BDD Mobile security testing with OWASP MASVS, OWASP MSTG and Calabash

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

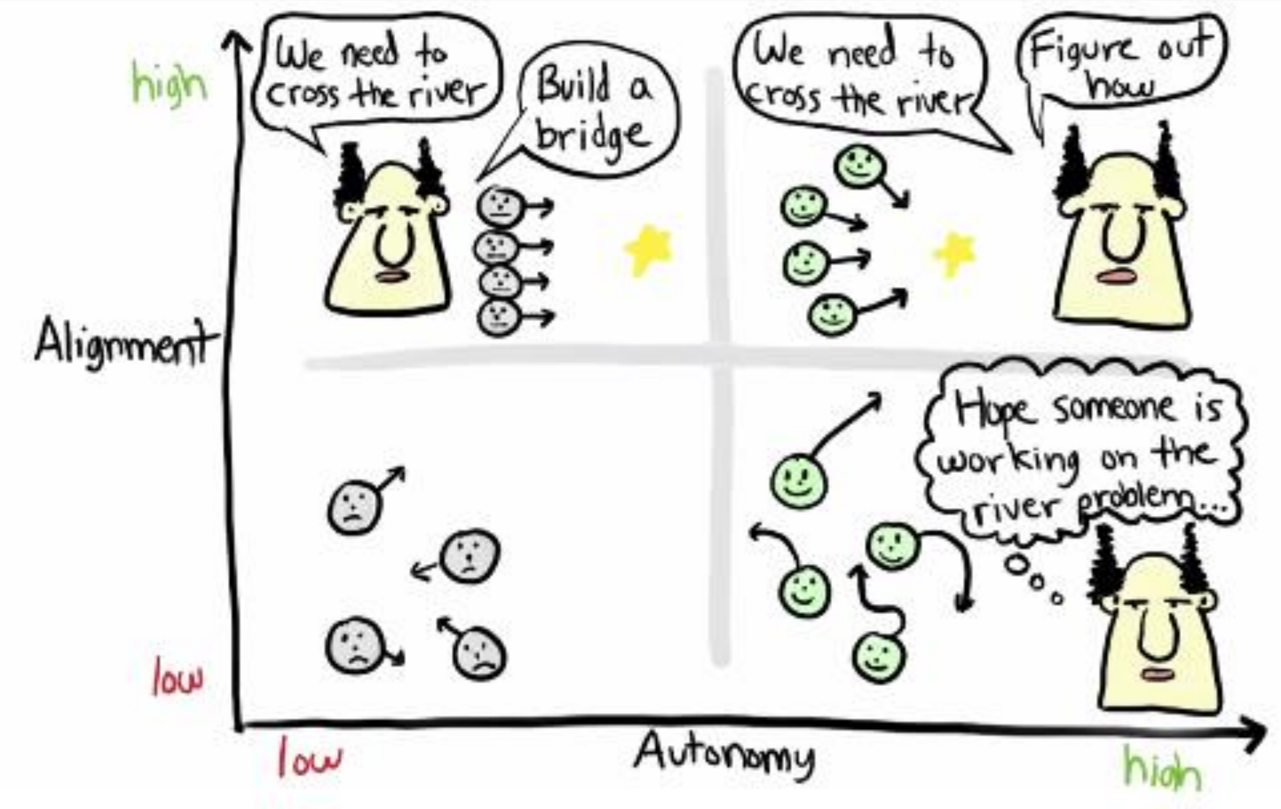
- #whoami

- Davide Cioccia
- Security Engineer @ ING Bank NL
- Italian leaving in the NL
- +7 years security experience
- Security magazines and OWASP MSTG contributor
- Focus:
  - Mobile application security
  - SSDLC
  - PT & VA
  - Incident Response

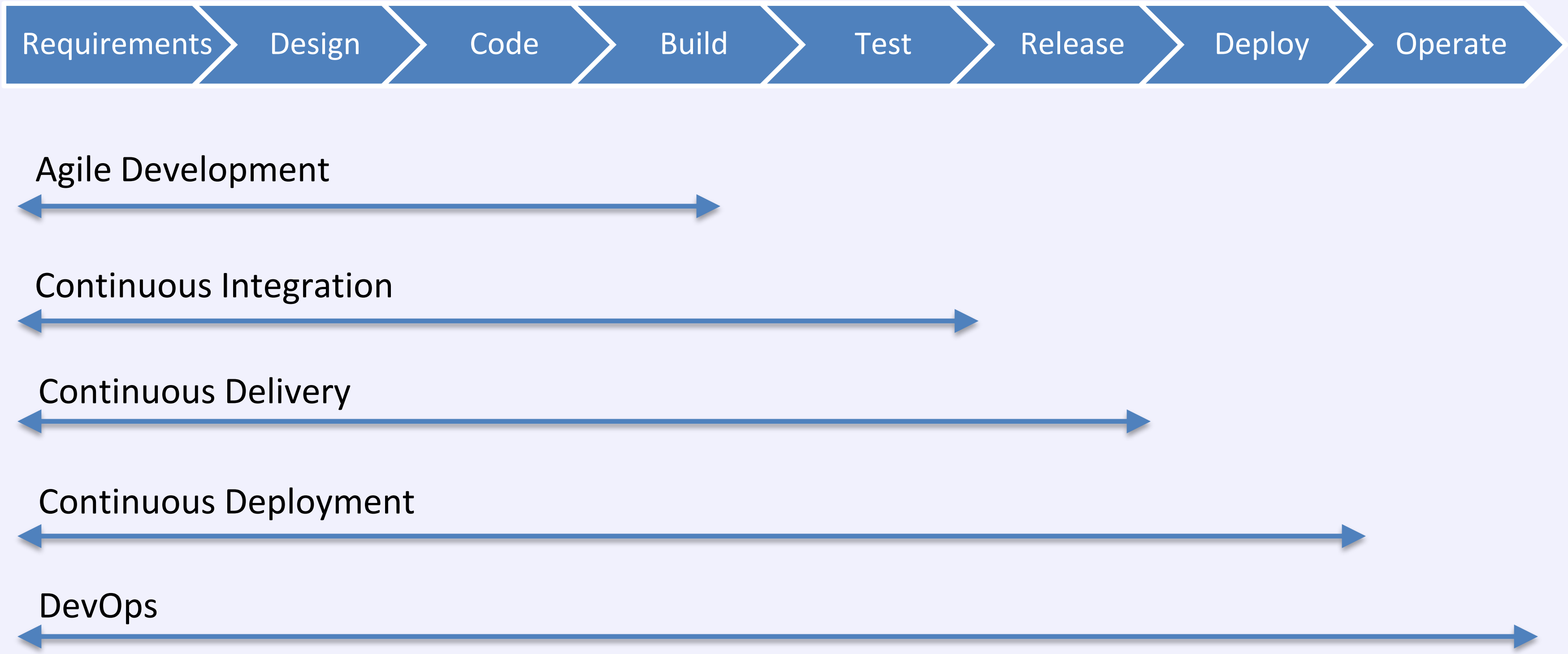
- Contacts:
  - davide.cioccia@owasp.com
  - davidecioccia.com

ING

- Agile Way of Working


high
We need to cross the river
Build a bridge
We need to cross the river
Figure out how
Alignment
Hope someone is working on the river problem...
low
low
Autonomy
high

- CI\CD



Requirements → Design → Code → Build → Test → Release → Deploy → Operate

Agile Development

Continuous Integration

Continuous Delivery

Continuous Deployment

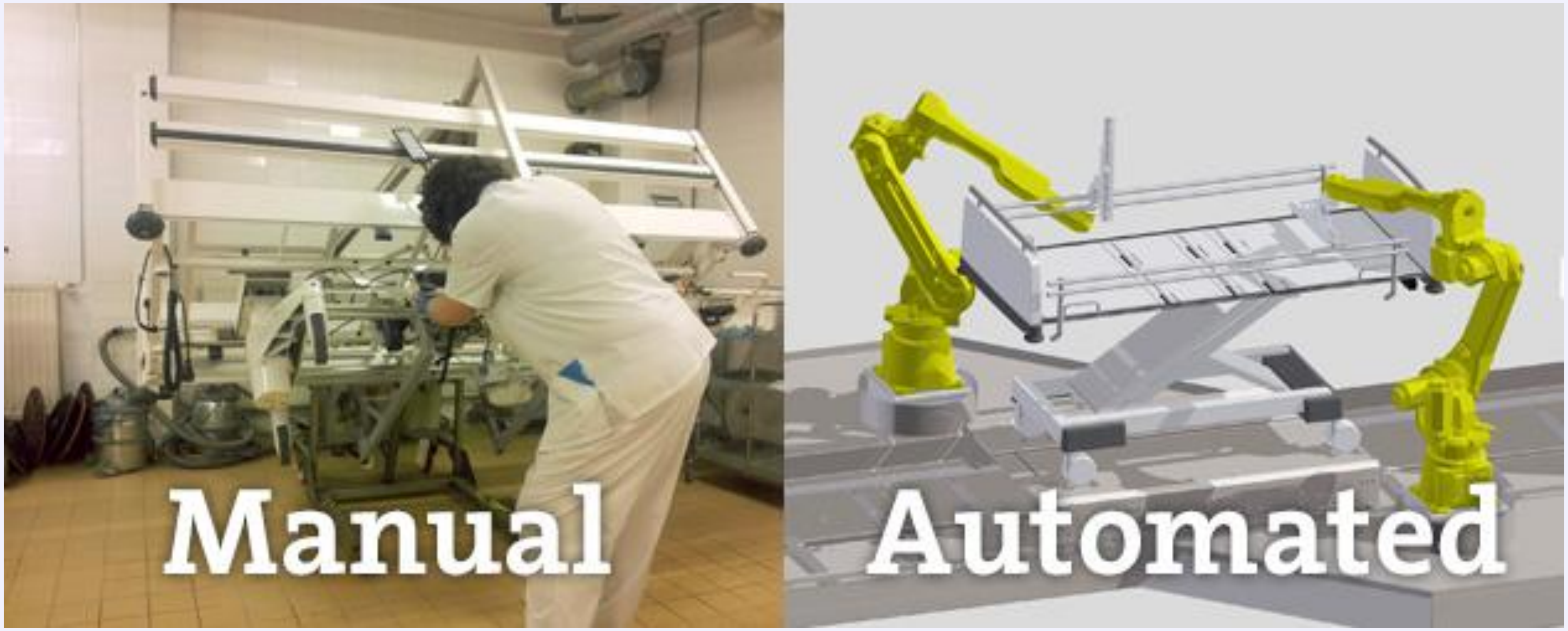
DevOps

- Security challenges

  - **Technical**:
    - Provide security at the DevOps speed
    - Detect vulnerabilities in early stage
    - Have developers understand security
    - Have Pentesters focus on “serious” stuff

  - **Business**
    - Lower cost to fix
    - Lower time to fix
    - Lower time for testing
    - Lower time to market

