OWASP FOUNDATION PRESENTS

APPSEC USA

NOVEMBER 18 - 21

NY MARRIOTT MARQUIS, NYC

2013

Insecure Expectations

Matt Konda
@mkonda
jemurai.com

Security For Software Developers

Jemurai

INTRODUCTION

MATT KONDA
@MKONDA
MKONDA@JEMURAI.COM

	Engineer/Consultant		Architect	Director	Founder	
1997	2000	2003	2006	2009	2012	Beyond
Perl Apache Oracle	Java Applet C++ Java Servlets J2EE BEA	Analytics Cubes / BI Still Java/J2EE	Spring Hibernate Still Java	Spring/Hibernate Java Ruby Flex	Ruby Rails	Ruby Rails AppSec Tools Training
	Masters in CS Thesis on securing distributed objects.	Agile	Project Management	Security	Business Conferences	

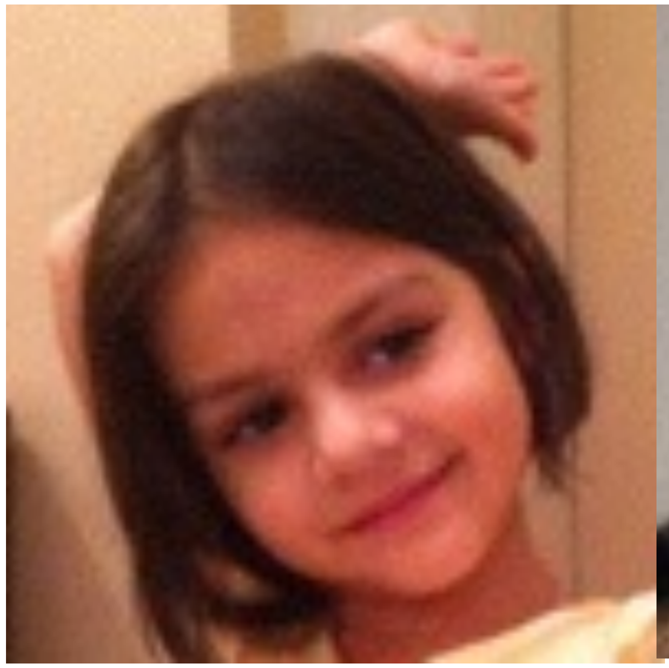
JEDI

SAMURAI

Security For Software Developers

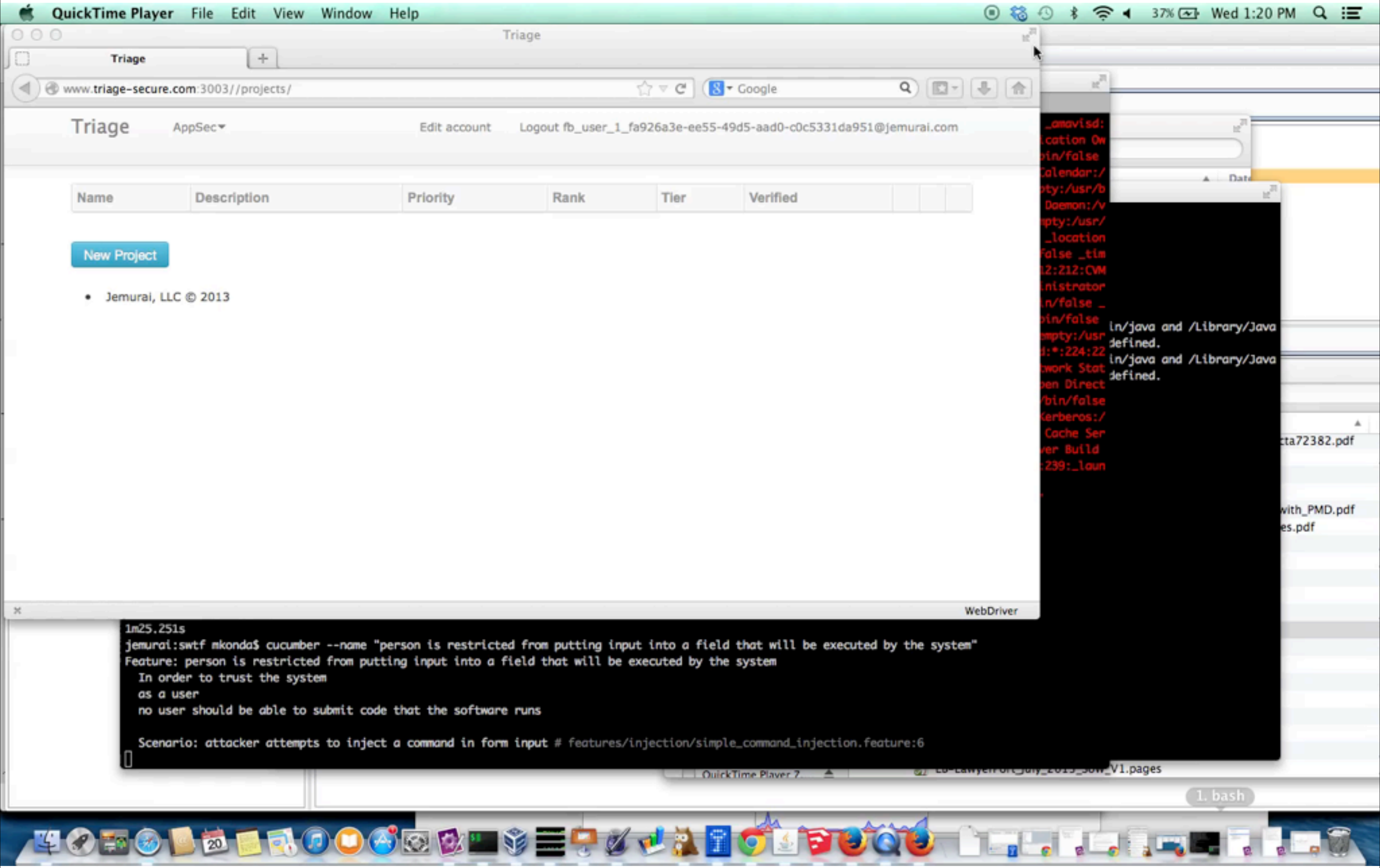
Jemurai

THANKS TO FAMILY!



DEMO

```
cucumber --name "person is restricted
from putting input into a field that
will be executed by the system"
```


QuickTime Player File Edit View Window Help
Wed 1:20 PM
Triage
www.triage-secure.com:3003//projects/
Triage AppSec▾ Edit account Logout fb_user_1_fa926a3e-ee55-49d5-aad0-c0c5331da951@jemurai.com
New Project
WebDriver

Name	Description	Priority	Rank	Tier	Verified

- Jemurai, LLC © 2013

```
1m25.251s
jemurai:swtf mkonda$ cucumber --name "person is restricted from putting input into a field that will be executed by the system"
Feature: person is restricted from putting input into a field that will be executed by the system
  In order to trust the system
  as a user
  no user should be able to submit code that the software runs

  Scenario: attacker attempts to inject a command in form input # features/injection/simple_command_injection.feature:6
```

Root cause

```
def destroy
    @project = Project.find(params[:id])

    name = @project.name
    `rm /tmp/#{name}.log`

    @project.destroy

    respond_to do |format|
      format.html { redirect_to projects_url }
      format.json { head :no_content }
    end
  end
```

```
What if @project.name is :
"; cat /etc/passwd > public/passwd.html;”
```

How many people here

<u>write tests?</u>

HOW MANY PEOPLE HERE

USE TDD?

HOW MANY PEOPLE HERE

USE BDD?

HOW MANY PEOPLE HERE

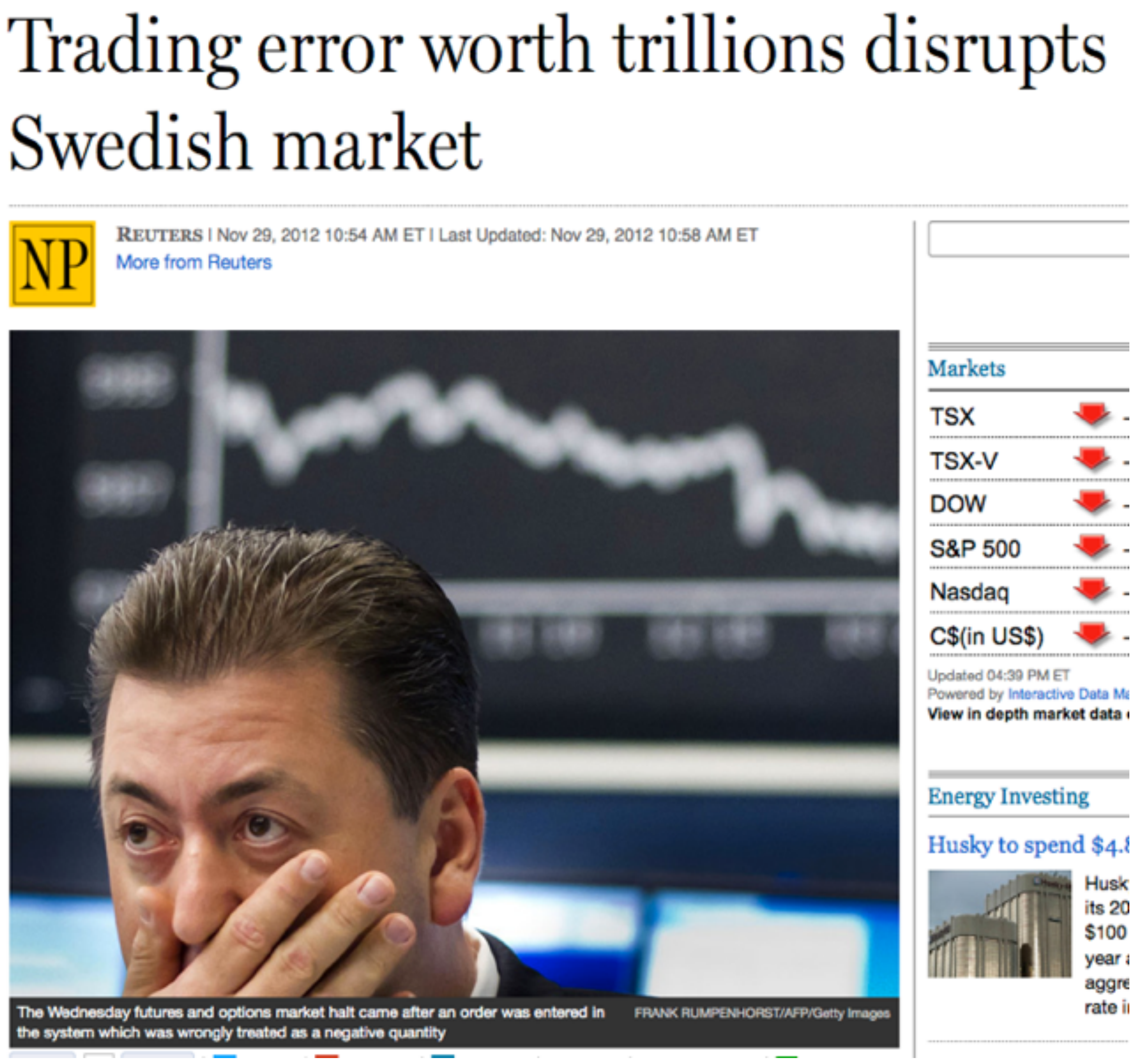
<u>KNOW OF OWASP?</u>

HOW MANY PEOPLE HERE

CURRENTLY WRITE SECURITY TESTS?

