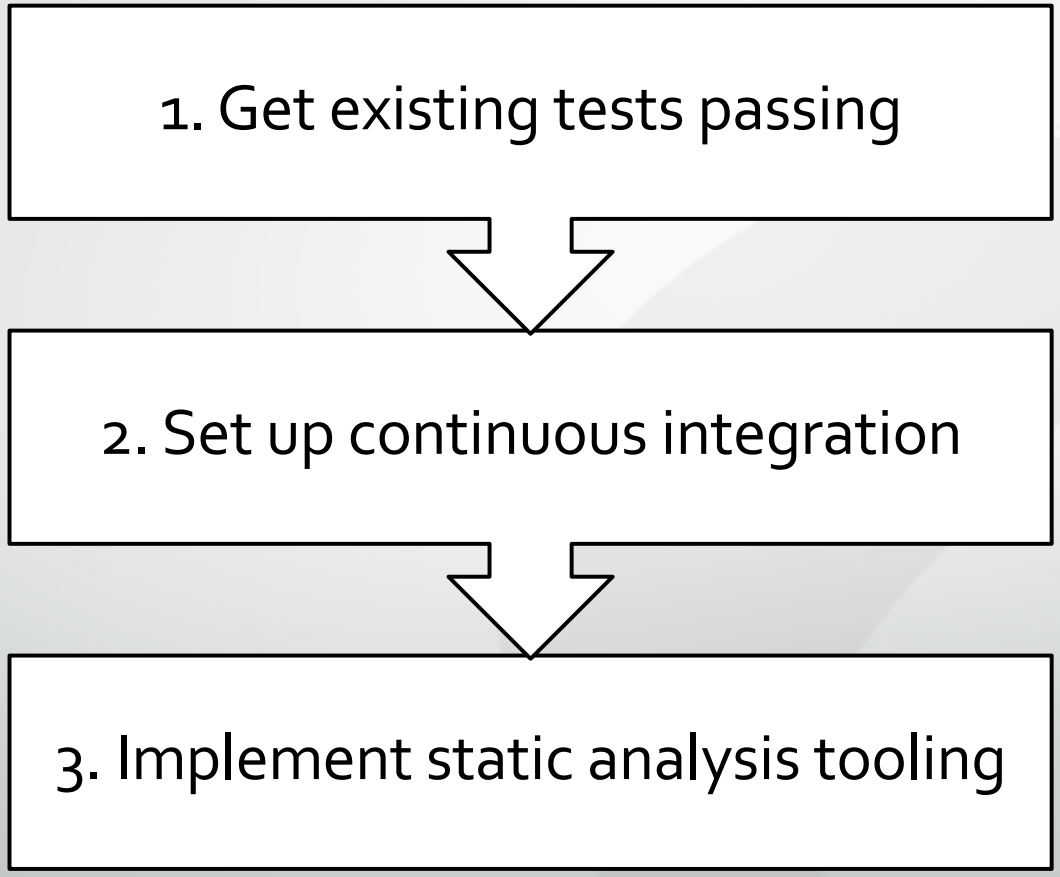
DYNAMIC TESTING

UNIT TESTS

INFRASTRUCTURE

Static Analysis

Static Analysis



Setting up Continuous Integration

Defining Static Analysis Tests

Gemfile:

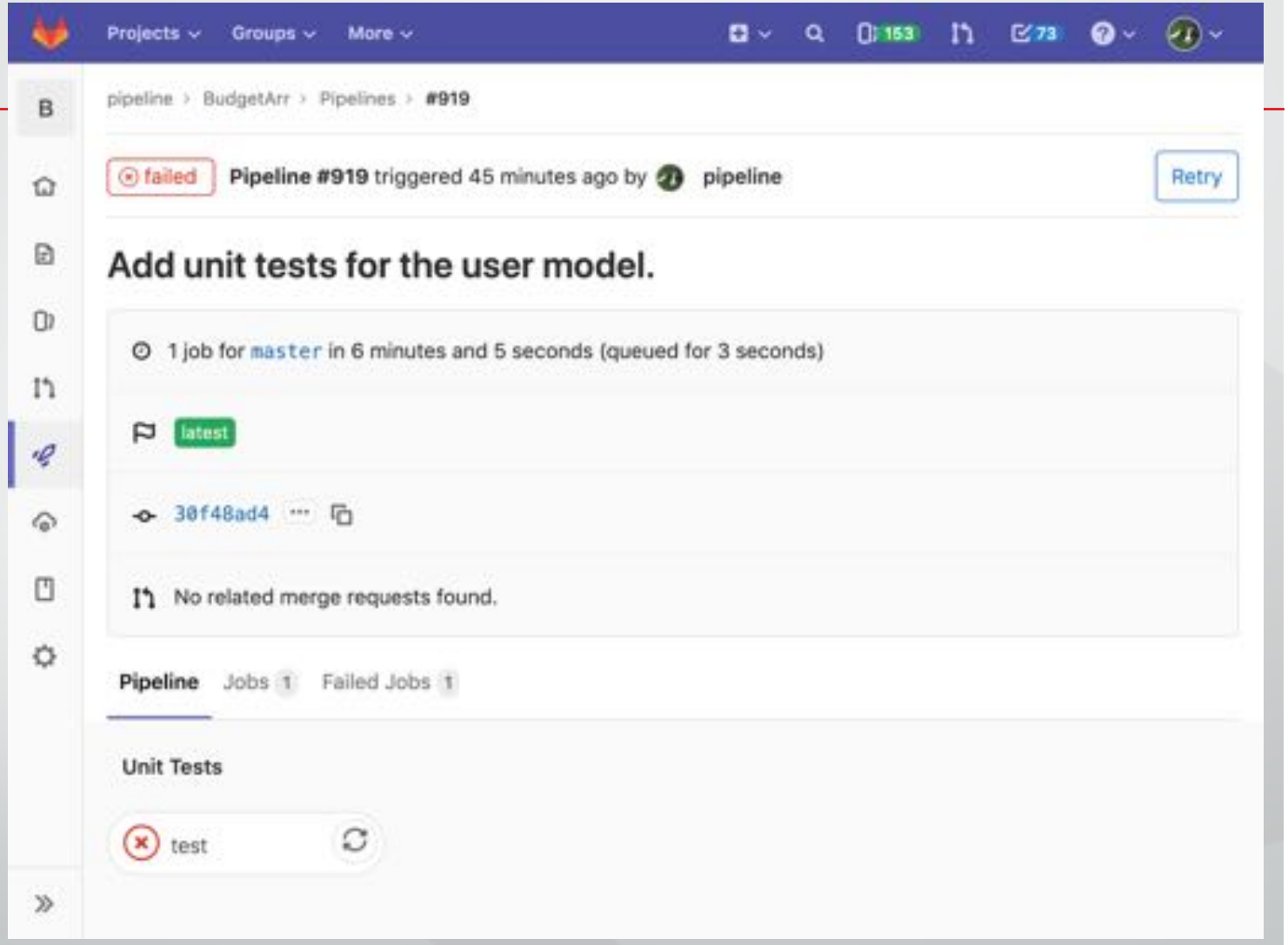
```
group :development, :test do
 gem 'brakeman', require: false
 gem ‘bundle-audit', require: false
end
```

Defining Static Analysis Tests

.gitlab-ci.yml:

```
test:
 stage: Unit Tests
 image: ruby:2.6
 script:
 - bundle install --path vendor
 - bundle exec rake db:create RAILS_ENV=test
 - bundle exec rake test
 - bundle exec brakeman -o brakeman.html
 - bundle exec bundle-audit check –update


 artifacts:
   when: always
   paths:
     - brakeman.html
```

Tests


Projects
Groups
More
153
73
pipeline › BudgetArr › Pipelines › #919
failed
Pipeline #919 triggered 45 minutes ago by pipeline
Retry
Add unit tests for the user model.
1 job for master in 6 minutes and 5 seconds (queued for 3 seconds)
latest
30f48ad4
No related merge requests found.
Pipeline
Jobs 1
Failed Jobs 1
Unit Tests
test