- Manual vs Automation



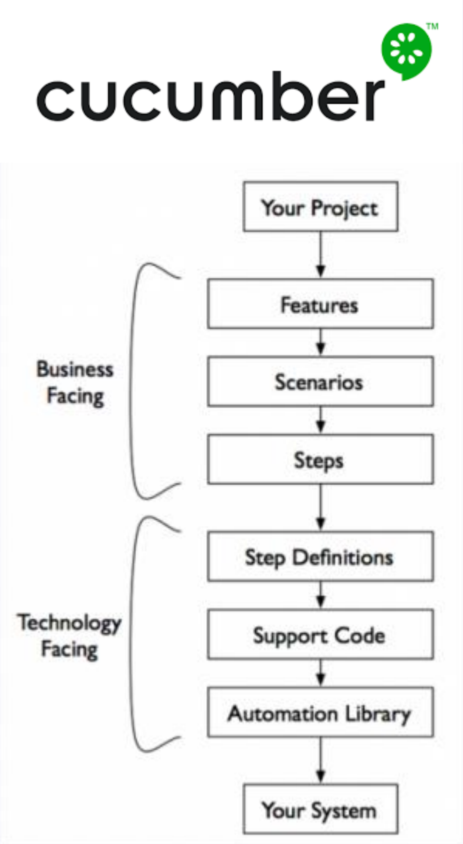
- Automate the testing: the biggest problem

- Solution: BDD Testing

Describe the behavior
of your software
in a very understandable
language

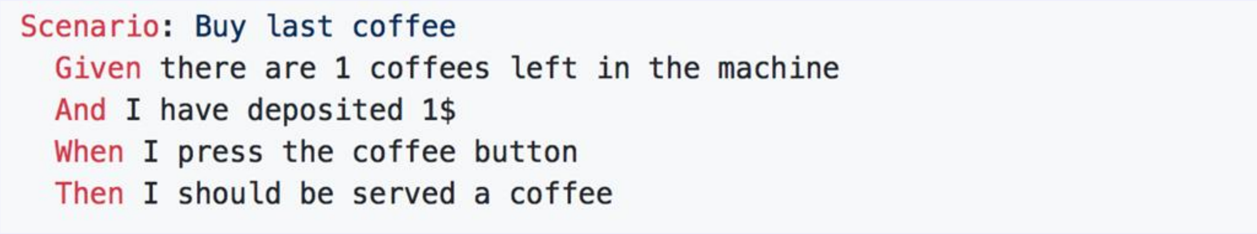
- Solution: BDD Testing with Cucumber and Gherkin

  - Automated
  - Understandable by all the stakeholders
  - It fits in the workflow of CI/CD



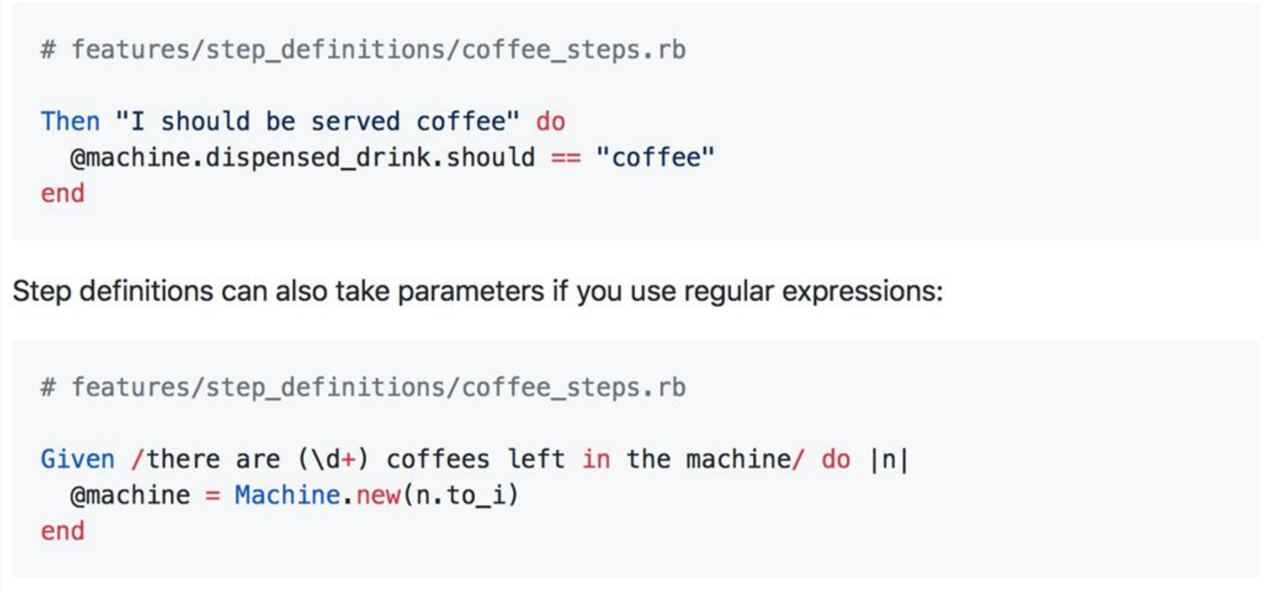
- BDD Testing

Business facing



```
Scenario: Buy last coffee
  Given there are 1 coffees left in the machine
  And I have deposited 1$
  When I press the coffee button
  Then I should be served a coffee
```

Technology facing



```
# features/step_definitions/coffee_steps.rb

Then "I should be served coffee" do
  @machine.dispensed_drink.should == "coffee"
end
```

Step definitions can also take parameters if you use regular expressions:

```
# features/step_definitions/coffee_steps.rb

Given /there are (\d+) coffees left in the machine/ do |n|
  @machine = Machine.new(n.to_i)
end
```

- BDD security tests
  - Different frameworks available in the market
  - Usage of PT tools, such as Nessus, ZAP, Burp etc
  - Focused on server side testing (API, Web Services..)

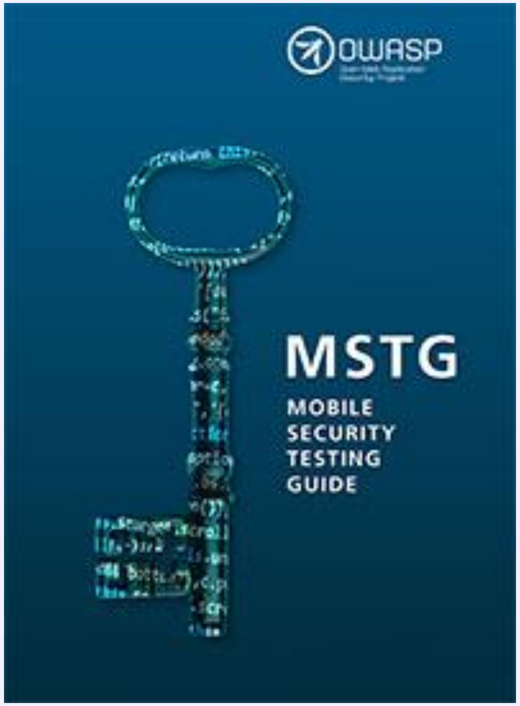
- Mobile BDD security tests?

- Mobile BDD security tests?

- Main problems
  - different Operating Systems
  - client side testing
  - different apps (native, hybrid,web)
  - different security controls
  - different way of testing (iOS, Android, ~~Windows Phone~~)

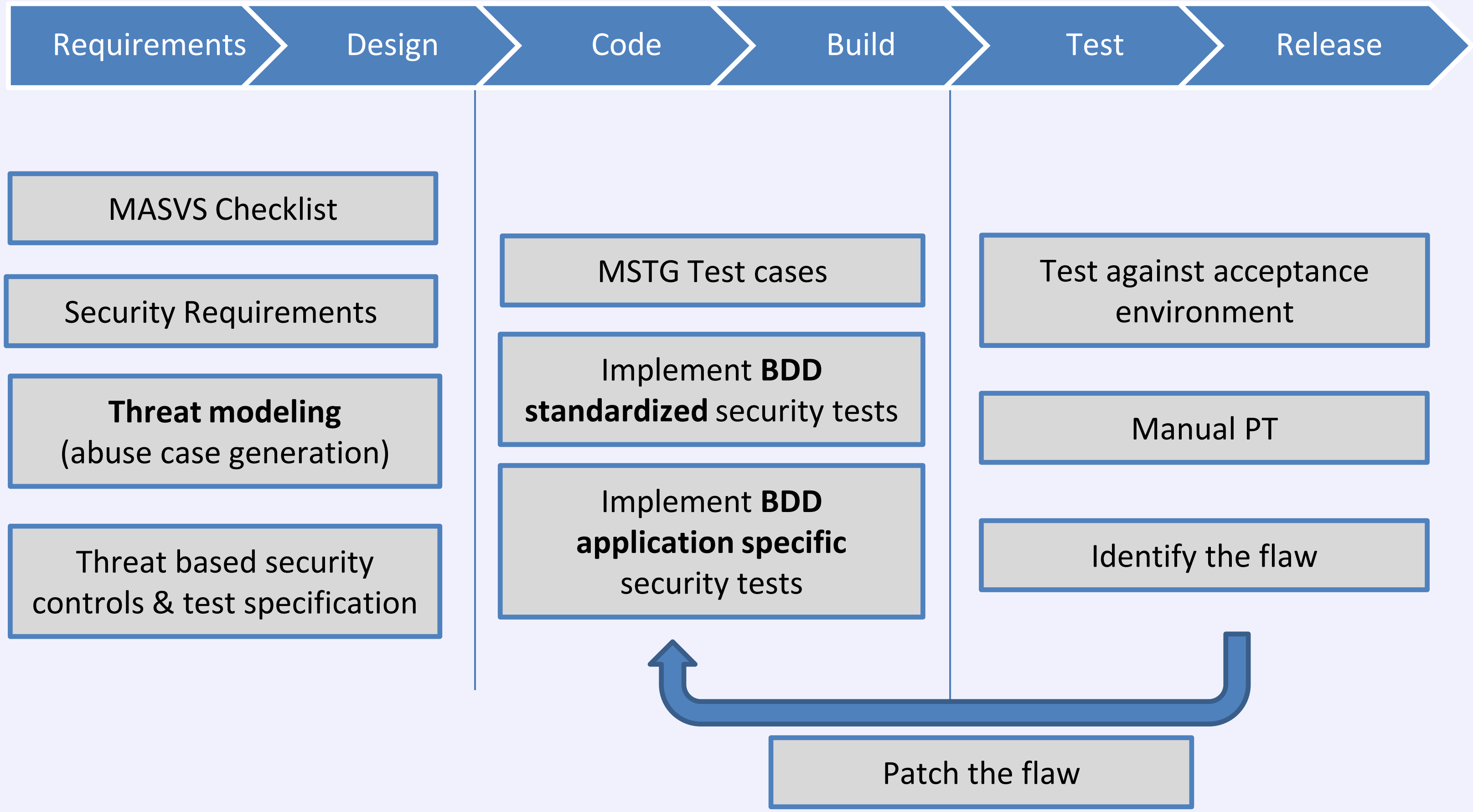
How to fix these problems?

