BDD Mobile security testing with OWASP MASVS, OWASP MSTG and Calabash
• #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
• Agile Way of Working
• CI\CD

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?

ABSOLUTELY
NOTHING
• 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?

THIS IS HOW

TO FIX THAT PROBLEM
• We need a security standard for Mobile Testing
• We need a process

- Requirements
  - MASVS Checklist
  - Security Requirements
  - Threat modeling (abuse case generation)
  - Threat based security controls & test specification

- Design

- Code
  - MSTG Test cases
  - Implement BDD standardized security tests
  - Implement BDD application specific security tests

- Build

- Test
  - Test against acceptance environment
  - Manual PT
  - Identify the flaw

- Release

- 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
Given I am on the first experience screen
And I choose to get more information
Then I am taken to the information screen

Scenario: Create new account
Given I am about to login
Then I am able to create an account

Scenario: Add site - Invalid login
Given I am about to login
When I enter invalid credentials
Then I am presented with an error message to correct credentials
• Calabash
• Integration with other mobile security frameworks

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

– Powered by MWRlab
Let’s try it out

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?
• What’s wrong here?

```java
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

```plaintext
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="\#{type}:\#{text}" | grep "#{loglevel}" | wc -l}
  clean_counter = counter.delete!("\n").delete(" ").to_i

  if clean_counter > 0
    fail(msg="MSV2.1: 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.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

```bash
#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
• 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

```javascript
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
• Use case 3: JavaScript in WebView must be disabled
  – Step

  ```plaintext
  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 provider is available
  results = %x(#{command} | grep #{information})
  occurrences = results.split.size
  if occurrences > 0
    fail("#{information} is exposed via Content Provider #{object} #{occurrences} 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

https://azevedorafaela.wordpress.com/2014/10/06/3-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