Brakeman

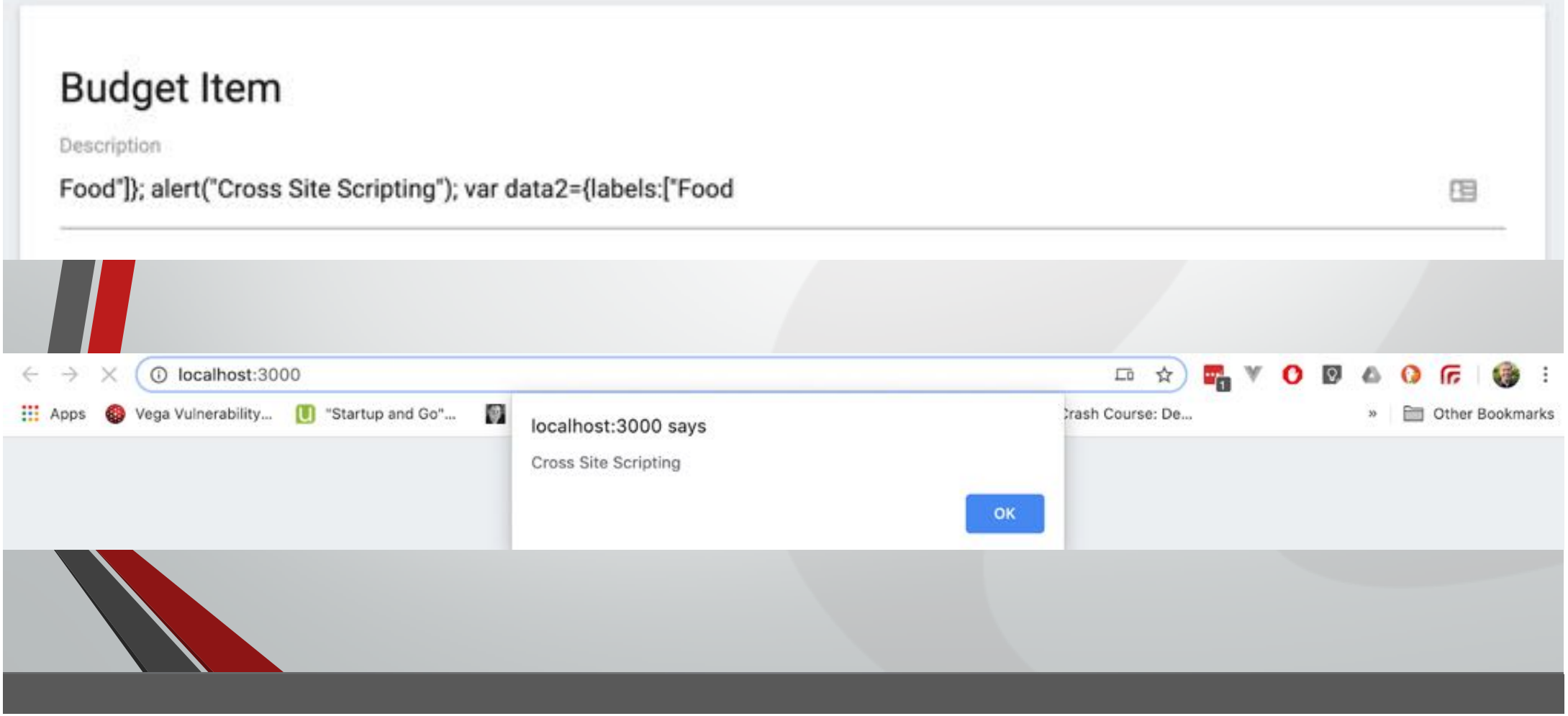
Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	user_params	Mass Assignment	Potentially dangerous key allowed for mass assignment near line 95: params.require(:user).permit(:email, :name, :admin, :password_digest)