- We need a security standard for Mobile Testing



OWASP
Standard
0.9
pre-release
Mobile AppSec Verification
Project Leaders: Bernhard Mueller and Sven Schleier
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

- We need a process



Requirements → Design → Code → Build → Test → Release

MASVS Checklist

Security Requirements

Threat modeling
(abuse case generation)

Threat based security controls & test specification

MSTG Test cases

Implement **BDD standardized** security tests

Implement **BDD application specific** security tests

Test against acceptance environment

Manual PT

Identify the flaw

Patch the flaw

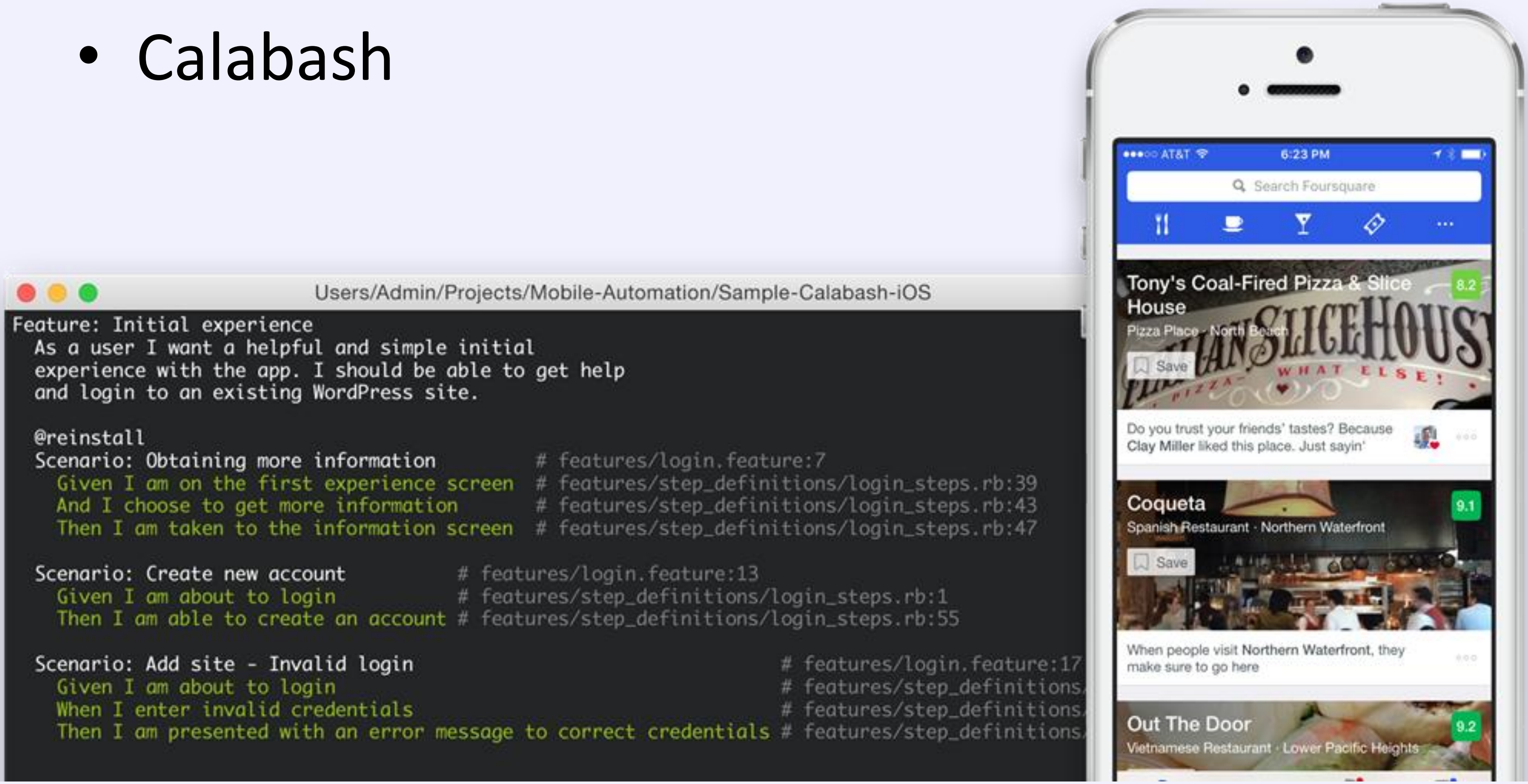
- We need a tool

  - Cross platform (Android, iOS), we just cut Windows Phone off right?
  - Support for hybrid apps
  - Running on emulators
  - Running on real devices
  - Possibility to integrate it in the CI/CD
  - Support for Gherkin syntax
  - A lot of customization
  - Free! (We like that :D)

- And the winner is …

calaba.sh

- Calabash



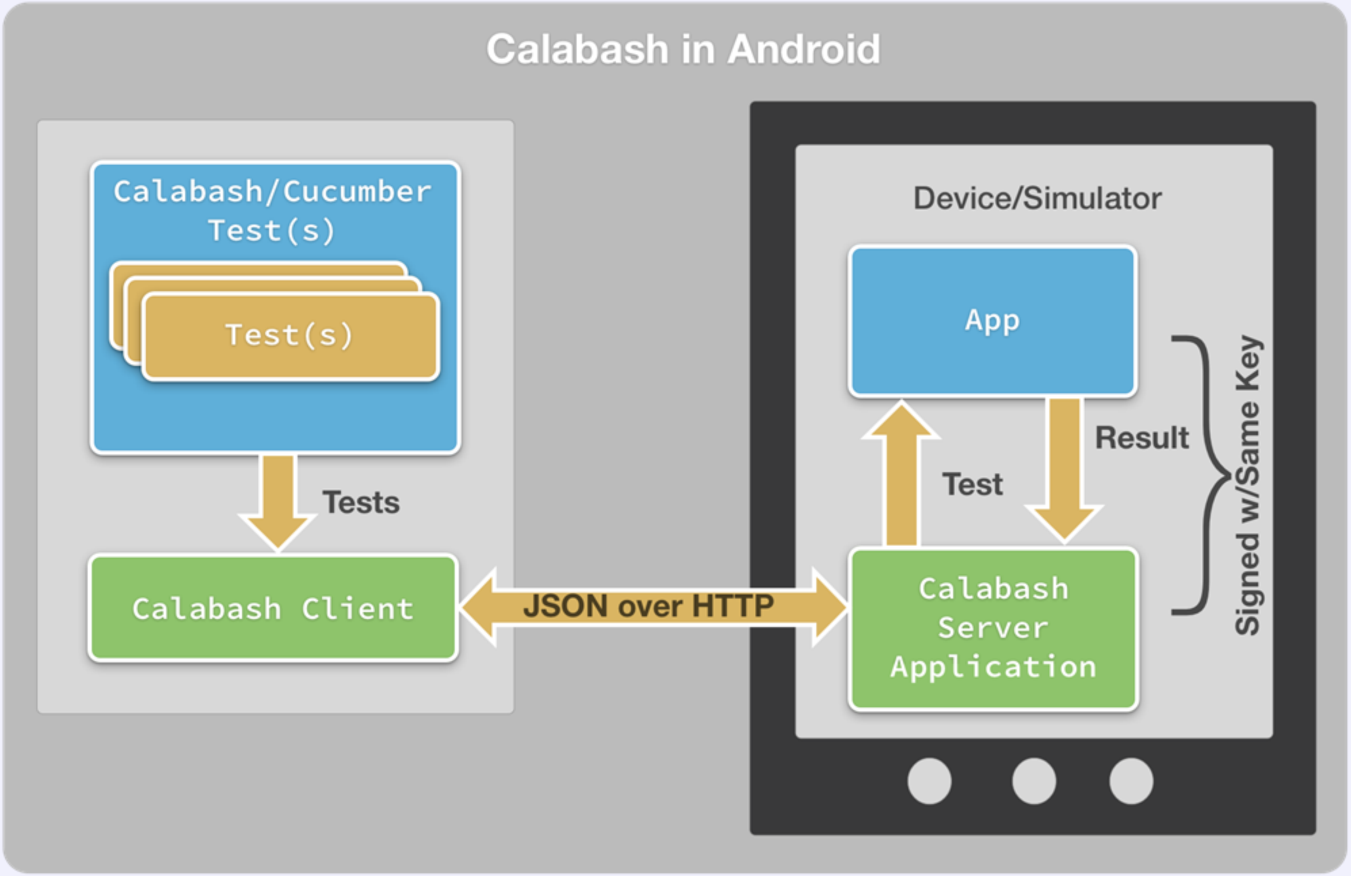
```
Feature: Initial experience
  As a user I want a helpful and simple initial
  experience with the app. I should be able to get help
  and login to an existing WordPress site.

  @reinstall
  Scenario: Obtaining more information         # features/login.feature:7
    Given I am on the first experience screen  # features/step_definitions/login_steps.rb:39
    And I choose to get more information       # features/step_definitions/login_steps.rb:43
    Then I am taken to the information screen  # features/step_definitions/login_steps.rb:47

  Scenario: Create new account          # features/login.feature:13
    Given I am about to login           # features/step_definitions/login_steps.rb:1
    Then I am able to create an account # features/step_definitions/login_steps.rb:55

  Scenario: Add site - Invalid login                             # features/login.feature:17
    Given I am about to login                                    # features/step_definitions
    When I enter invalid credentials                             # features/step_definitions
    Then I am presented with an error message to correct credentials # features/step_definitions
```

●●●○○ AT&T
6:23 PM
Search Foursquare
Tony's Coal-Fired Pizza & Slice House
8.2
Pizza Place · North Beach
Save
Coqueta
9.1
Spanish Restaurant · Northern Waterfront
Save
Out The Door
9.2
Vietnamese Restaurant · Lower Pacific Heights

Do you trust your friends' tastes? Because Clay Miller liked this place. Just sayin'

When people visit Northern Waterfront, they make sure to go here

- Calabash


Calabash in Android
Calabash/Cucumber Test(s)
Test(s)
Tests
Calabash Client
JSON over HTTP
Device/Simulator
App
Test
Result
Calabash Server Application
Signed w/Same Key