INSECURE EXPECTATIONS

`rspec`



Trading error worth trillions disrupts Swedish market

NP

REUTERS | Nov 29, 2012 10:54 AM ET | Last Updated: Nov 29, 2012 10:58 AM ET

More from Reuters

The Wednesday futures and options market halt came after an order was entered in the system which was wrongly treated as a negative quantity

FRANK RUMPENHORST/AFP/Getty Images

Markets

TSX	🔻
TSX-V	🔻
DOW	🔻
S&P 500	🔻
Nasdaq	🔻
C$(in US$)	🔻

Updated 04:39 PM ET

Powered by Interactive Data Ma

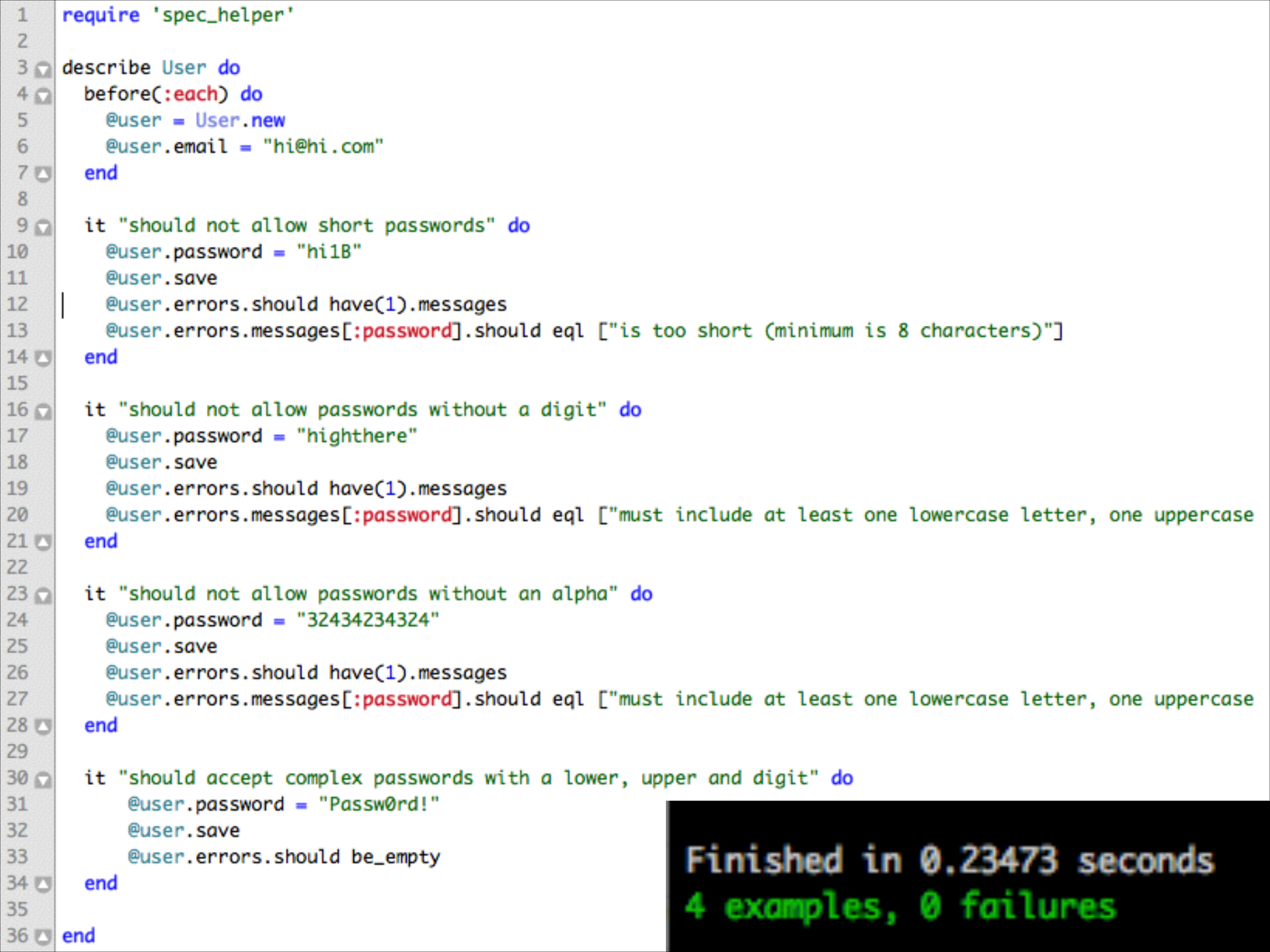
View in depth market data

Energy Investing

Husky to spend $4.

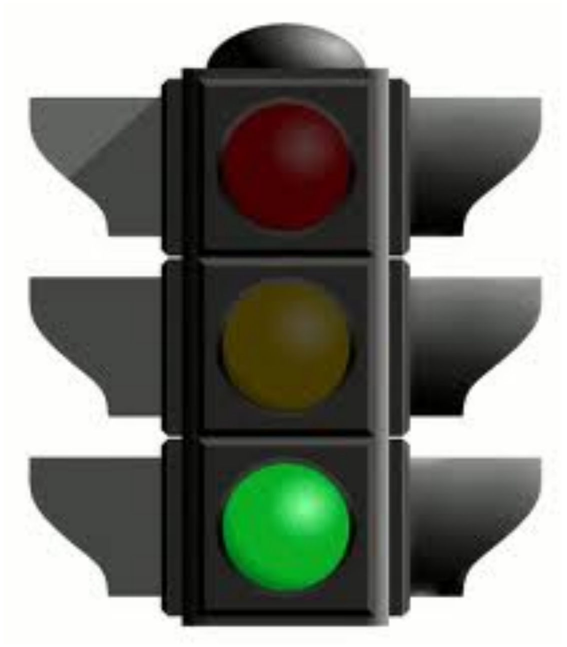
Husk
its 20
$100
year
aggre
rate i

-6 = 64.1 Trillion



```ruby
require 'spec_helper'

describe User do
  before(:each) do
    @user = User.new
    @user.email = "hi@hi.com"
  end

  it "should not allow short passwords" do
    @user.password = "hi1B"
    @user.save
    @user.errors.should have(1).messages
    @user.errors.messages[:password].should eql ["is too short (minimum is 8 characters)"]
  end

  it "should not allow passwords without a digit" do
    @user.password = "highthere"
    @user.save
    @user.errors.should have(1).messages
    @user.errors.messages[:password].should eql ["must include at least one lowercase letter, one uppercase
  end

  it "should not allow passwords without an alpha" do
    @user.password = "32434234324"
    @user.save
    @user.errors.should have(1).messages
    @user.errors.messages[:password].should eql ["must include at least one lowercase letter, one uppercase
  end

  it "should accept complex passwords with a lower, upper and digit" do
      @user.password = "Passw0rd!"
      @user.save
      @user.errors.should be_empty
  end

end
```

```
Finished in 0.23473 seconds
4 examples, 0 failures
```