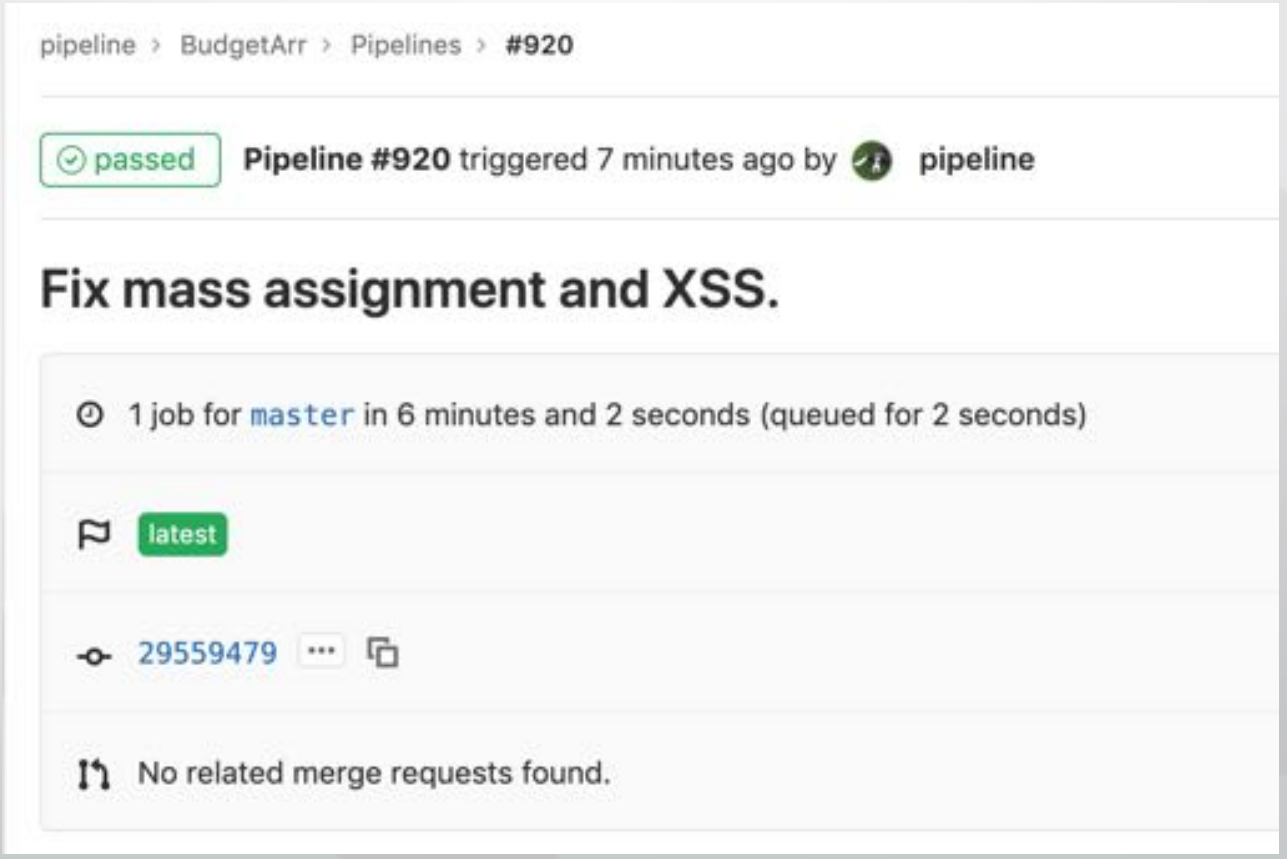
View Warnings

Confidence	Template	Warning Type	Message
Weak	users/_monthly_breakdown (Template:users/dashboard)	Cross-Site Scripting	Unescaped model attribute near line 16: LineItem.monthly_breakdown_by_category.map do "\"#{x[:name]}\"".html_safe end.join(",")
Weak	users/_monthly_breakdown (Template:users/dashboard)	Cross-Site Scripting	Unescaped model attribute near line 20: LineItem.monthly_breakdown_by_category.map do "#{(x[:total].to_f / 100.0)}" end.join(",")
Weak	users/_monthly_breakdown (Template:users/dashboard)	Cross-Site Scripting	Unescaped model attribute near line 22: LineItem.monthly_breakdown_by_category.map do "\"#{x[:colour]}\"".html_safe end.join(",")
Weak	users/_monthly_breakdown (Template:users/dashboard)	Cross-Site Scripting	Unescaped model attribute near line 25: LineItem.monthly_breakdown_by_category.map do "\"#{x[:colour]}\"".html_safe end.join(",")

Brakeman


Budget Item
Description
Food"]}; alert("Cross Site Scripting"); var data2={labels:["Food
localhost:3000
Apps
Vega Vulnerability...
"Startup and Go"...
Other Bookmarks
localhost:3000 says
Cross Site Scripting
OK

Brakeman


pipeline › BudgetArr › Pipelines › #920
passed
Pipeline #920 triggered 7 minutes ago by pipeline
Fix mass assignment and XSS.
1 job for master in 6 minutes and 2 seconds (queued for 2 seconds)
latest
29559479
No related merge requests found.