- Integration with with other mobile security frameworks

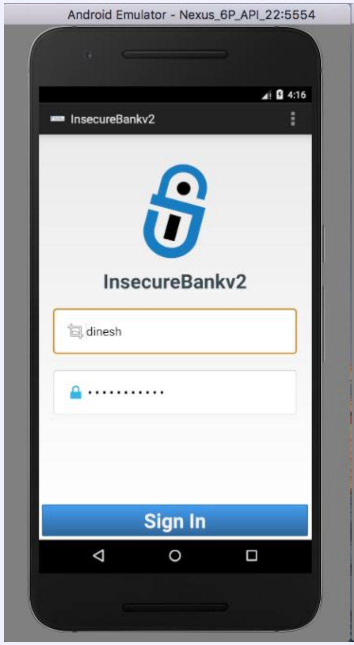
  - Pentest frameworks for Android and iOS
  - Automate manual activities
  - ***scriptable***
  - the agent must run on the device

drozer

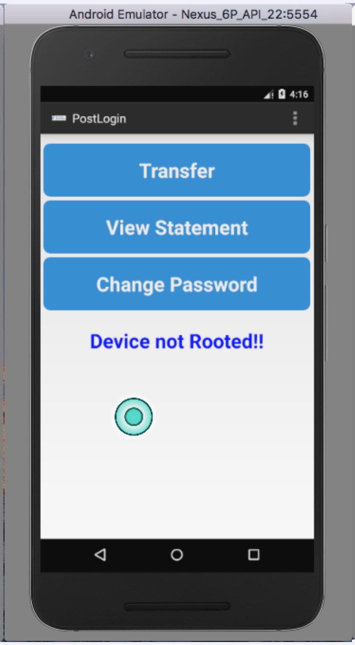
  – Powered by MWRlab

needle

Let’s try it out

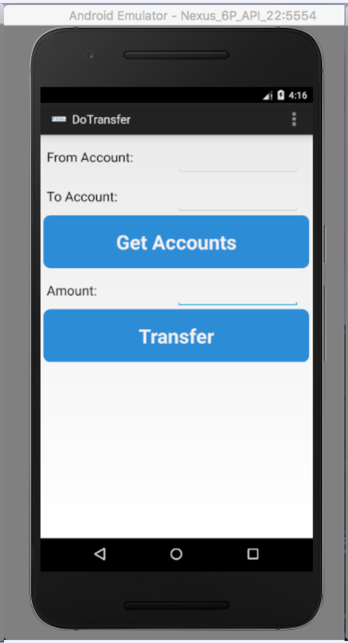


Android Emulator - Nexus_6P_API_22:5554



Android Emulator - Nexus_6P_API_22:5554

Device not Rooted!!

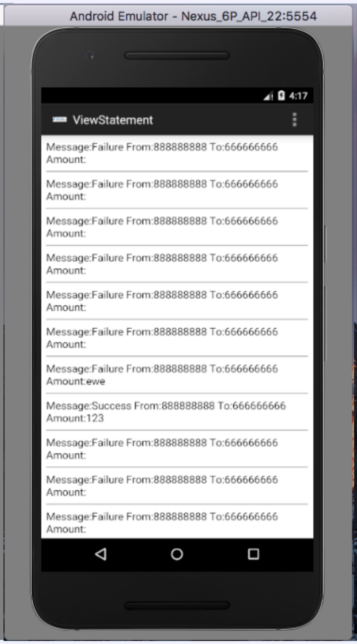


Android Emulator - Nexus_6P_API_22:5554

From Account:

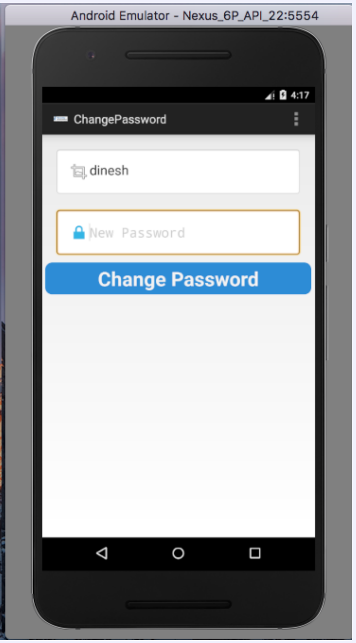
To Account:

Amount:



Android Emulator - Nexus_6P_API_22:5554

```
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:ewe
Message:Success From:888888888 To:666666666
Amount:123
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
Message:Failure From:888888888 To:666666666
Amount:
```



Android Emulator - Nexus_6P_API_22:5554

dinesh

New Password

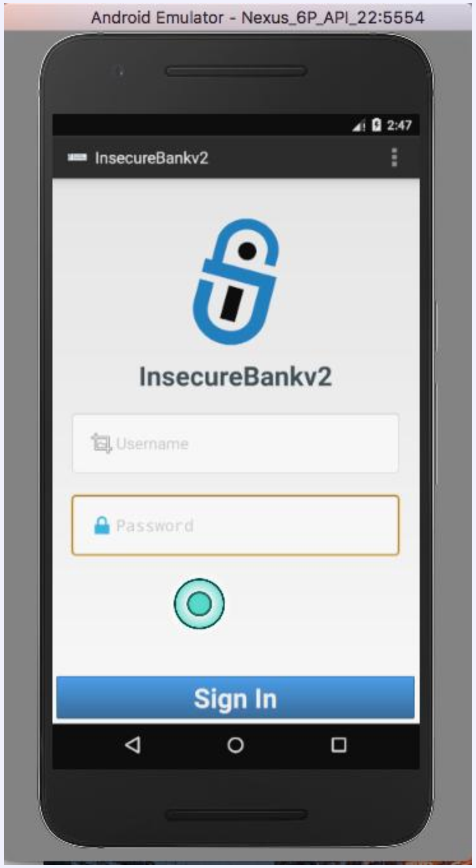
https://github.com/dineshshetty/Android-InsecureBankv2

- UC1: sensitive information in log file (standard test)
  - Requirements

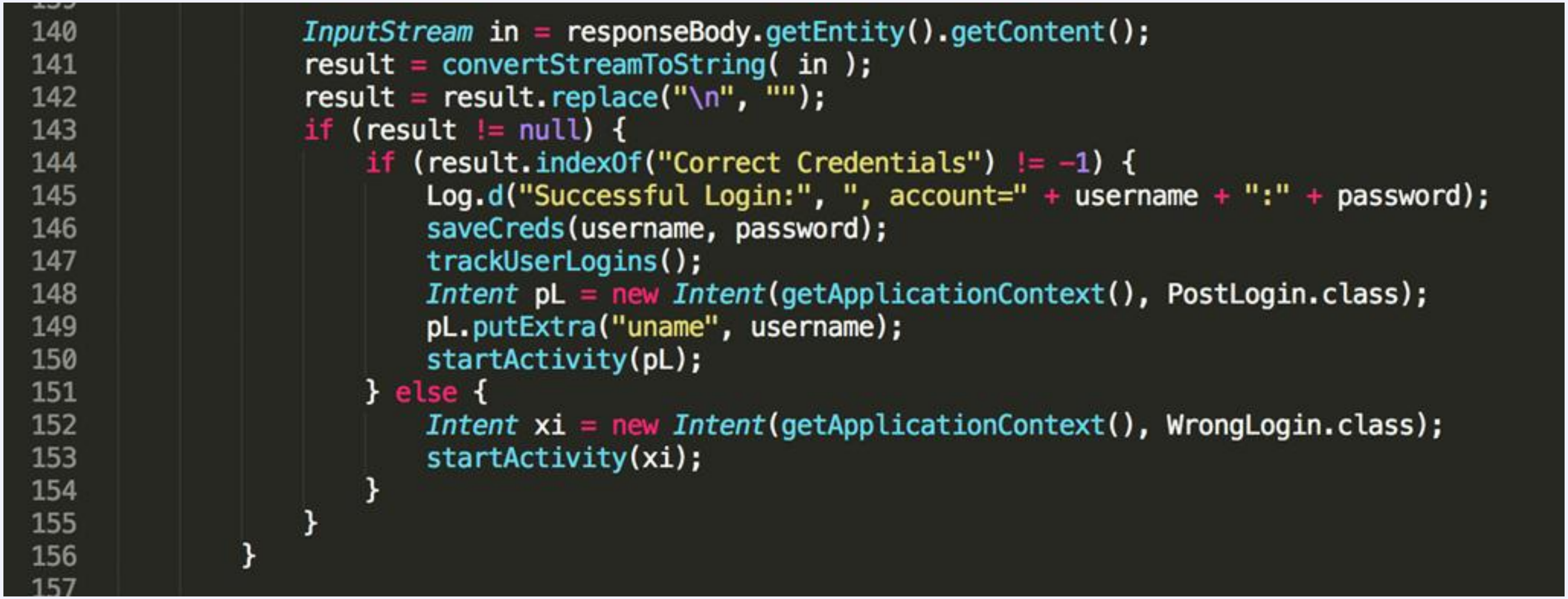
1. Logs must not contain usernames
2. Logs must not contain passwords
3. Logs must not contain information related to the user
4. Logs must not disclose sensitive information

MASVS V2 - Data Storage and Privacy

MSTG 2.1: Sensitive information in log files

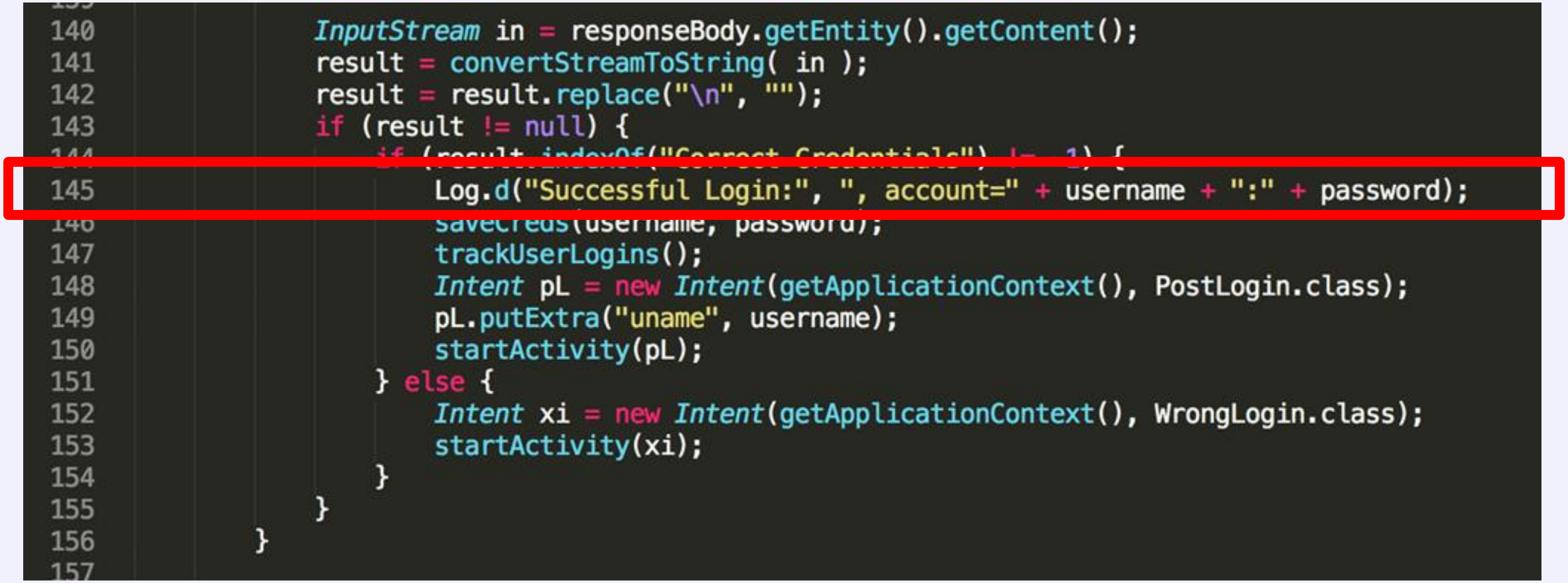


- What’s wrong here?