Feature
Scenario

Given
When
Then

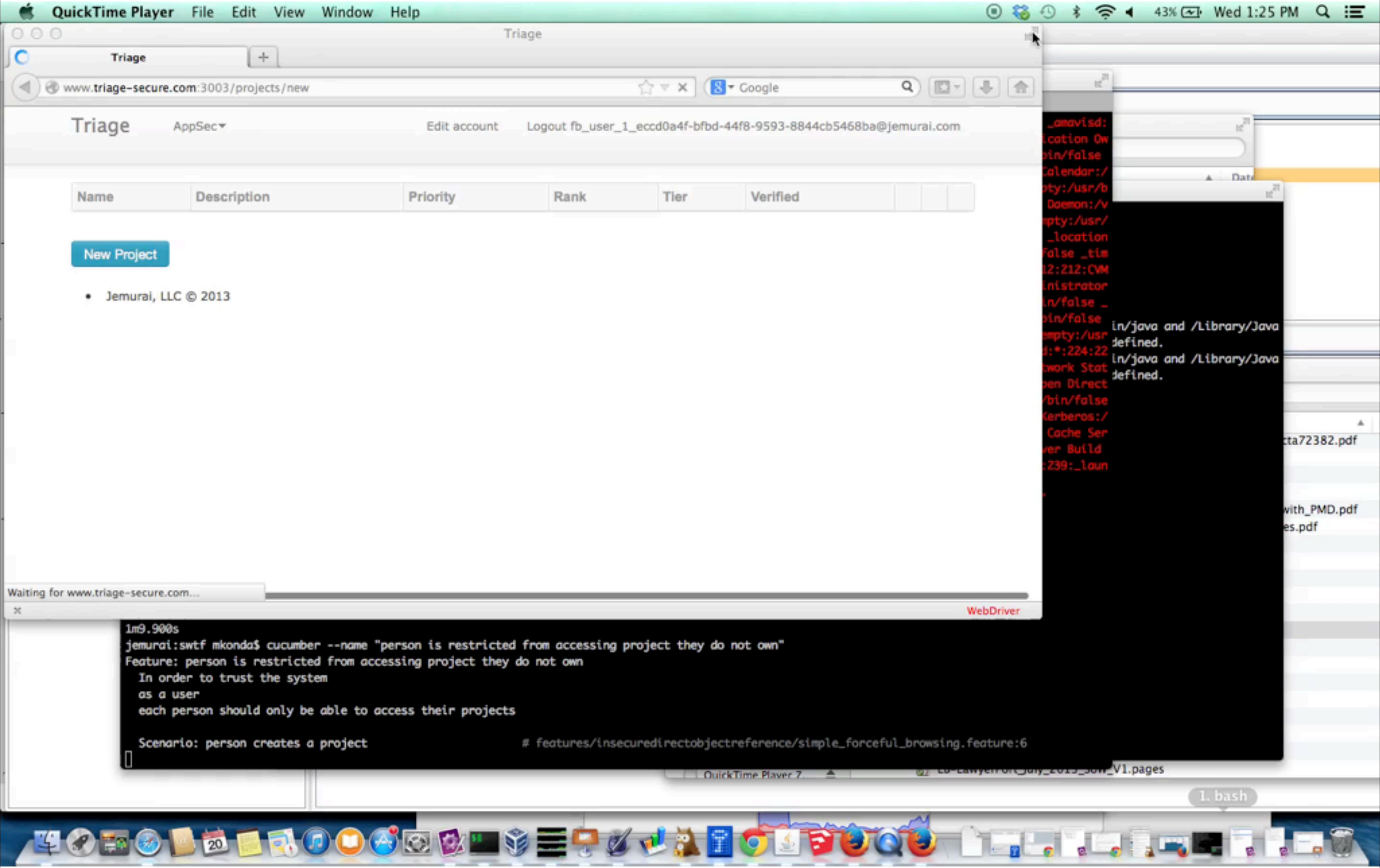
Feature: person is restricted from accessing project they do not own

Scenario: person accesses a project that is not theirs

Given a new project created by a user
When a different person attempts to access the project
Then the system should prevent access

DEMO

```
cucumber --name "person is restricted from accessing project they do not own"
```


QuickTime Player File Edit View Window Help
Wed 1:25 PM
Triage
www.triage-secure.com:3003/projects/new
Triage
AppSec
Edit account
Logout fb_user_1_eccd0a4f-bfbd-44f8-9593-8844cb5468ba@jemurai.com
Name
Description
Priority
Rank
Tier
Verified
New Project
Jemurai, LLC © 2013
Waiting for www.triage-secure.com...
WebDriver

```
1m9.900s
jemurai:swtf mkonda$ cucumber --name "person is restricted from accessing project they do not own"
Feature: person is restricted from accessing project they do not own
  In order to trust the system
  as a user
  each person should only be able to access their projects

  Scenario: person creates a project                    # features/insecuredirectobjectreference/simple_forceful_browsing.feature:6
```

```
Given(/^a new project created by a user$/) do
  uuid = SecureRandom.uuid
  @user1 = "fb_user_1_#{uuid}@jemurai.com"
  register_as_user(@user1, "password")
  new_project("Insecure Direct Object Reference #{uuid}",
    "Forceful Browsing Desc")
  @url = current_url
end

When(/^a different person attempts to access the project$/) do
  logout(@user1)
  uuid = SecureRandom.uuid
  @user2 = "fb_user_2_#{uuid}@jemurai.com"
  register_as_user(@user2, "password")
end

Then(/^the system should prevent access$/) do
  visit @url
  expect(page).not_to have_content "Forceful Browsing Desc"
end
```

INTRODUCING: TRIAGE

https://github.com/Jemurai/triage

http://localhost:3000/projects?name=%27A%27%29%20or%201=1%20--

HANDY

```
def index
   email = current_user.email
  conditions = "owner LIKE '#{email}'"
  if params[:name]
     conditions = "name like #{params[:name]} " + conditions
  end
  @projects = Project.find(:all, :conditions=>conditions)

   respond_to do |format|
     format.html # index.html.erb
     format.json { render json: @projects }
   end
 end
```

FOR ILLUSTRATION

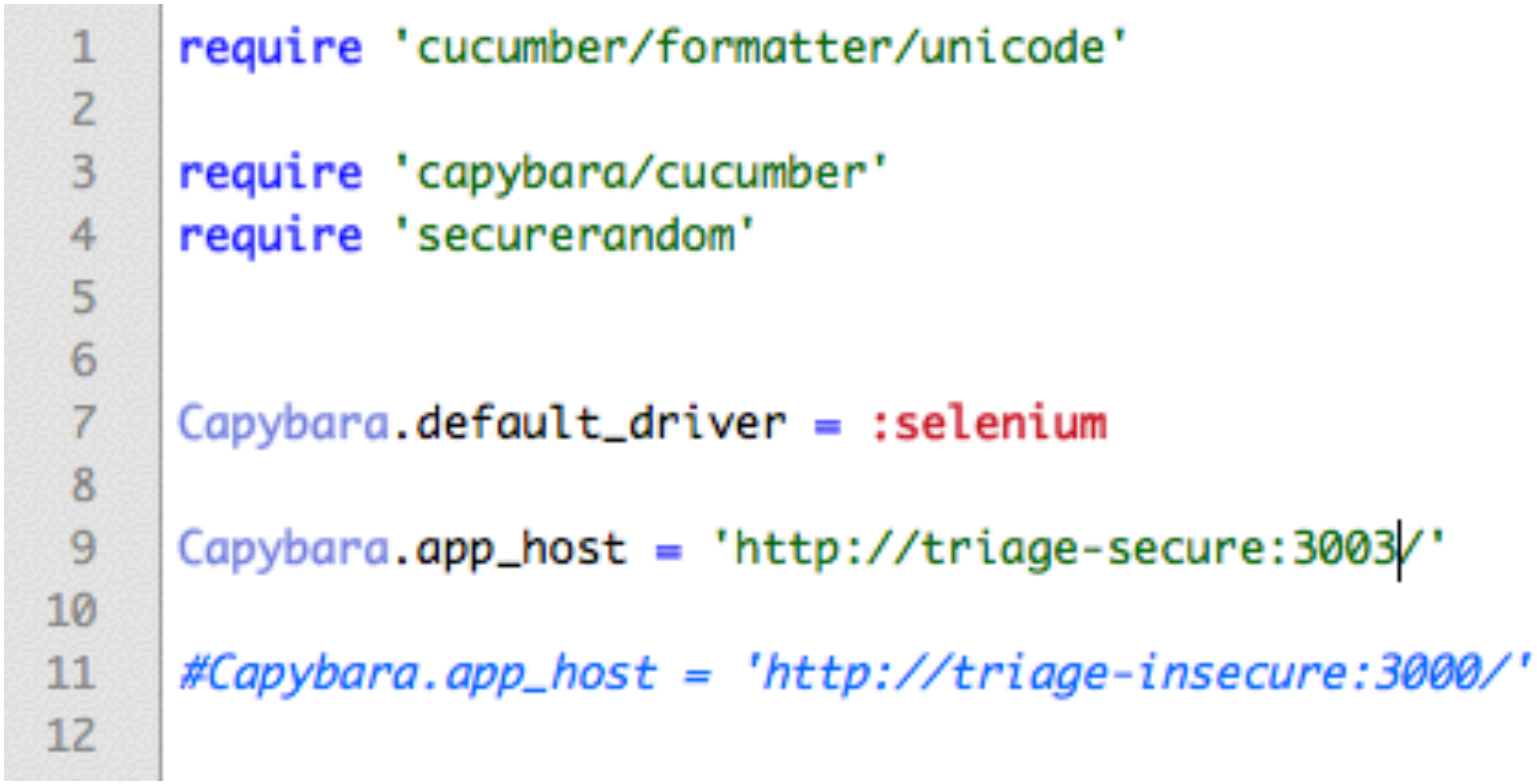
```
SELECT "projects".* FROM "projects"
WHERE (name like 'A') or 1=1 -- owner LIKE 'test@test.com')
```