Static Analysis Weaknesses

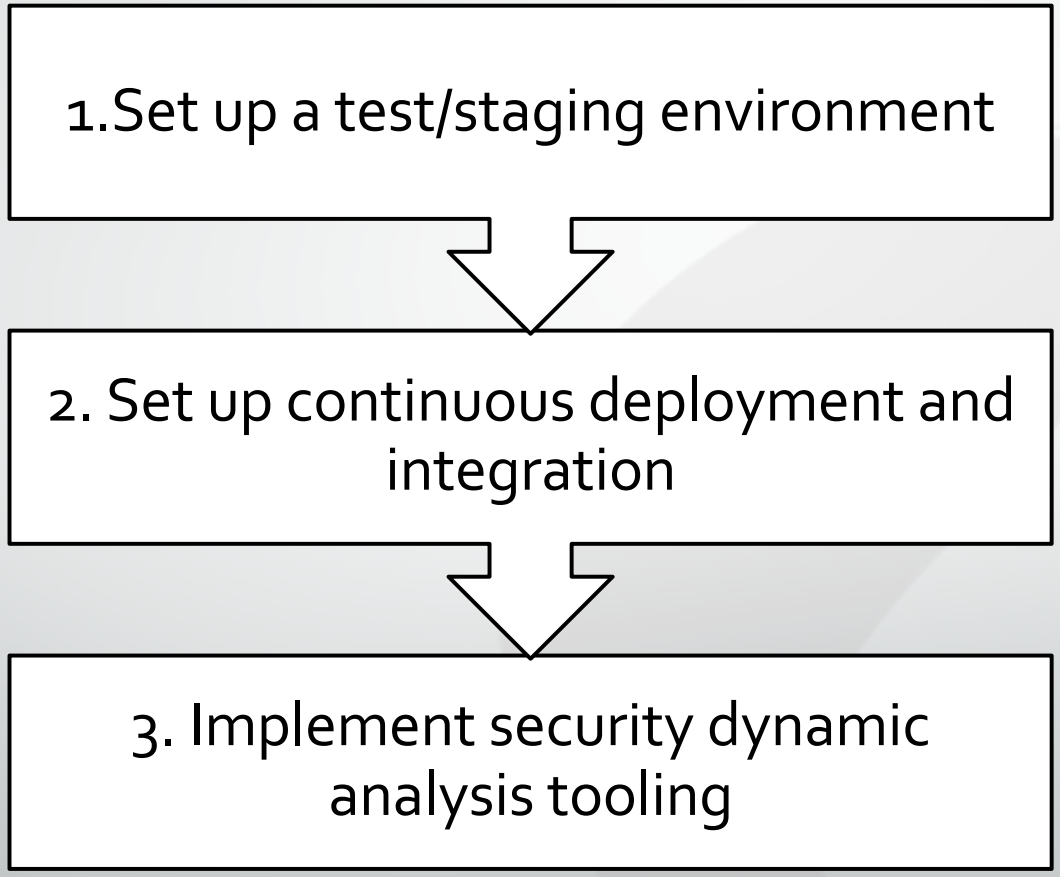
- Can't find logic flaws
  - Business logic
  - Authentication
  - Authorisation
- Potential false positives
- Configuration

Static Analysis

https://owasp.org/www-community/Source_Code_Analysis_Tools

Dynamic Tests

Dynamic Analysis



Docker ZAP

.gitlab-ci.yml:

```
zap_test:
 stage: Security Test
 image: owasp/zap2docker-weekly
 script:
 - zap-baseline.py -t https://budgetarr.XXX.com
```

Unit Testing

Unit Tests

- Authentication
- Authorisation
  - Access to data
  - Create/update/deletion on objects

Unit Tests - Authentication

```
test "should not access mortgages while not logged in" do
  get mortgages_url
  assert_response :success

  get signout_users_url

  get mortgages_url
  assert_redirected_to signin_users_path
end
```

Unit Tests - Authorisation

```
test "index should only contain my budget items" do
  get budget_items_url(format: :json)
  assert_response :success

  initial_count = JSON.parse(@response.body).count

  users(:two).budget_items.create(
      description: 'Test',
      expense_category: users(:two).expense_categories.first
  )

  get budget_items_url(format: :json)
  assert_response :success

  assert_equal initial_count, JSON.parse(@response.body).count
end
```

Unit Tests - Authorisation

```
Minitest::Assertion: Expected: 4
  Actual: 5
test/controllers/budget_items_controller_test.rb:28:in
`block in <class:BudgetItemsControllerTest>'
```

Unit Tests - Authorisation

```
def index
  @budget_items = BudgetItem.all
end
```

```
def index
  @budget_items = @current_user.budget_items
end
```

Unit Tests - Authorisation

```
Finished in 0.55500s

1 tests, 3 assertions, 0 failures, 0 errors, 0 skips
```

Infrastructure

ASD

- Patching
- Continuous incident detection/response
- Hardening

Patching

```
- name: Install unattended updates
  apt:
    name: unattended-upgrades

- name: Set unattended upgrade settings
  template: src=50unattended-upgrades.j2
dest=/etc/apt/apt.conf.d/50unattended-upgrades

- name: Set unattended upgrade settings
  template: src=20auto-upgrades.j2
dest=/etc/apt/apt.conf.d/20auto-upgrades
```