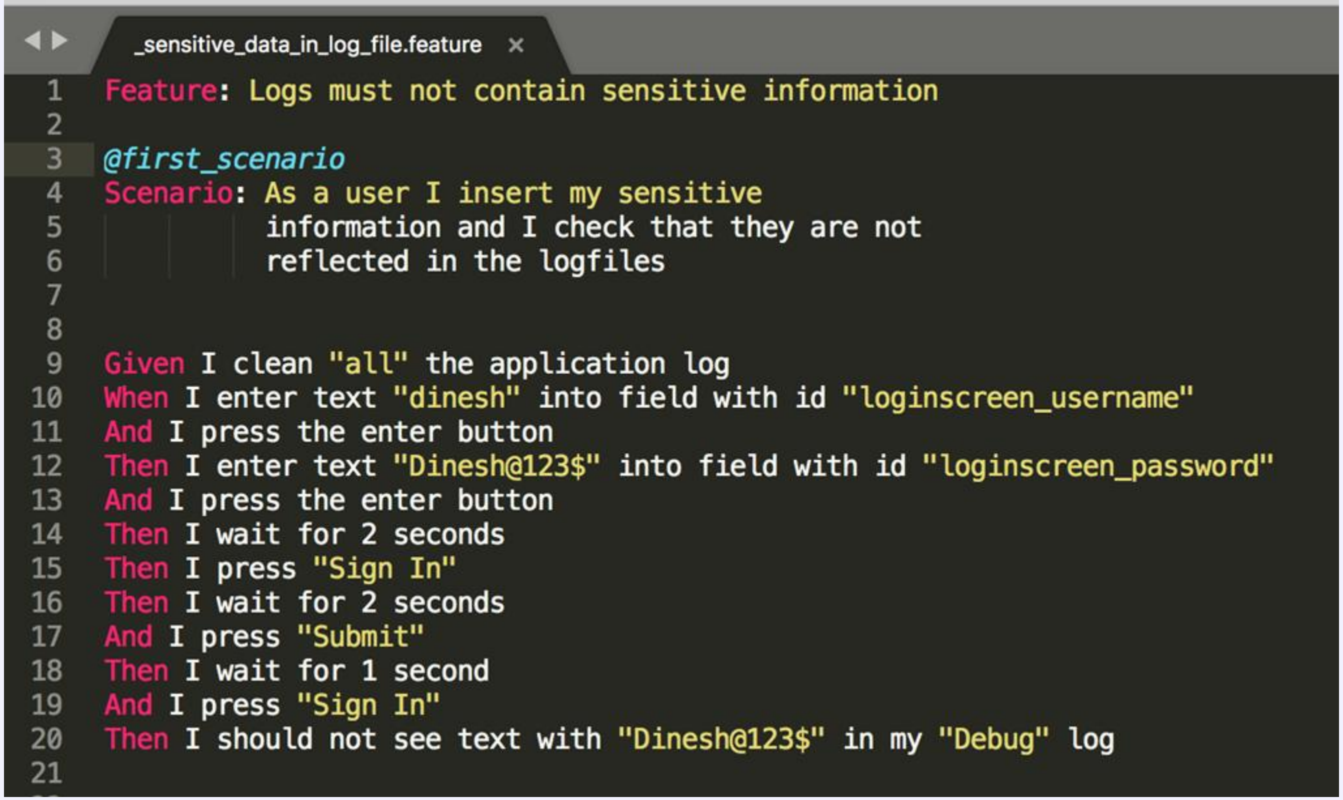
```
            InputStream in = responseBody.getEntity().getContent();
            result = convertStreamToString( in );
            result = result.replace("\n", "");
            if (result != null) {
                if (result.indexOf("Correct Credentials") != -1) {
                    Log.d("Successful Login:", ", account=" + username + ":" + password);
                    saveCreds(username, password);
                    trackUserLogins();
                    Intent pL = new Intent(getApplicationContext(), PostLogin.class);
                    pL.putExtra("uname", username);
                    startActivity(pL);
                } else {
                    Intent xi = new Intent(getApplicationContext(), WrongLogin.class);
                    startActivity(xi);
                }
            }
        }
```

- What's wrong here?



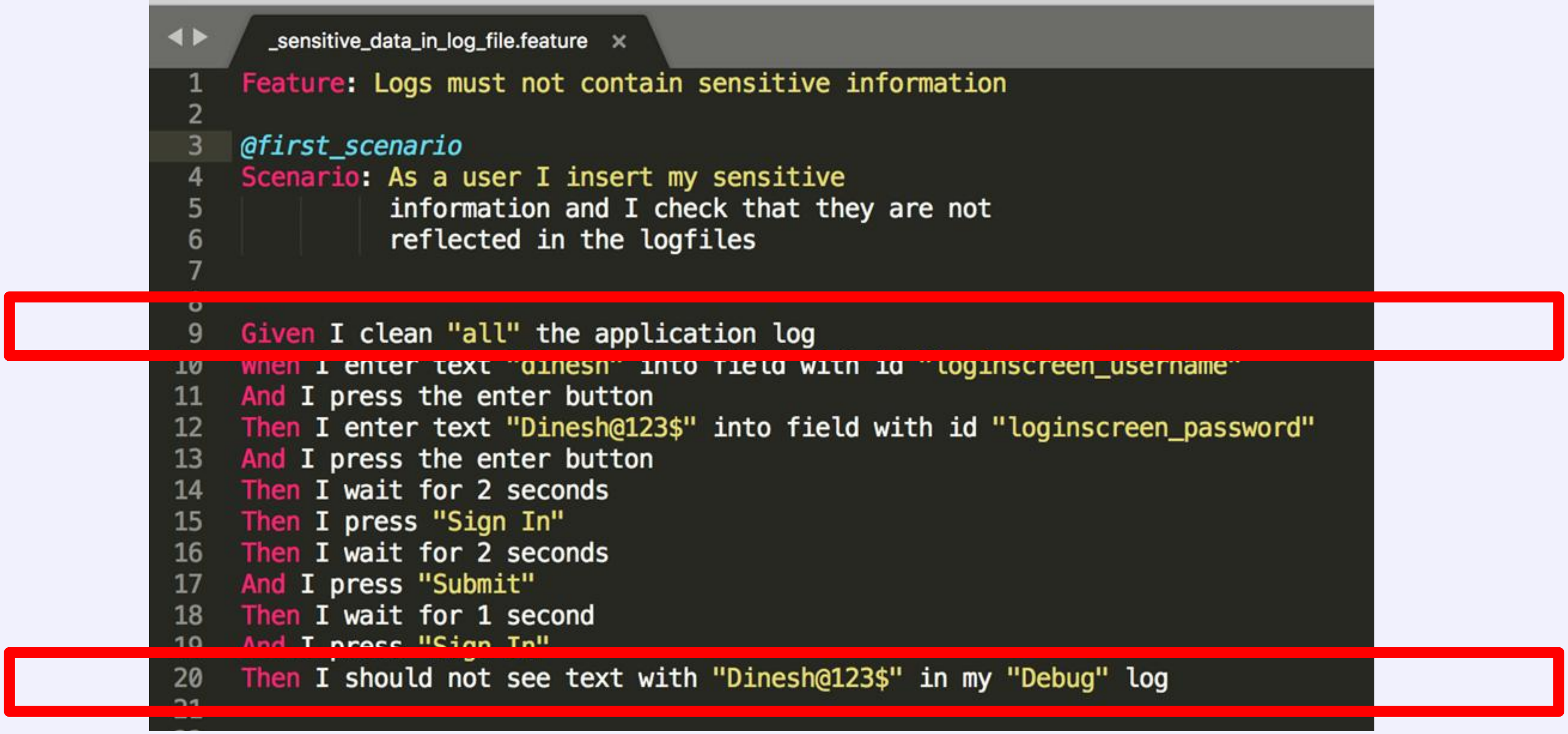
```
                InputStream in = responseBody.getEntity().getContent();
                result = convertStreamToString( in );
                result = result.replace("\n", "");
                if (result != null) {
                    if (result.indexOf("Correct Credentials") != -1) {
                        Log.d("Successful Login:", ", account=" + username + ":" + password);
                        saveCreds(username, password);
                        trackUserLogins();
                        Intent pL = new Intent(getApplicationContext(), PostLogin.class);
                        pL.putExtra("uname", username);
                        startActivity(pL);
                    } else {
                        Intent xi = new Intent(getApplicationContext(), WrongLogin.class);
                        startActivity(xi);
                    }
                }
            }
```