INTRODUCING: SWTF

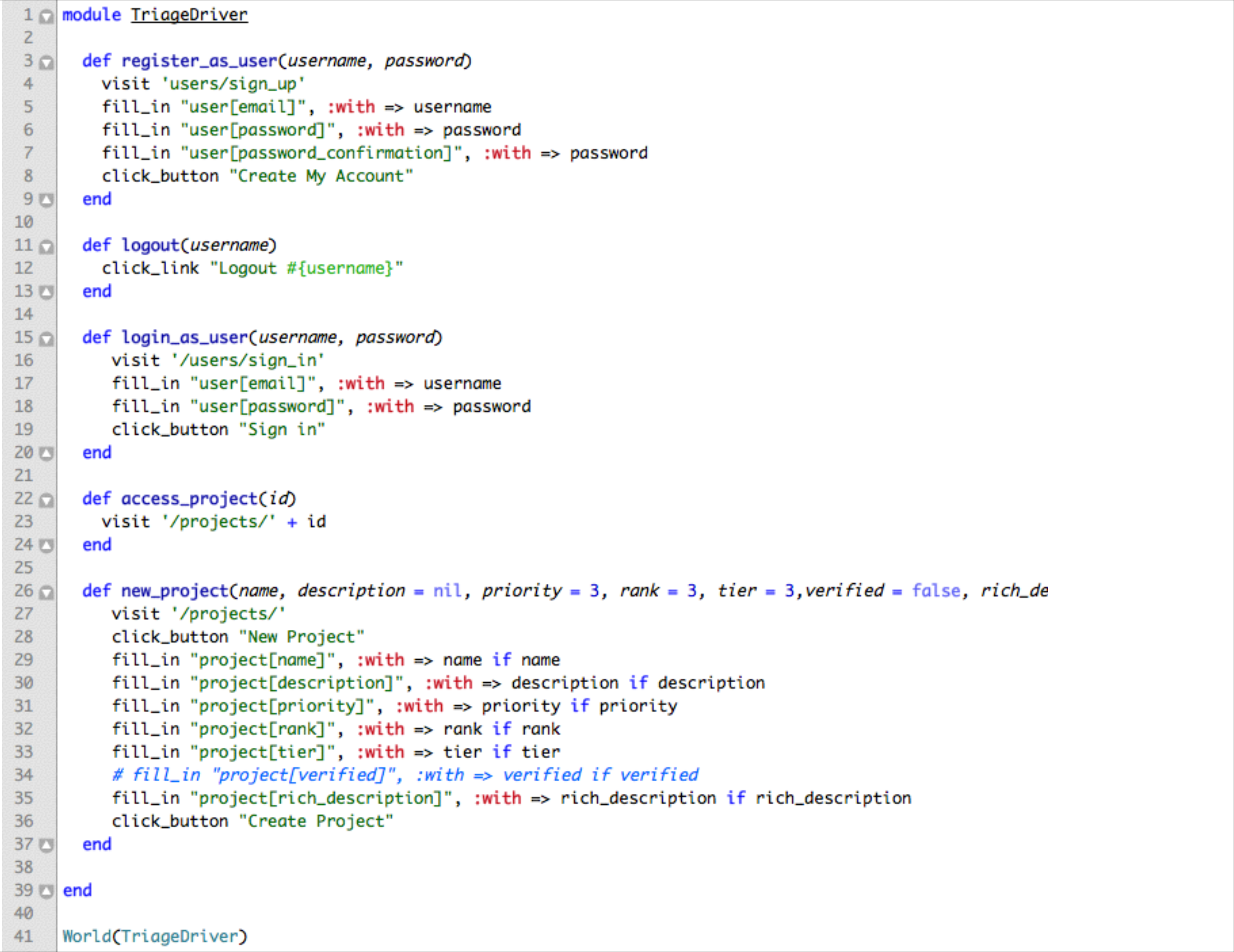
Security Web Testing Framework

SECURITY WTF

FEATURES/ENV.RB



```ruby
require 'cucumber/formatter/unicode'

require 'capybara/cucumber'
require 'securerandom'


Capybara.default_driver = :selenium

Capybara.app_host = 'http://triage-secure:3003/'

#Capybara.app_host = 'http://triage-insecure:3000/'

```

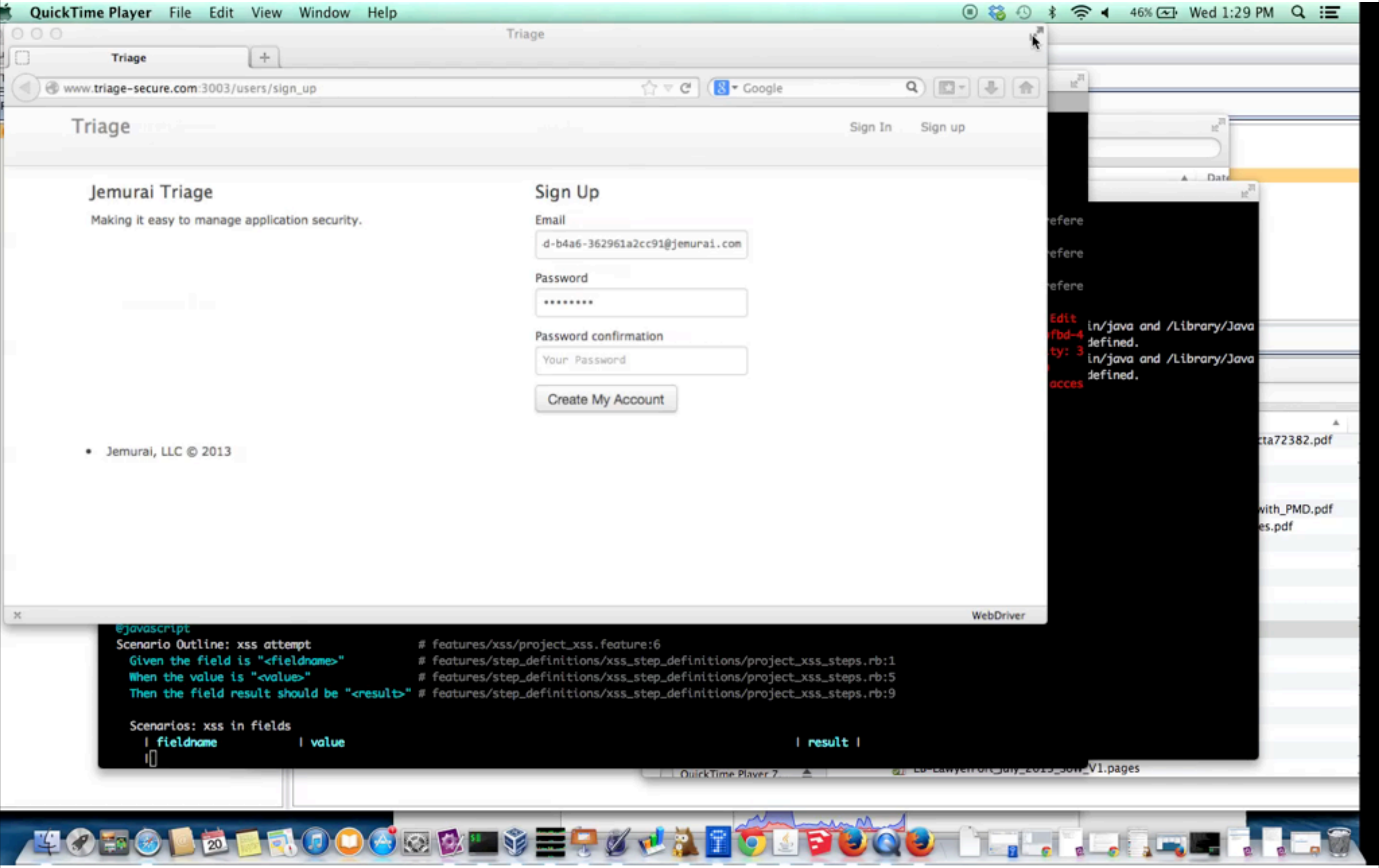


```ruby
module TriageDriver

  def register_as_user(username, password)
    visit 'users/sign_up'
    fill_in "user[email]", :with => username
    fill_in "user[password]", :with => password
    fill_in "user[password_confirmation]", :with => password
    click_button "Create My Account"
  end

  def logout(username)
    click_link "Logout #{username}"
  end

  def login_as_user(username, password)
     visit '/users/sign_in'
     fill_in "user[email]", :with => username
     fill_in "user[password]", :with => password
     click_button "Sign in"
  end

  def access_project(id)
    visit '/projects/' + id
  end

  def new_project(name, description = nil, priority = 3, rank = 3, tier = 3,verified = false, rich_de
     visit '/projects/'
     click_button "New Project"
     fill_in "project[name]", :with => name if name
     fill_in "project[description]", :with => description if description
     fill_in "project[priority]", :with => priority if priority
     fill_in "project[rank]", :with => rank if rank
     fill_in "project[tier]", :with => tier if tier
     # fill_in "project[verified]", :with => verified if verified
     fill_in "project[rich_description]", :with => rich_description if rich_description
     click_button "Create Project"
  end

end

World(TriageDriver)
```

```
Feature: user is prevented from putting XSS in project form fields
   A user wants to be sure that others users can't
   put XSS in the projects pages
   in order to ensure that their sessions and information are safe.

   @javascript
   Scenario Outline:  xss attempt
      Given the field is "<fieldname>"
      When the value is "<value>"
      Then the field result should be "<result>"

      Scenarios: xss in fields
         | fieldname | value | result |
         | project[name] | ProjectName | noxss |
         | project[name] | ProjectName <script>alert('project[name]-
>xss');</script>   | xss    |
         | project[description] | ProjectDescription
<script>alert('project[description]->xss');</script> | noxss |
new_project("XSS Name #{@field} #{uniq}","XSS Desc #{@field}"+ uniq)
click_link 'Edit'
fill_in @field, :with => @value
click_button "Update Project"
if @result == "xss"
  # This should have xss in it...did it stick?
  alerted = false
  begin
    page.driver.browser.switch_to.alert.accept
    alerted = true
  rescue
  end
  if alerted
    fail("XSS Used to create Popup in #{@field} with #{@value}")
  else
    puts "Good news, no xss where expected."
  end
else
  expect(page).to have_content @value
end
```

DEMO

```
cucumber --name "user is prevented from
putting XSS in project form fields"
```


QuickTime Player File Edit View Window Help
46% Wed 1:29 PM
Triage
www.triage-secure.com:3003/users/sign_up
Google
Triage
Sign In
Sign up
WebDriver

Jemurai Triage

Making it easy to manage application security.