20auto-upgrades.j2:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
APT::Periodic::AutocleanInterval "7";
```

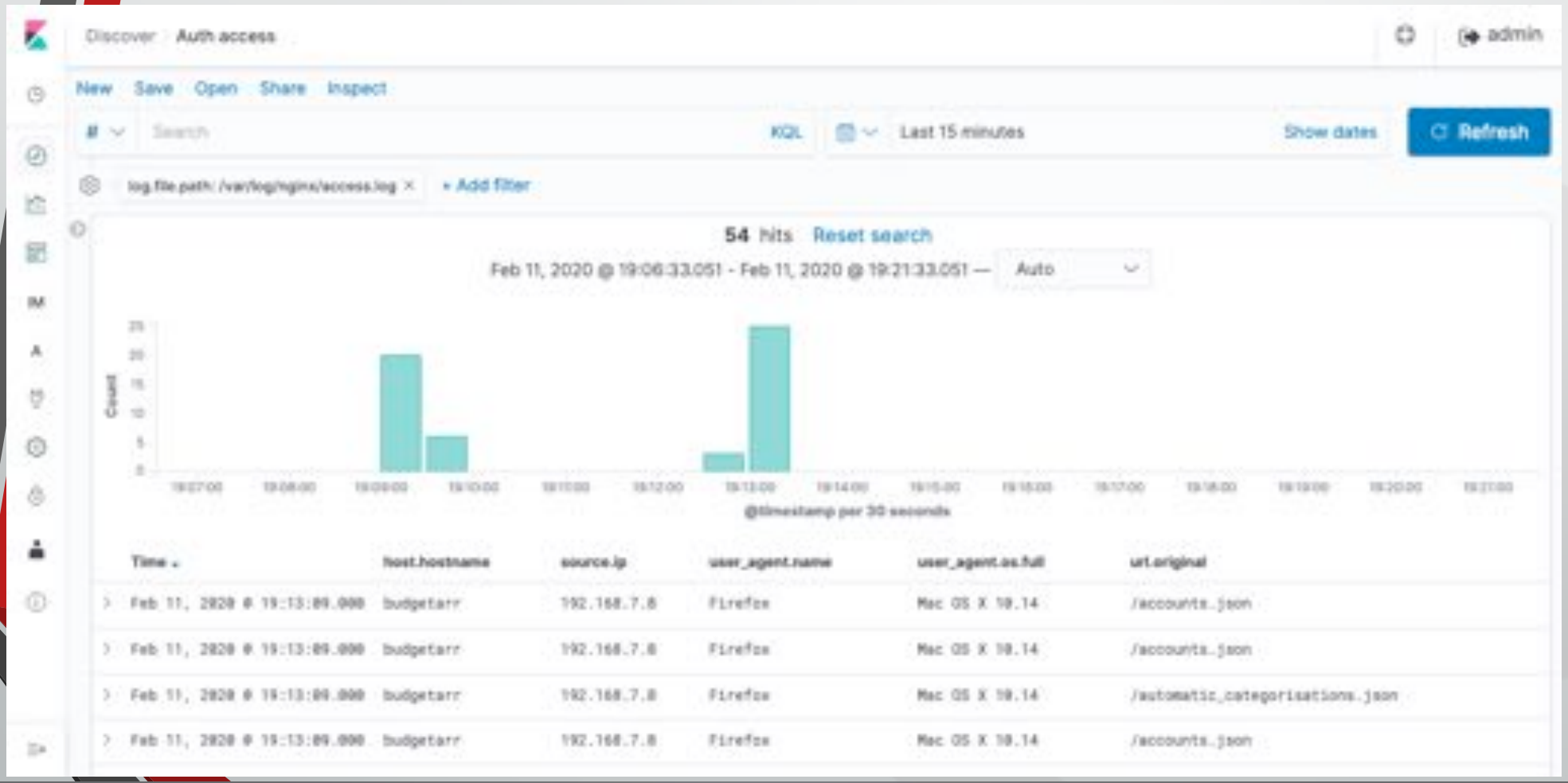
50unattended-upgrades.j2:

```
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:00";
```

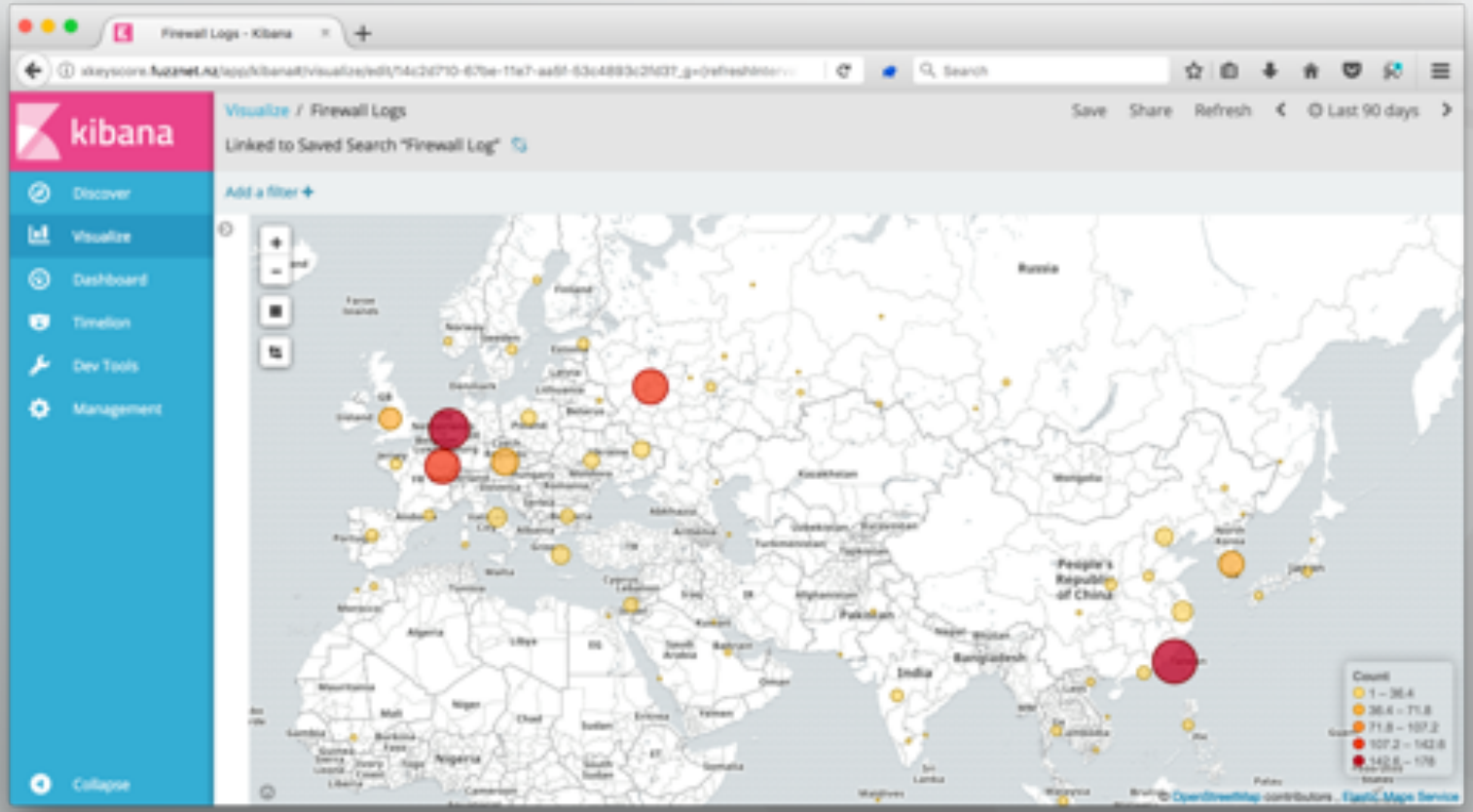
Logging/Monitoring/Alerting

```
- name: Add ElasticSearch GPG Key
 apt_key:
   url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
   state: present

- name: Add ElasticSearch repository
 apt_repository:
   repo: deb https://artifacts.elastic.co/packages/oss-7.x/apt stable main
   state: present
   filename: elasticsearch
   update_cache: yes

- name: Install FileBeat
 apt:
   name: filebeat
   state: present
   update_cache: yes

- name: Create filebeat config
 template: src=filebeat.yml.j2 dest=/etc/filebeat/filebeat.yml
```

Logging/Monitoring/Alerting



Logging/Monitoring/Alerting



Hardening