- Use case 1: sensitive information in log file
  - Feature



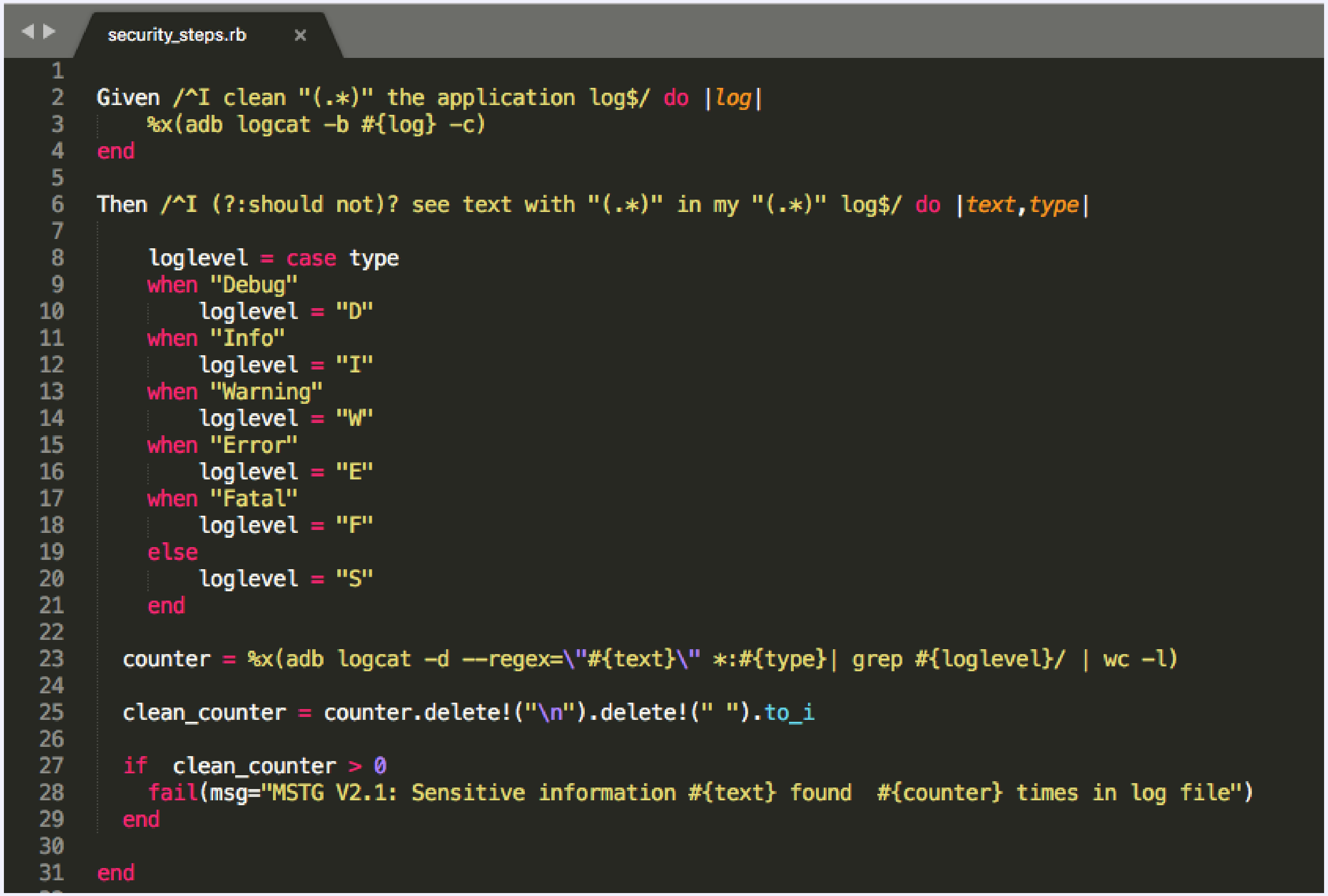
```
Feature: Logs must not contain sensitive information

@first_scenario
Scenario: As a user I insert my sensitive
          information and I check that they are not
          reflected in the logfiles


Given I clean "all" the application log
When I enter text "dinesh" into field with id "loginscreen_username"
And I press the enter button
Then I enter text "Dinesh@123$" into field with id "loginscreen_password"
And I press the enter button
Then I wait for 2 seconds
Then I press "Sign In"
Then I wait for 2 seconds
And I press "Submit"
Then I wait for 1 second
And I press "Sign In"
Then I should not see text with "Dinesh@123$" in my "Debug" log

```

- Use case 1: sensitive information in log file
  - Feature



```
Feature: Logs must not contain sensitive information

@first_scenario
Scenario: As a user I insert my sensitive
          information and I check that they are not
          reflected in the logfiles


Given I clean "all" the application log
When I enter text "dinesh" into field with id "loginscreen_username"
And I press the enter button
Then I enter text "Dinesh@123$" into field with id "loginscreen_password"
And I press the enter button
Then I wait for 2 seconds
Then I press "Sign In"
Then I wait for 2 seconds
And I press "Submit"
Then I wait for 1 second
And I press "Sign In"
Then I should not see text with "Dinesh@123$" in my "Debug" log
```

- Use case 1: sensitive information in log file
  - Step



```ruby

Given /^I clean "(.*)" the application log$/ do |log|
    %x(adb logcat -b #{log} -c)
end

Then /^I (?:should not)? see text with "(.*)" in my "(.*)" log$/ do |text,type|

    loglevel = case type
    when "Debug"
        loglevel = "D"
    when "Info"
        loglevel = "I"
    when "Warning"
        loglevel = "W"
    when "Error"
        loglevel = "E"
    when "Fatal"
        loglevel = "F"
    else
        loglevel = "S"
    end

  counter = %x(adb logcat -d --regex=\"#{text}\" *:#{type}| grep #{loglevel}/ | wc -l)

  clean_counter = counter.delete!("\n").delete!(" ").to_i

  if  clean_counter > 0
    fail(msg="MSTG V2.1: Sensitive information #{text} found  #{counter} times in log file")
  end

end
```

- Similar tests implemented

  - Sensitive data in the clipboard

    -
      ```
      adb shell su <uid> service call
      clipboard 2 s16 <package_name>
      ```
  - Sensitive data in keyboard cache
    - query
      ```
      /data/data/com.android.providers.user
      dictionary/databases/user_dict.db
      ```

- Use case 2: Internal activities must not be exported
  - Requirements

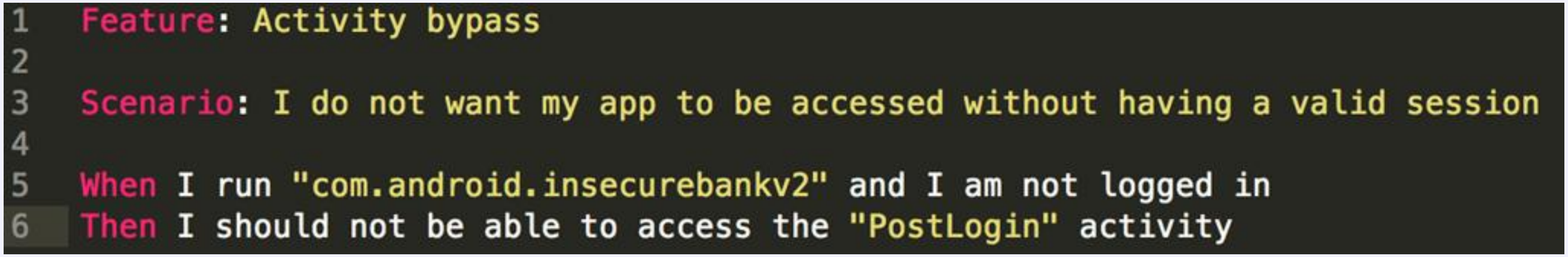
1. The only exported activity must be the login
2. Internal activities should have the flag exported set to false

MASVS:

V6 - Platform Interaction

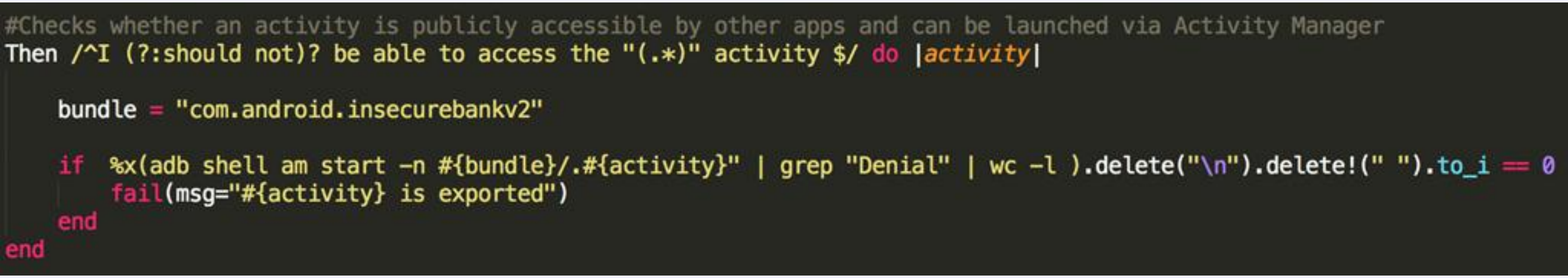
V4 - Authentication and Session Management

- Use case 2: Internal activities must not be exported
  - Feature



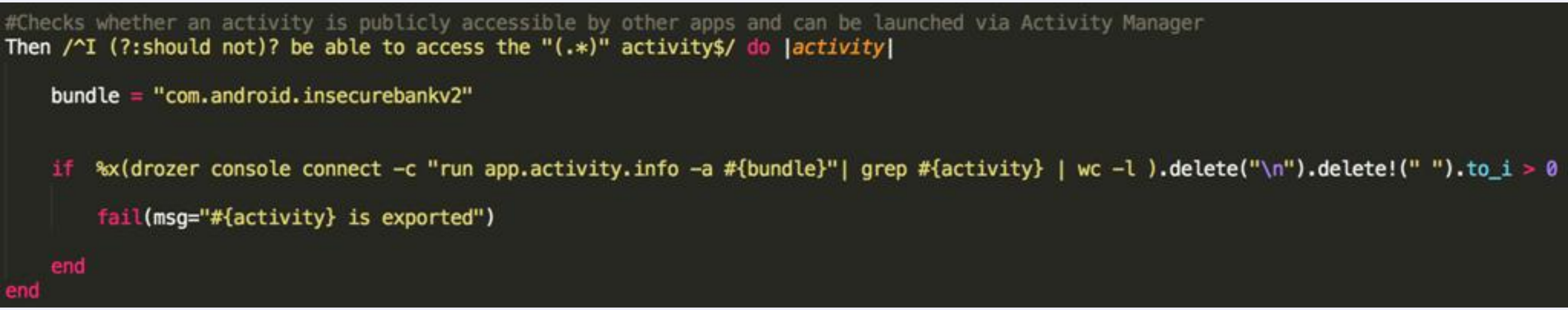
```
Feature: Activity bypass

Scenario: I do not want my app to be accessed without having a valid session

When I run "com.android.insecurebankv2" and I am not logged in
Then I should not be able to access the "PostLogin" activity
```

- Use case 2: Internal activities must not be exported
  - Step without Drozer



```
#Checks whether an activity is publicly accessible by other apps and can be launched via Activity Manager
Then /^I (?:should not)? be able to access the "(.*)" activity $/ do |activity|

    bundle = "com.android.insecurebankv2"

    if  %x(adb shell am start -n #{bundle}/.#{activity}" | grep "Denial" | wc -l ).delete("\n").delete!(" ").to_i == 0
        fail(msg="#{activity} is exported")
    end
end
```

- Use case 2: Internal activities must not be exported
  - Step with Drozer



```
#Checks whether an activity is publicly accessible by other apps and can be launched via Activity Manager
Then /^I (?:should not)? be able to access the "(.*)" activity$/ do |activity|

    bundle = "com.android.insecurebankv2"


    if  %x(drozer console connect -c "run app.activity.info -a #{bundle}"| grep #{activity} | wc -l ).delete("\n").delete!(" ").to_i > 0

        fail(msg="#{activity} is exported")

    end
end
```