Sign Up

Email

d-b4a6-362961a2cc91@jemurai.com

Password

•••••••••

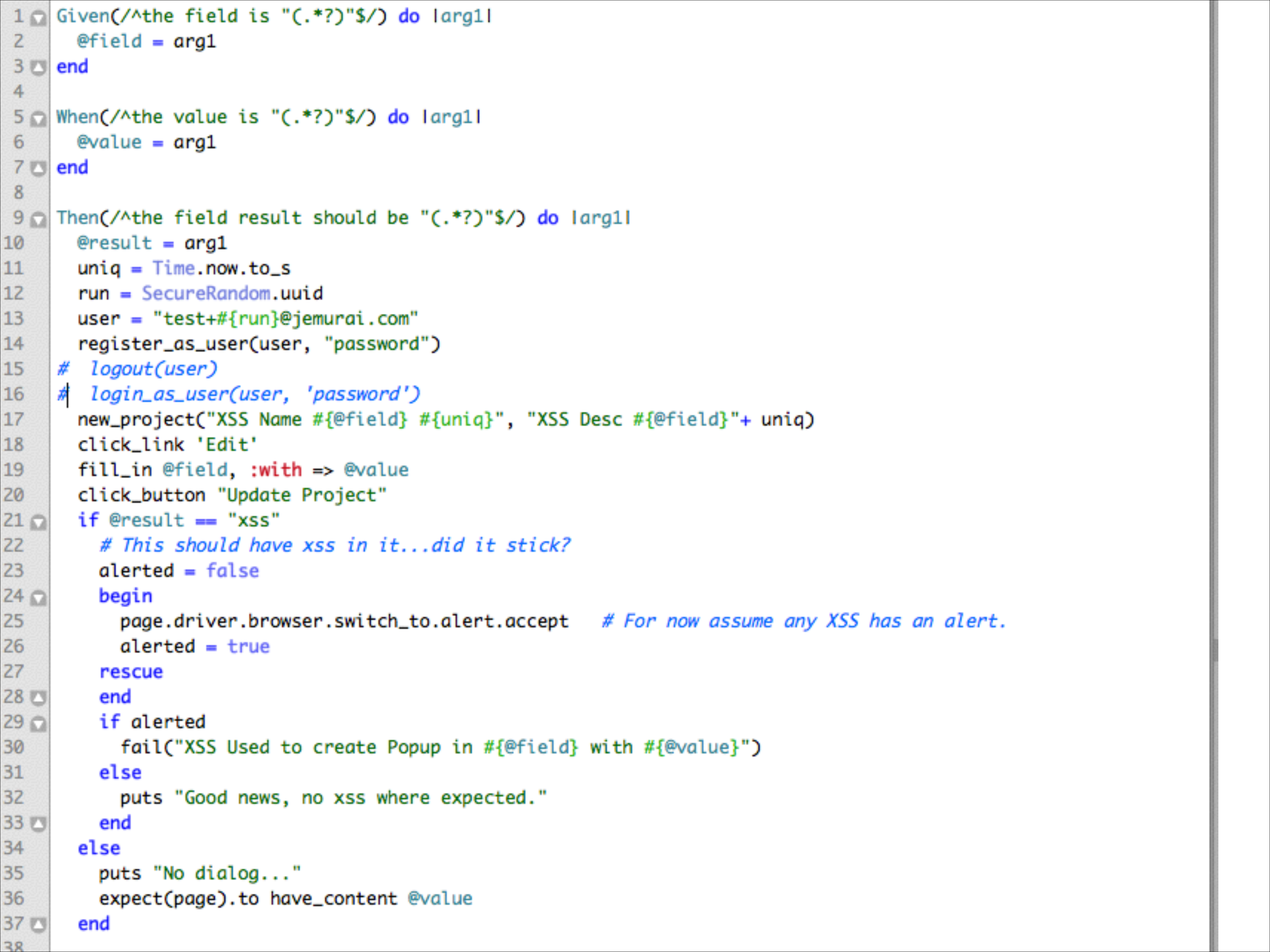
Password confirmation

Your Password

Create My Account

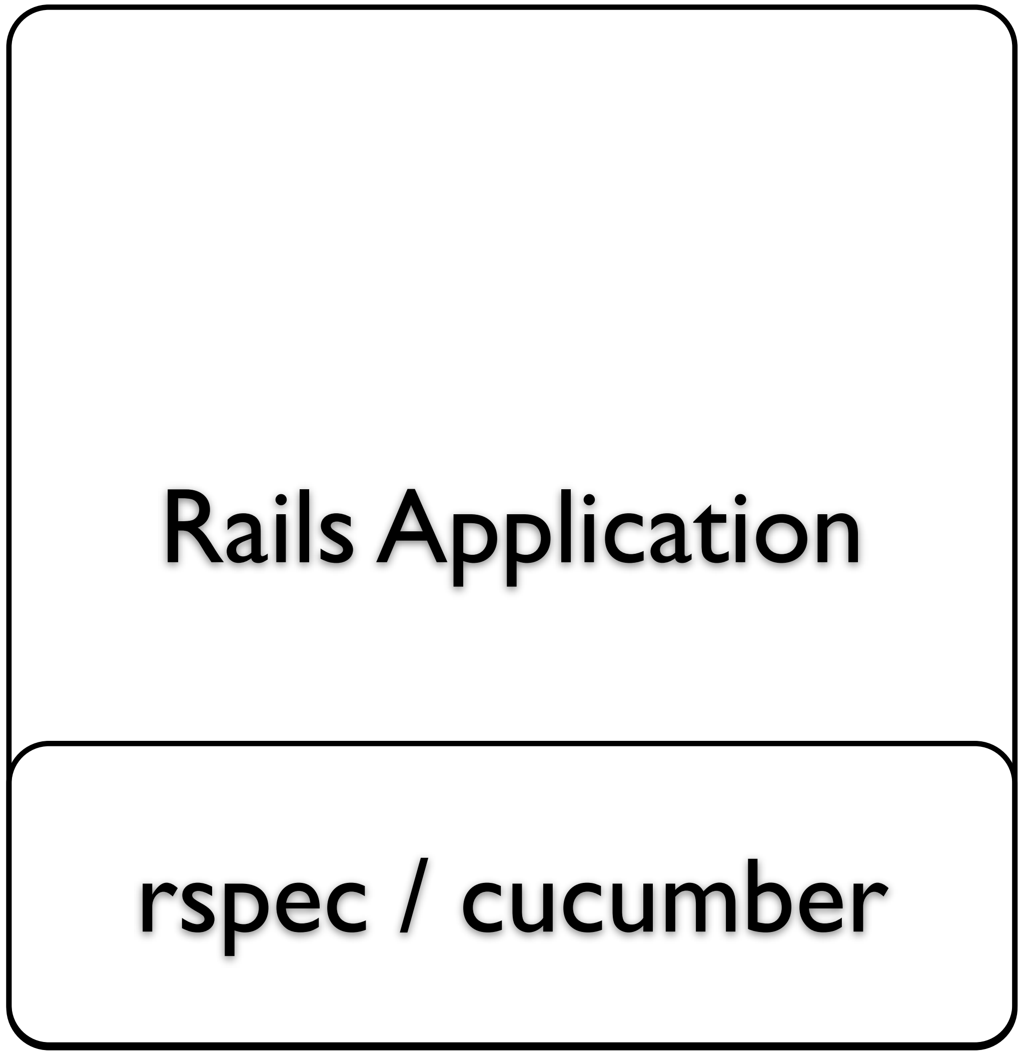
- Jemurai, LLC © 2013

```
@javascript
Scenario Outline: xss attempt                   # features/xss/project_xss.feature:6
  Given the field is "<fieldname>"              # features/step_definitions/xss_step_definitions/project_xss_steps.rb:1
  When the value is "<value>"                   # features/step_definitions/xss_step_definitions/project_xss_steps.rb:5
  Then the field result should be "<result>"    # features/step_definitions/xss_step_definitions/project_xss_steps.rb:9

  Scenarios: xss in fields
    | fieldname        | value                                                                  | result |
    |
```

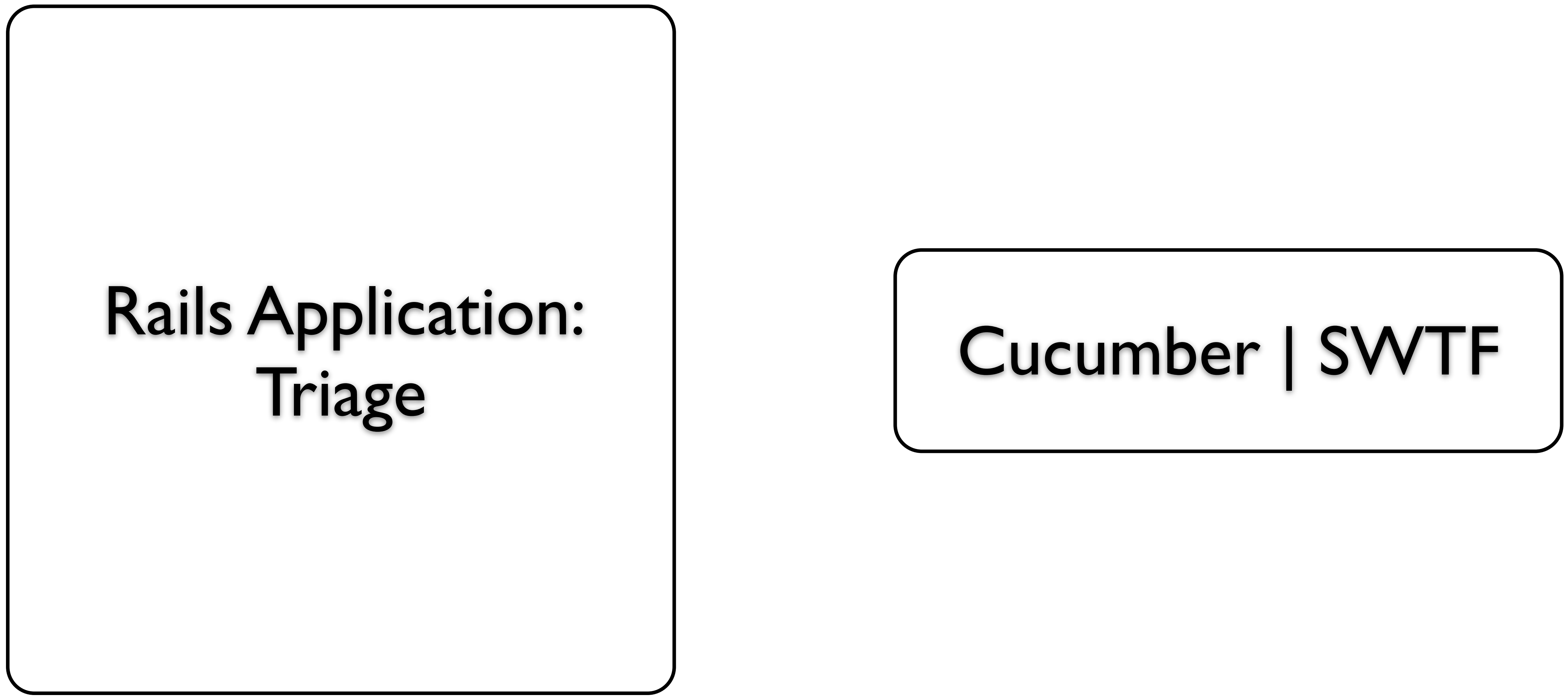


```ruby
Given(/^the field is "(.*?)"$/) do |arg1|
  @field = arg1
end

When(/^the value is "(.*?)"$/) do |arg1|
  @value = arg1
end

Then(/^the field result should be "(.*?)"$/) do |arg1|
  @result = arg1
  uniq = Time.now.to_s
  run = SecureRandom.uuid
  user = "test+#{run}@jemurai.com"
  register_as_user(user, "password")
#  logout(user)
#  login_as_user(user, 'password')
  new_project("XSS Name #{@field} #{uniq}", "XSS Desc #{@field}"+ uniq)
  click_link 'Edit'
  fill_in @field, :with => @value
  click_button "Update Project"
  if @result == "xss"
    # This should have xss in it...did it stick?
    alerted = false
    begin
      page.driver.browser.switch_to.alert.accept   # For now assume any XSS has an alert.
      alerted = true
    rescue
    end
    if alerted
      fail("XSS Used to create Popup in #{@field} with #{@value}")
    else
      puts "Good news, no xss where expected."
    end
  else
    puts "No dialog..."
    expect(page).to have_content @value
  end
```