```
ansible-galaxy install dev-sec.os-hardening
ansible-galaxy install dev-sec.ssh-hardening
ansible-galaxy install dev-sec.nginx-hardening
ansible-galaxy install dev-sec.mysql-hardening
```

Hardening

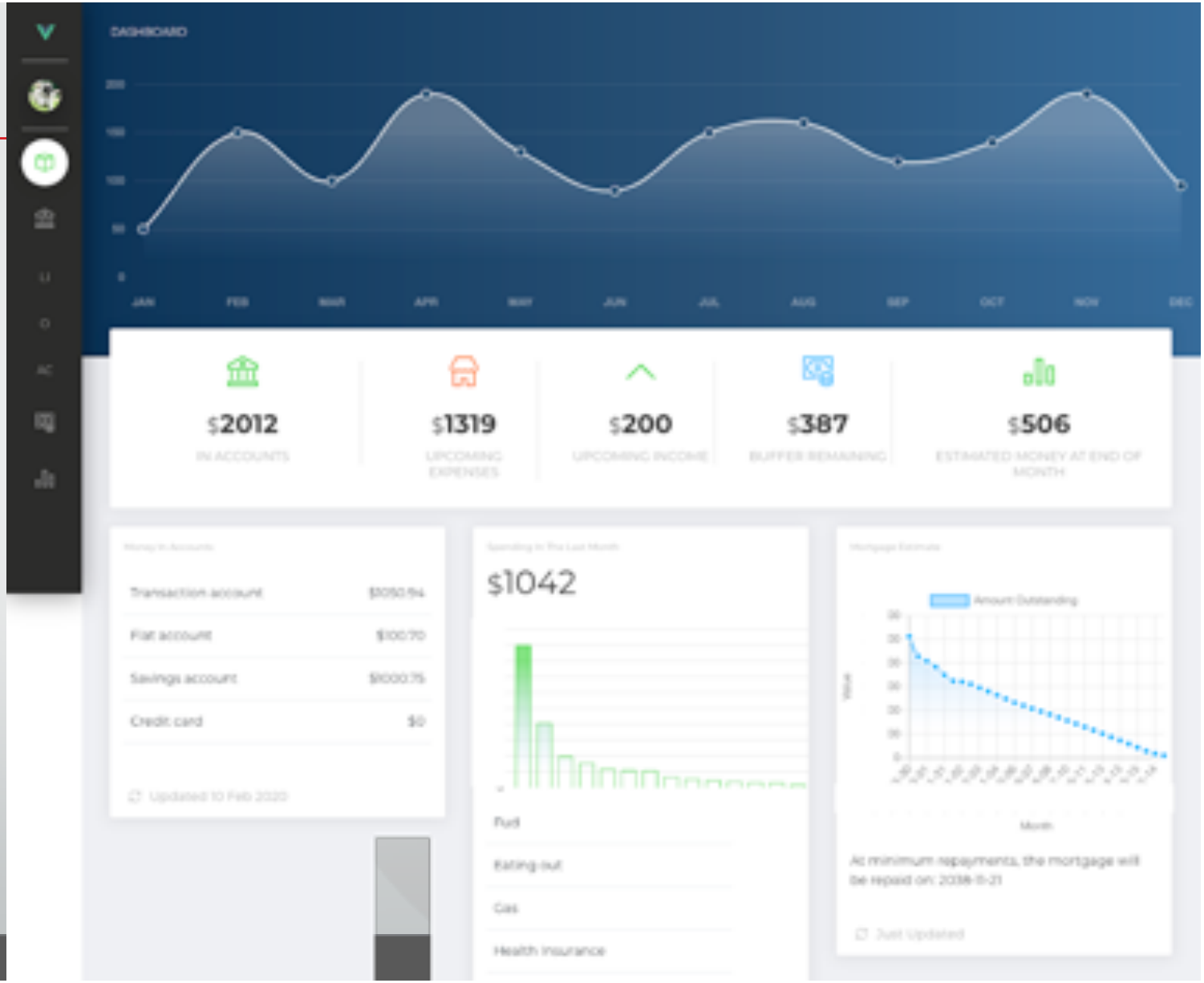
Sites.yml:

```
- name: Harden hosts
  hosts: all
  remote_user: ben
  become: true

 roles:
    - ubuntu_server
    - dev-sec.os-hardening
    - dev-sec.ssh-hardening
```

Infrastructure

Summary

End State


DASHBOARD
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
$2012
IN ACCOUNTS
$1319
UPCOMING EXPENSES
$200
UPCOMING INCOME
$387
BUFFER REMAINING
$506
ESTIMATED MONEY AT END OF MONTH
Transaction account
Flat account
Savings account
Credit card
$1042
Fuel
Eating out
Gas
Health Insurance
Amount Outstanding
Month

End state


SCENARIOS
Mortgage Estimate
Scenario
Base
Month
In this scenario the mortgage will be paid off on: XXXX-08-10, the base case will have it repaid on the XXXX-03-21.
And you will save $XXXX
Run scenario
Calculate

Limitations

VULNERABILITY DATABASE

INTEGRATIONS

BUSINESS LOGIC

Addressing Limitations

MANUAL AUDITS

PEER REVIEW

EXTERNAL REVIEW
& PENTESTING

LATERAL SECURITY

We're Hiring

- Careers:

careers@lateralsecurity.com

- Questions:

benjamin@lateralsecurity.com