- Use case 3: JavaScript in WebView must be disabled
  - Requirements

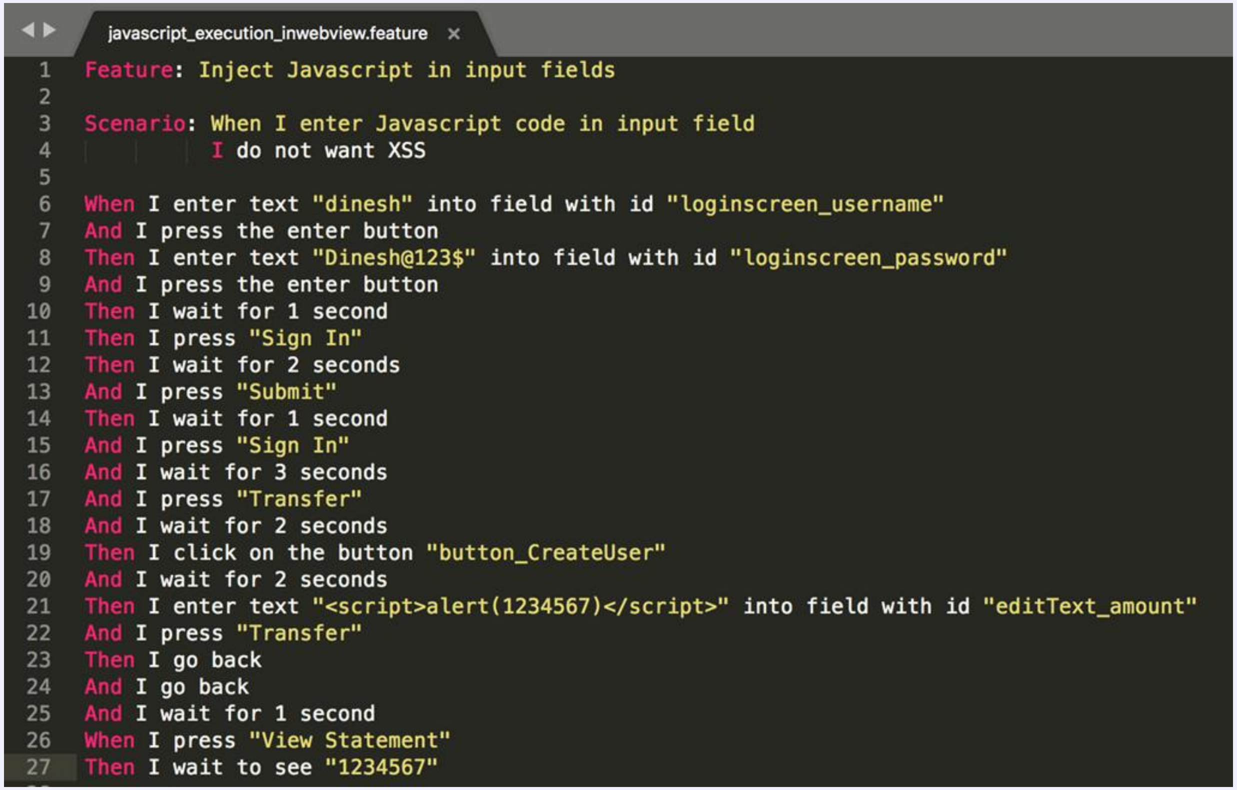
1. The Webview must not execute JavaScript code
2. If an input is reflected in the WebView it must be sanitized

MASVS V6: Platform interaction

MSTG:

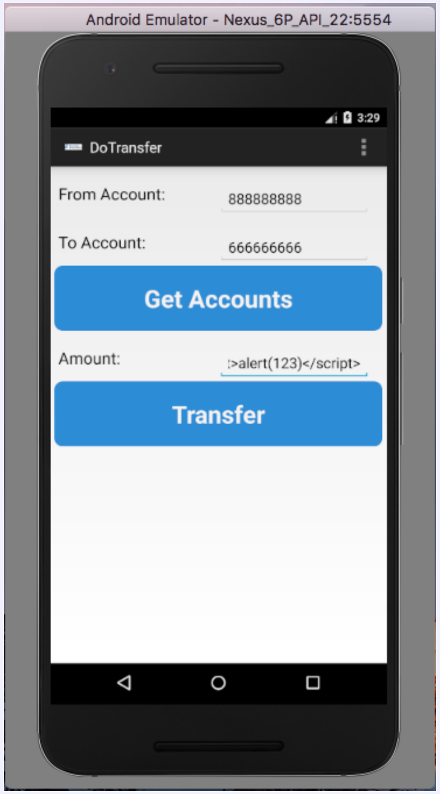
V6.5: JavaScript is disabled in WebViews unless explicitly required.

- Use case 3: JavaScript in WebView must be disabled
  - Feature



```
Feature: Inject Javascript in input fields

Scenario: When I enter Javascript code in input field
          I do not want XSS

When I enter text "dinesh" into field with id "loginscreen_username"
And I press the enter button
Then I enter text "Dinesh@123$" into field with id "loginscreen_password"
And I press the enter button
Then I wait for 1 second
Then I press "Sign In"
Then I wait for 2 seconds
And I press "Submit"
Then I wait for 1 second
And I press "Sign In"
And I wait for 3 seconds
And I press "Transfer"
And I wait for 2 seconds
Then I click on the button "button_CreateUser"
And I wait for 2 seconds
Then I enter text "<script>alert(1234567)</script>" into field with id "editText_amount"
And I press "Transfer"
Then I go back
And I go back
And I wait for 1 second
When I press "View Statement"
Then I wait to see "1234567"
```

- Use case 3: JavaScript in WebView must be disabled



Android Emulator - Nexus_6P_API_22:5554

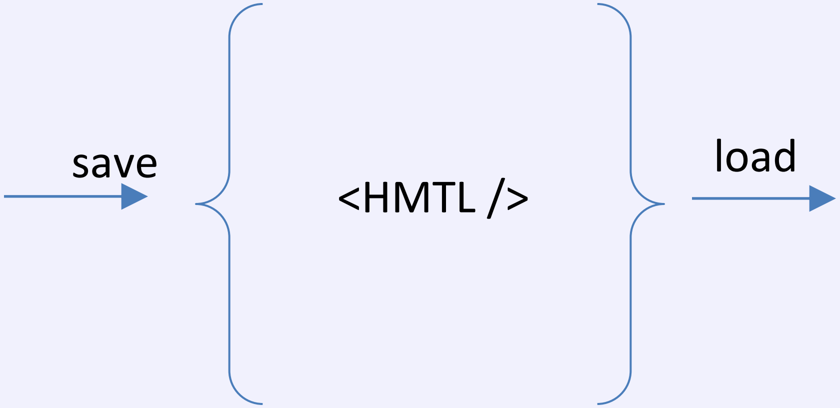
3:29

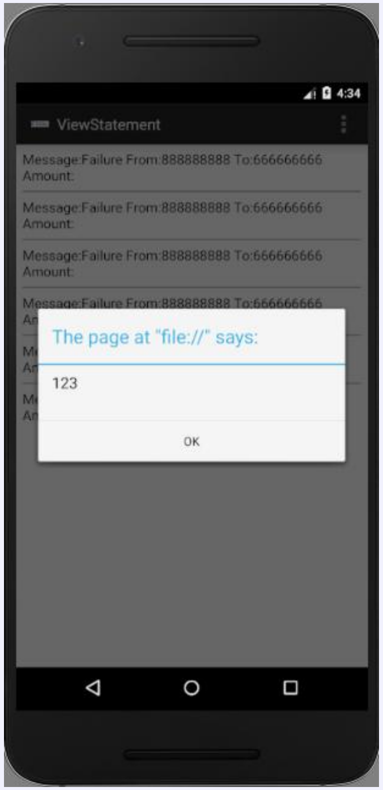
DoTransfer

From Account: 888888888

To Account: 666666666

Amount: t>alert(123)</script>





4:34

ViewStatement

Message:Failure From:888888888 To:666666666
Amount:

Message:Failure From:888888888 To:666666666
Amount:

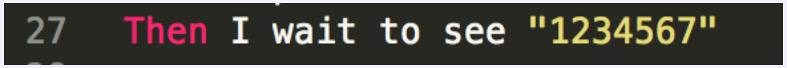
Message:Failure From:888888888 To:666666666
Amount:

Message:Failure From:888888888 To:666666666

The page at "file://" says:

123

- Use case 3: JavaScript in WebView must be disabled
  - Step



```
Then I wait to see "1234567"
```

- Provided by calabash
- Checks if an alert box is executed and contains the text specified

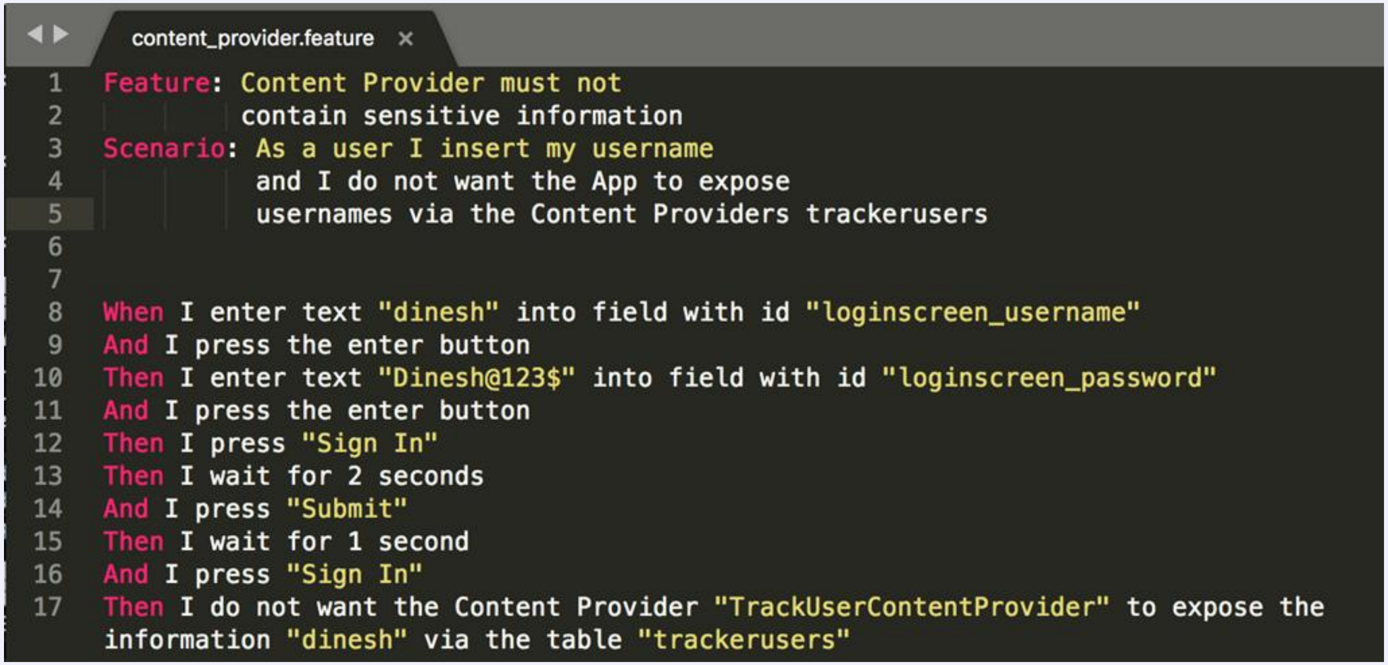
- Use case 4: Content provider information disclosure
  - Requirements