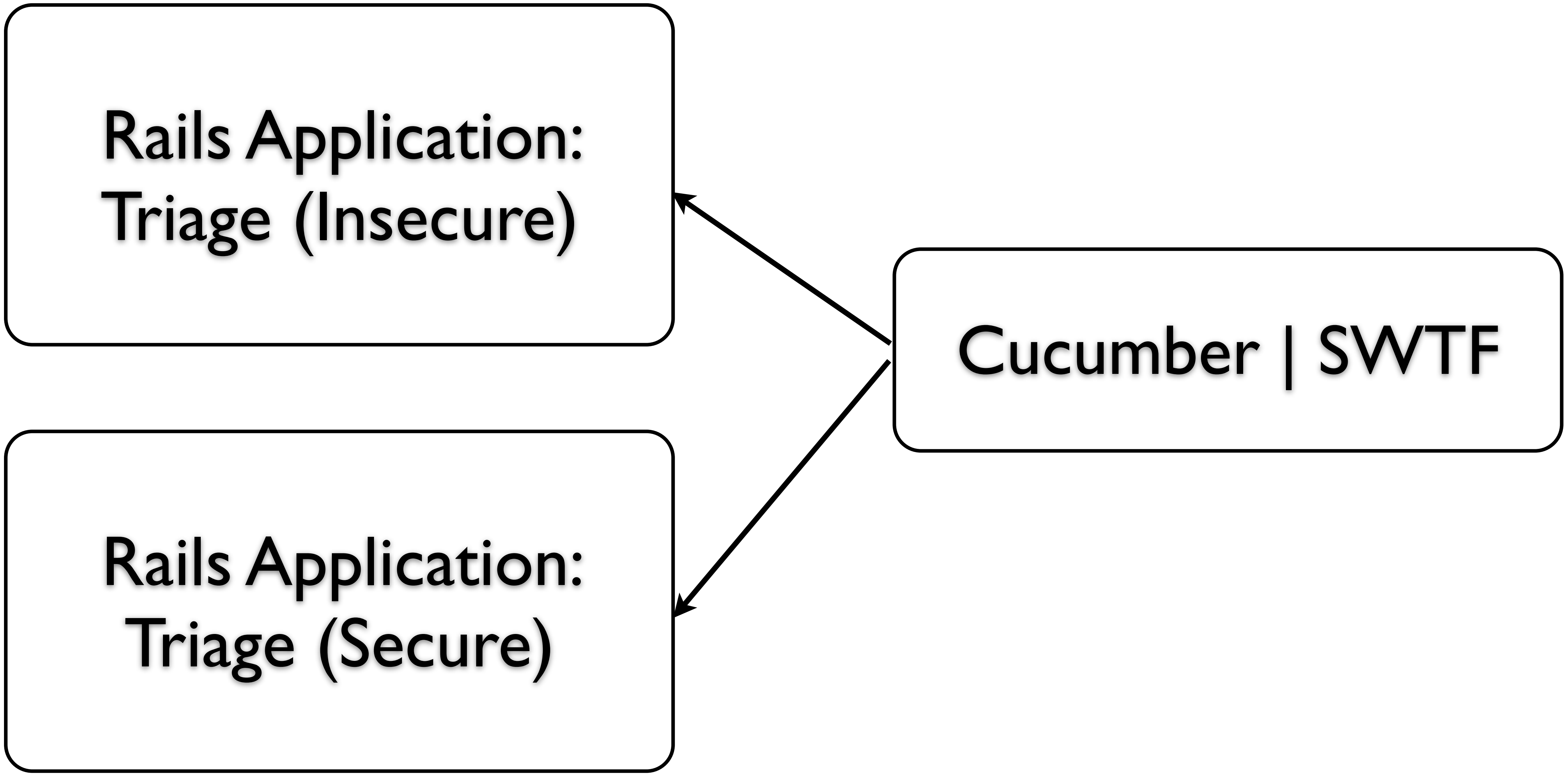
TESTS IN APP



Tests out of App



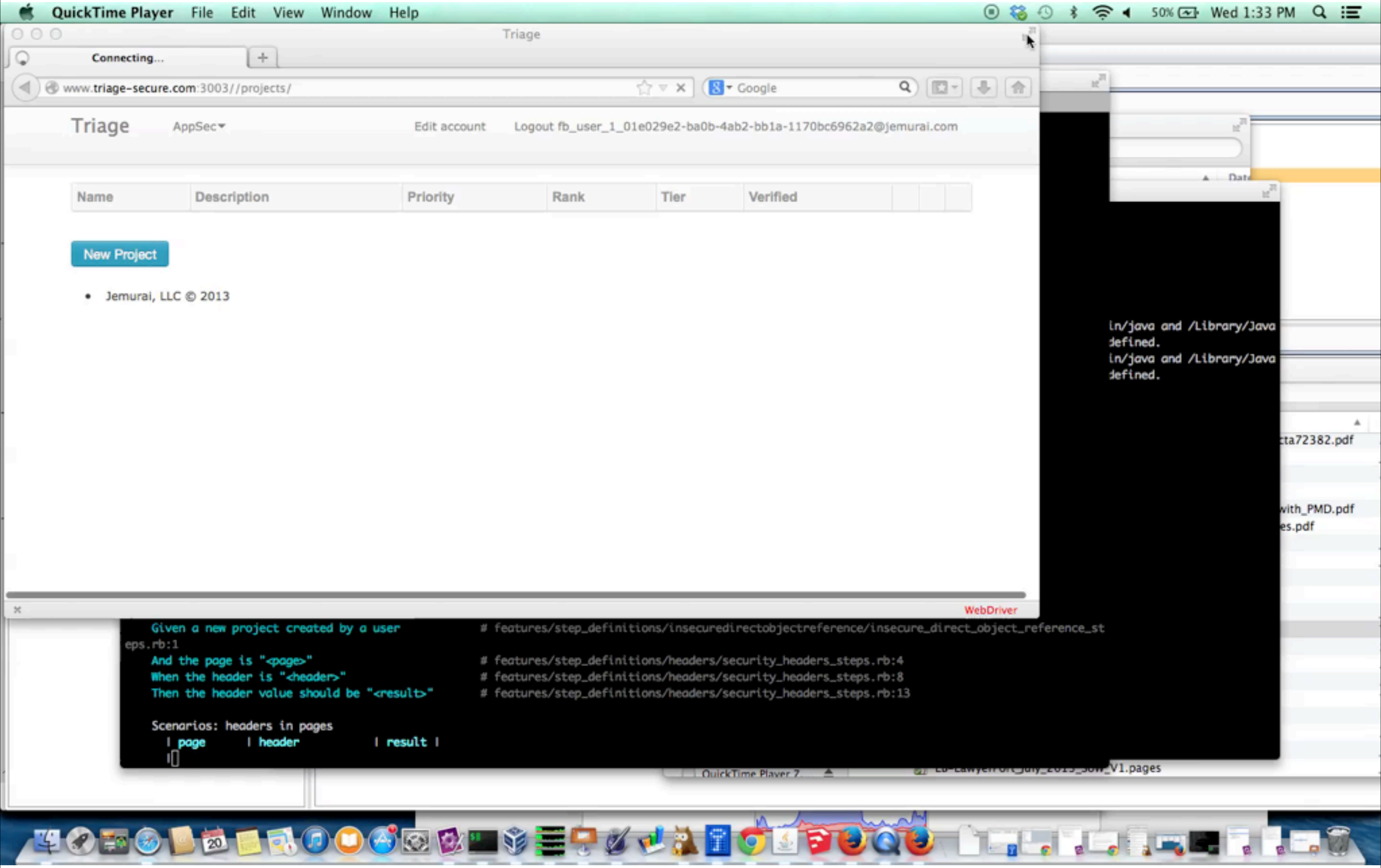
Tests out of App


Rails Application: Triage (Insecure)
Rails Application: Triage (Secure)
Cucumber | SWTF

Means they can be easily adapted to test different apps

DEMO

```
cucumber --name "user is protected from malicious content and having their page framed"
```


QuickTime Player File Edit View Window Help
Wed 1:33 PM
Triage
Connecting...
www.triage-secure.com:3003//projects/
Google
Triage AppSec▾ Edit account Logout fb_user_1_01e029e2-ba0b-4ab2-bb1a-1170bc6962a2@jemurai.com
New Project
WebDriver

Name	Description	Priority	Rank	Tier	Verified

- Jemurai, LLC © 2013

```
in/java and /Library/Java
defined.
in/java and /Library/Java
defined.
```

```
    Given a new project created by a user          # features/step_definitions/insecuredirectobjectreference/insecure_direct_object_reference_st
eps.rb:1
    And the page is "<page>"                       # features/step_definitions/headers/security_headers_steps.rb:4
    When the header is "<header>"                  # features/step_definitions/headers/security_headers_steps.rb:8
    Then the header value should be "<result>"     # features/step_definitions/headers/security_headers_steps.rb:13

    Scenarios: headers in pages
      | page      | header          | result |
      |
Feature: user is protected from malicious content and
having their page framed
   A user wants to be sure that effective browser
protections are enabled
   in order to ensure that their information is safe.

   @javascript
   Scenario Outline:  check for secure headers attempt
      Given a new project created by a user
      And the page is "<page>"
      When the header is "<header>"
      Then the header value should be "<result>"

      Scenarios: headers in pages
         | page | header | result |
         | projects/  | X-Frame-Options | DENY |
         | projects/  | X-XSS-Protection | 1 |
  cookies = Capybara.current_session.driver.browser.manage.all_cookies
  csrf_token =
Capybara.current_session.driver.browser.find_element(:xpath, "//
meta[@name='csrf-token']").attribute('content');
  # Switch mode to net::http
  uri = URI.parse(url)
  http = Net::HTTP.new(uri.host, uri.port)
  http.verify_mode = OpenSSL::SSL::VERIFY_NONE
  request = Net::HTTP::Post.new(uri.request_uri)
  request['Cookie'] = cookies
  request.set_form_data( {
      "_method" => "put",
      "authenticity_token" => "#{csrf_token}",
      "project[name]"=> "header updated and verified",
      "commit"=>"Update Project" })
  response = http.request(request)

  ...

  if response[@header] == @result
    #pass
  else
    fail("Header #{@header} not set to #{@result} as expected.
           Instead was #{response[@header]}.")
  end
```

TAKE A VULNERABLE PROJECT

Write tests that illustrate the security issues

TRY TO ILLUSTRATE HOW EASY IT WOULD BE TO WRITE SECURITY TESTS

IN LANGUAGE EVERYONE
CAN UNDERSTAND

Why is Application Scanning So Hard?

What if the dev writing the code were testing security cases along the way?

Much smarter.

EXPLORATORY TESTING

QUIZ

- USER SHOULD NOT BE ABLE TO SET FIELDS NOT SHOWN IN THE FORM

Quiz

- User should not be able to submit forms in anothers session

Are Stakeholders Asking for Security?

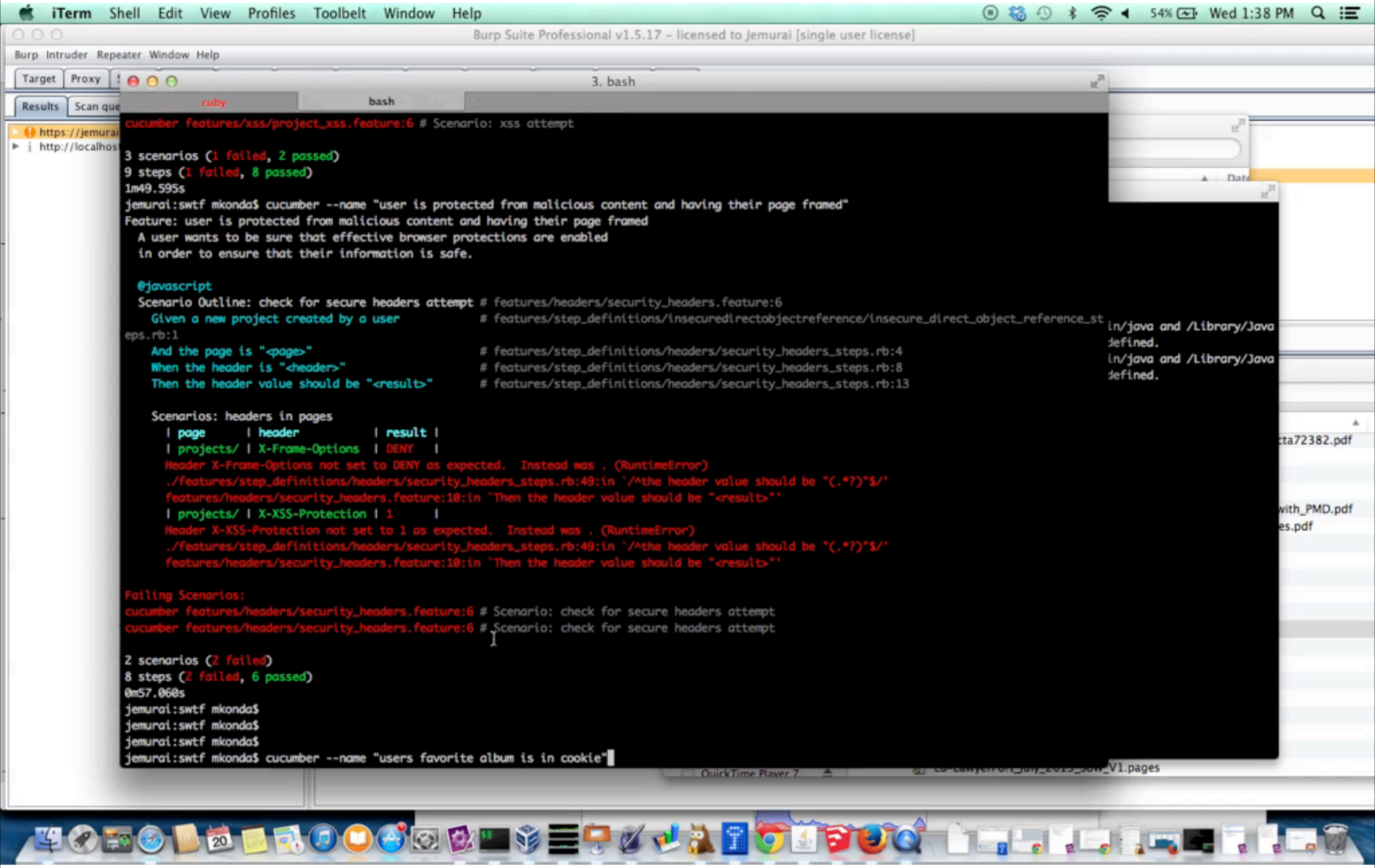
BUT IF YOU ASK THEM ABOUT THESE FEATURES THEY MIGHT WANT THEM

Current Tests

- Injection / SQL Injection
- Cross Site Scripting
- Mass Assignment
- Cross Site Request Forgery
- Secure Headers
- Sensitive Data Exposure (Session Cookie)

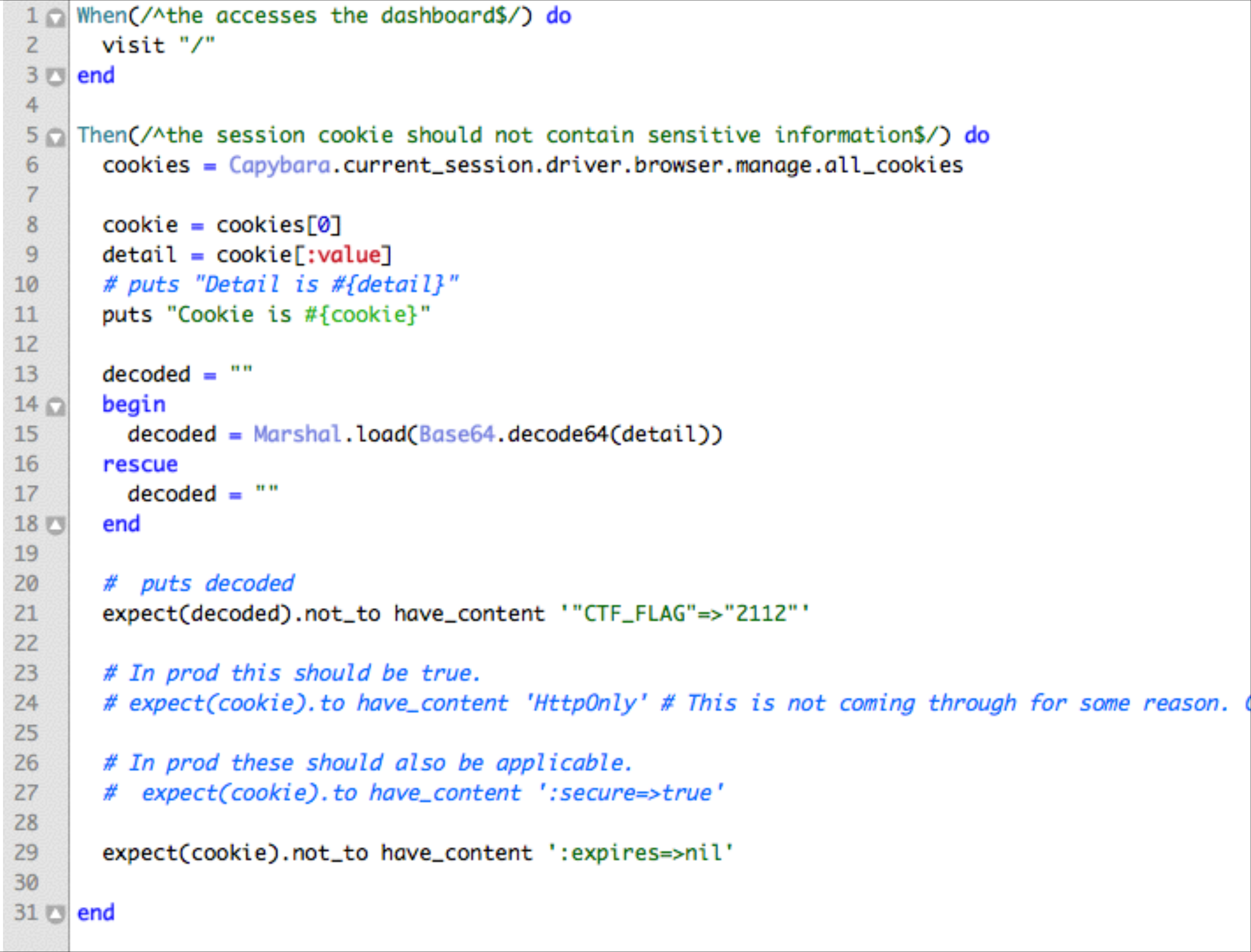
DEMO

```
cucumber --name "users favorite album is
in cookie"
```



```
cucumber features/xss/project_xss.feature:6 # Scenario: xss attempt

3 scenarios (1 failed, 2 passed)
9 steps (1 failed, 8 passed)
1m49.595s
jemurai:swtf mkonda$ cucumber --name "user is protected from malicious content and having their page framed"
Feature: user is protected from malicious content and having their page framed
  A user wants to be sure that effective browser protections are enabled
  in order to ensure that their information is safe.

  @javascript
  Scenario Outline: check for secure headers attempt # features/headers/security_headers.feature:6
    Given a new project created by a user            # features/step_definitions/insecuredirectobjectreference/insecure_direct_object_reference_st
eps.rb:1
    And the page is "<page>"                         # features/step_definitions/headers/security_headers_steps.rb:4
    When the header is "<header>"                    # features/step_definitions/headers/security_headers_steps.rb:8
    Then the header value should be "<result>"       # features/step_definitions/headers/security_headers_steps.rb:13

    Scenarios: headers in pages
      | page      | header           | result |
      | projects/ | X-Frame-Options  | DENY   |
      Header X-Frame-Options not set to DENY as expected.  Instead was . (RuntimeError)
      ./features/step_definitions/headers/security_headers_steps.rb:49:in `/^the header value should be "(.*?)"$/'
      features/headers/security_headers.feature:10:in `Then the header value should be "<result>"'
      | projects/ | X-XSS-Protection | 1      |
      Header X-XSS-Protection not set to 1 as expected.  Instead was . (RuntimeError)
      ./features/step_definitions/headers/security_headers_steps.rb:49:in `/^the header value should be "(.*?)"$/'
      features/headers/security_headers.feature:10:in `Then the header value should be "<result>"'

Failing Scenarios:
cucumber features/headers/security_headers.feature:6 # Scenario: check for secure headers attempt
cucumber features/headers/security_headers.feature:6 # Scenario: check for secure headers attempt

2 scenarios (2 failed)
8 steps (2 failed, 6 passed)
0m57.060s
jemurai:swtf mkonda$
jemurai:swtf mkonda$
jemurai:swtf mkonda$
jemurai:swtf mkonda$ cucumber --name "users favorite album is in cookie"
```