1. Content Providers must not expose sensitive information
2. Content Providers must not be exported if there are no other apps from the same developer
3. Content Providers must use **android:export = false** instead of **android:export = true**

MASVS V6: Platform Interaction

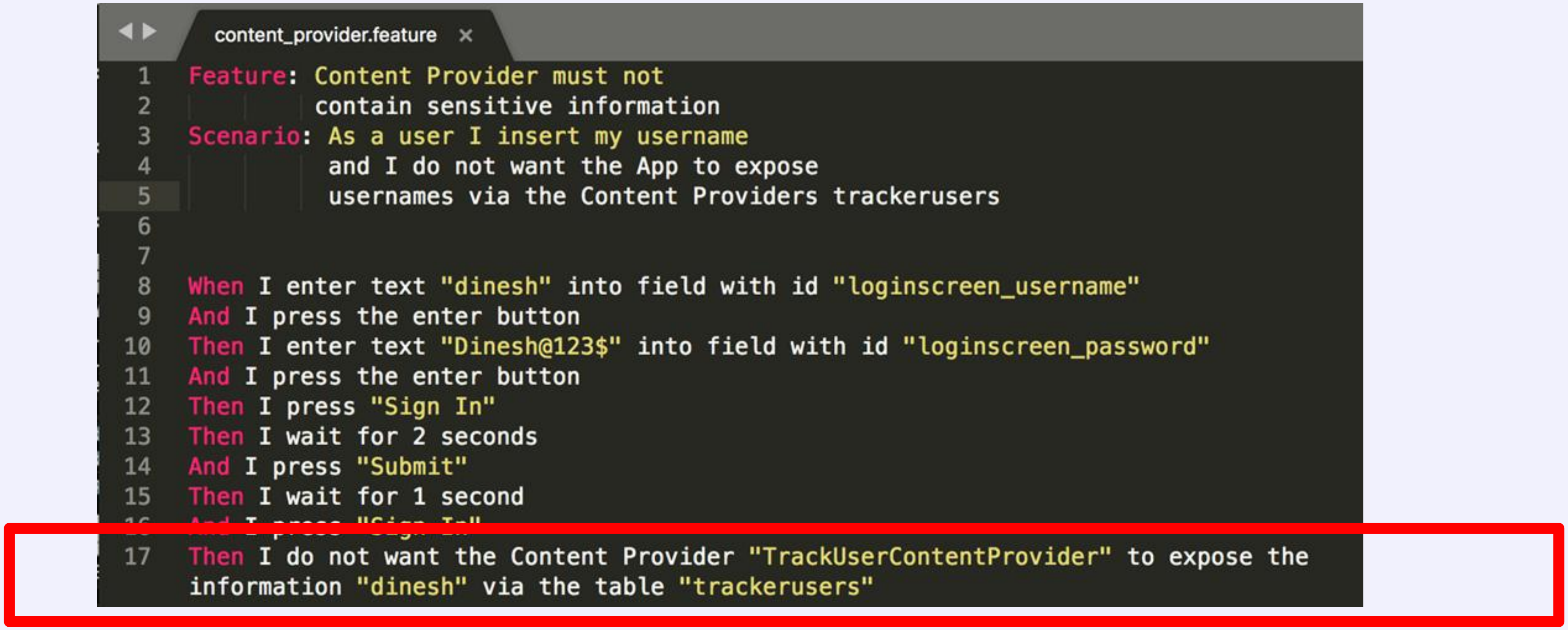
MSTG: Testing Platform Interaction on Android

- Use case 4: Content provider information disclosure
  - Feature



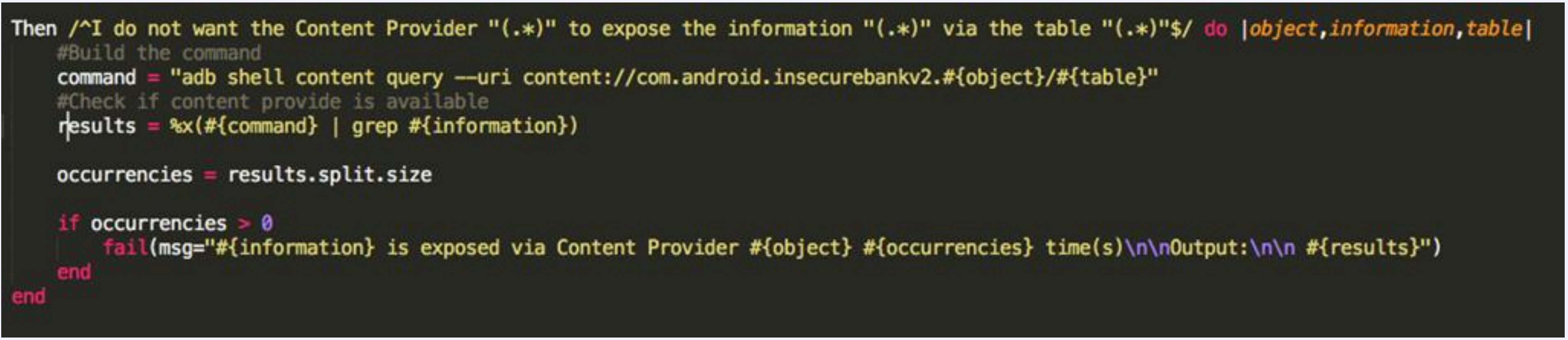
```
Feature: Content Provider must not
         contain sensitive information
Scenario: As a user I insert my username
          and I do not want the App to expose
          usernames via the Content Providers trackerusers


When I enter text "dinesh" into field with id "loginscreen_username"
And I press the enter button
Then I enter text "Dinesh@123$" into field with id "loginscreen_password"
And I press the enter button
Then I press "Sign In"
Then I wait for 2 seconds
And I press "Submit"
Then I wait for 1 second
And I press "Sign In"
Then I do not want the Content Provider "TrackUserContentProvider" to expose the
information "dinesh" via the table "trackerusers"
```

- Use case 4: Content provider information disclosure
  - Feature



```
Feature: Content Provider must not
         contain sensitive information
Scenario: As a user I insert my username
          and I do not want the App to expose
          usernames via the Content Providers trackerusers


When I enter text "dinesh" into field with id "loginscreen_username"
And I press the enter button
Then I enter text "Dinesh@123$" into field with id "loginscreen_password"
And I press the enter button
Then I press "Sign In"
Then I wait for 2 seconds
And I press "Submit"
Then I wait for 1 second
And I press "Sign In"
Then I do not want the Content Provider "TrackUserContentProvider" to expose the
information "dinesh" via the table "trackerusers"
```

- Use case 4: Content provider information disclosure
  - Step

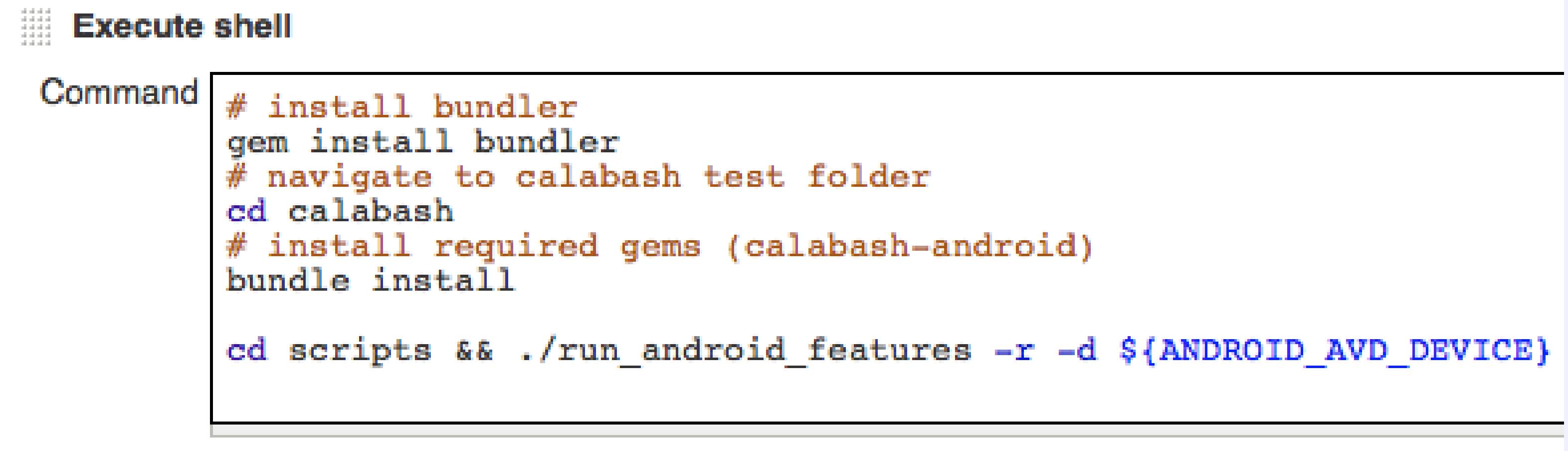


```
Then /^I do not want the Content Provider "(.*)" to expose the information "(.*)" via the table "(.*)"$/ do |object,information,table|
    #Build the command
    command = "adb shell content query --uri content://com.android.insecurebankv2.#{object}/#{table}"
    #Check if content provide is available
    results = %x(#{command} | grep #{information})

    occurrencies = results.split.size

    if occurrencies > 0
        fail(msg="#{information} is exposed via Content Provider #{object} #{occurrencies} time(s)\n\nOutput:\n\n #{results}")
    end
end
```

Other tests implemented:

- Exploit Broadcast Receivers
- Intent Sniffing
- Sensitive information in Pasteboard
- More…

- Integration with CI/CD (Jenkins)
  - Android emulator plugin
  - Add Gemfile to your workspace
  - Shell script



Execute shell

Command

```
# install bundler
gem install bundler
# navigate to calabash test folder
cd calabash
# install required gems (calabash-android)
bundle install

cd scripts && ./run_android_features -r -d ${ANDROID_AVD_DEVICE}
```

https://azevedorafaela.wordpress.com/2014/10/08/9-steps-to-configure-jenkins-with-calabashcucumber/

Improvements

- Include OWASP ZAP for API test
- Use the ”backdoor” feature to modify the code at runtime
- ?

DEMO

- Achievements
  - Speed
  - Quality
  - Accuracy
  - Scalability
  - Maturity

“Trying to speed project schedule by reducing testing is like trying to lose weight by donating blood”

Klaus Leopold

THANK YOU

Davide Cioccia
email: davide.cioccia@ing.nl
web: davidecioccia.com