iTerm Shell Edit View Profiles Toolbelt Window Help
Wed 1:38 PM
Burp Suite Professional v1.5.17 – licensed to Jemurai [single user license]
Burp Intruder Repeater Window Help
Target Proxy
Results Scan que
3. bash
ruby
bash



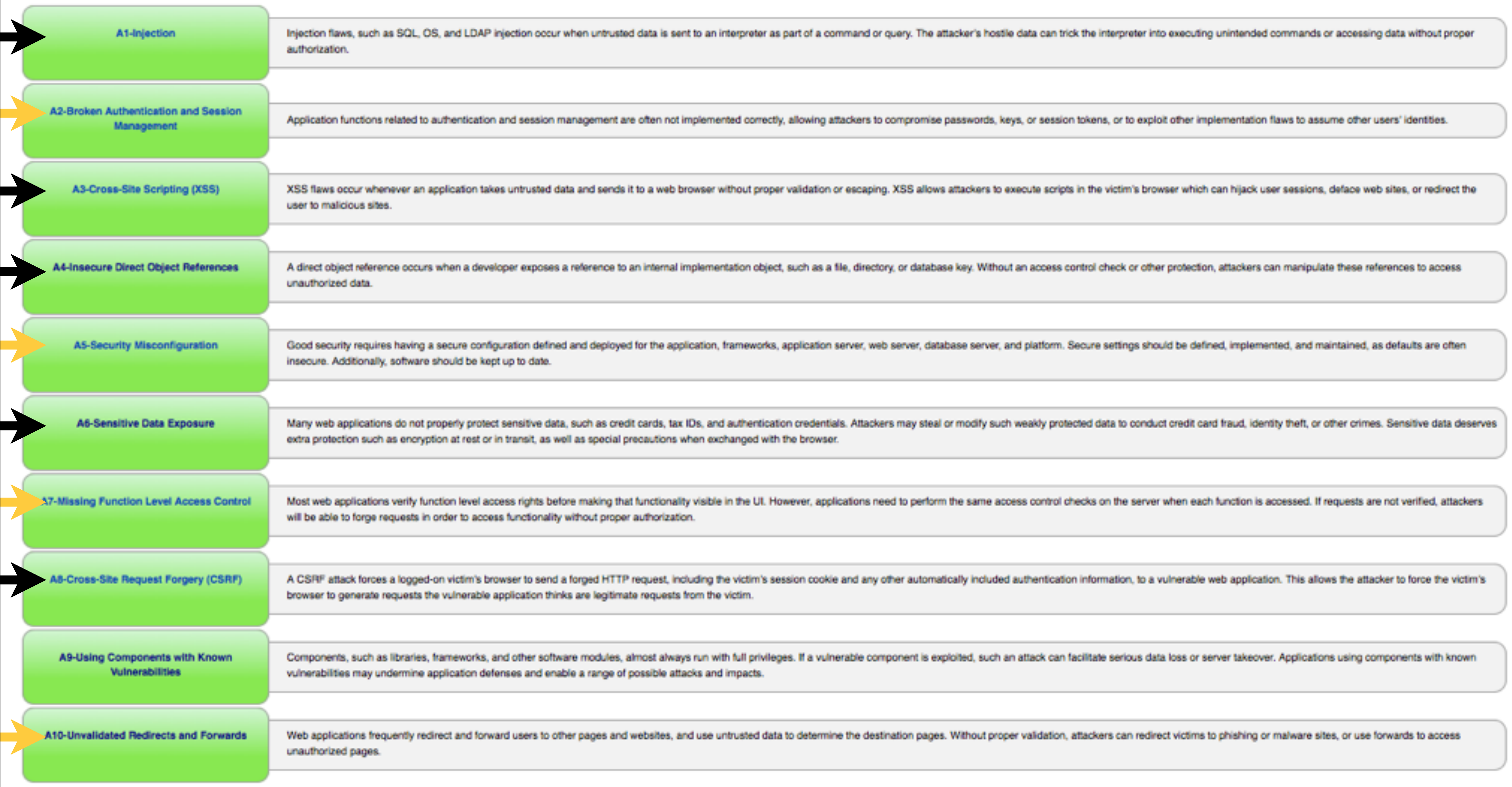
```ruby
When(/^the accesses the dashboard$/) do
  visit "/"
end

Then(/^the session cookie should not contain sensitive information$/) do
  cookies = Capybara.current_session.driver.browser.manage.all_cookies

  cookie = cookies[0]
  detail = cookie[:value]
  # puts "Detail is #{detail}"
  puts "Cookie is #{cookie}"

  decoded = ""
  begin
    decoded = Marshal.load(Base64.decode64(detail))
  rescue
    decoded = ""
  end

  #  puts decoded
  expect(decoded).not_to have_content '"CTF_FLAG"=>"2112"'

  # In prod this should be true.
  # expect(cookie).to have_content 'HttpOnly' # This is not coming through for some reason.

  # In prod these should also be applicable.
  #  expect(cookie).to have_content ':secure=>true'

  expect(cookie).not_to have_content ':expires=>nil'

end
```

Simplified Steps

- Injection: Inject commands into fields and detect functions being called.
- XSS: Inject scripts into fields and detect that alerts are thrown
- Mass Assignment: Set raw form data with Net::HTTP and send it to see how the server responds
- CSRF: Alter CSRF token and send otherwise valid request
- Headers: Interact with system and verify that headers are being set
- Sensitive Data: Open session cookie and inspect

OWASP TOP 10

From: owasp.org



A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7-Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8-Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10-Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

A NATURAL EXTENSION IS TO MAKE IT EASY TO FUZZ FORMS

THERE IS NO

GOAL #1: PLATFORM FOR EDUCATING DEVELOPERS

Goal #2: Language for communicating with business owners

Goal #3: Mechanism for making it easier to implement tests.

OMEGA

HOW MANY PEOPLE HAVE HAD A PENETRATION TEST AGAINST THEIR APPLICATION?

INSTEAD OF A PDF, WHAT IF WE DELIVER FINDINGS WITH WORKING TESTS!

What if a developer could fix a security issue by making the

test pass.

WANDER

GOOD: ALMOST EVERY CLIENT ENGAGEMENT BENEFITS FROM OWASP

BAD: OWASP MEETINGS I HAVE BEEN TO ARE PREDOMINANTLY SECURITY PEOPLE

HOW DO WE "COMMUNICATE"

Cheat Sheets

How many people here

<u>have attended developer conferences this year?</u>

WindyCityRails

HOW MANY PEOPLE HERE

<u>COMMIT TO DEVELOPMENT PROJECTS?</u>

COMMUNITY ORGANIZING

Ideas:

Go to dev meetup
Go dev conference
Contribute to OSS
Listen

MORE IDEAS:

IDENTIFY TECHNOLOGY LEADERS AND APPROACH THEM

Make Developer Friends

MAKE DEVELOPER FRIENDS

MORE IDEAS:

FORM AN OUTREACH SUBCOMMITTEE

More ideas:

De-"criminalize" application security ignorance

More ideas:

Invite developers to speak

More ideas:

Find activities that developers can participate in at meetings

More ideas:

Emphasize developer contributions to OWASP site

MORE IDEAS:

GET DEVELOPERS ON THE OWASP BOARD

More ideas:

???

BASICALLY, I WANT TO SEE OWASP TRY TO BUILD COMMUNITY ORGANIZING WITH DEVELOPERS INTO A MODEL THAT CAN BE REPEATED

THANKS!

Justin Collins @presidentbeef
Jeff Jarmoc @jjarmoc
Ben Toews @mastahyeti
Neil Matatall @ndm
Aaron Bedra @abedra
Jon Claudius @claudijd
Chris Oliver @excid3
Chris Hildebrand @ckhrysze
Jon Rose
Brett Hardin @miscsecurity
Elizabeth Hendrickson @testobsessed

References

- https://github.com/Jemurai/triage
- https://bitbucket.org/mkonda/swtf/
- http://speakerdeck.com/mkonda
- http://brakemanscanner.org
- http://rails-sqli.org
- https://github.com/twitter/secureheaders
- http://testobsessed.com/wp-content/uploads/2011/04/testheuristicscheatsheetv1.pdf
- https://www.owasp.org/index.php/Ruby_on_Rails_Cheatsheet

THANKS!

New York City Chapter

OWASP FOUNDATION PRESENTS

APPSEC USA

NOVEMBER 18 - 21

NY MARRIOTT MARQUIS, NYC

2013

OWASP

The Open Web Application Security Project

Features

- Person is restricted from putting input into a field that will be executed by the system
- User is prevented from putting XSS in project form fields
- User should not be able to set fields not shown in the form
- User should not be able to submit forms in anothers session
- User is protected from malicious content and having their page framed
- Users favorite album is in cookie