



# Narzędzia w testowaniu

Radosław  
Kowal  
04.09.2021

# Agenda



- 1) Wprowadzenie do narzędzi
- 2) Zarządzanie testami i incydentami
- 3) Narzędzia pomocnicze (robienie screenshotów, generatory)
- 4) Systemy kontroli wersji
- 5) Continuous Integration
- 6) Testy wydajnościowe
- 7) Testy webservice'ów
- 8) Testy bezpieczeństwa

# Czym są narzędzia testowe i po co nam one?



Są one wykorzystywane do czynności testowych przez zautomatyzowanie powtarzających się zadań lub wsparcie dla czynności testowych wykonywanych ręcznie takich jak: planowanie testów, projektowanie testów, raportowanie i monitorowanie testów

Automatyzacja czynności które zajmuje dużo czasu ręcznie (analiza statyczna)

Automatyzować czynności, które nie mogą być wykonane ręcznie (np. testy aplikacji klient-serwer na wielką skalę)

Poprawić „niezawodność testów” (np. przez automatyzację porównywanie dużej ilości danych lub symulacje)

# Przykładowe narzędzia



Zarządzanie błędami i testami

Tworzenie screenshotów i nagrywanie ekranu

Generatory

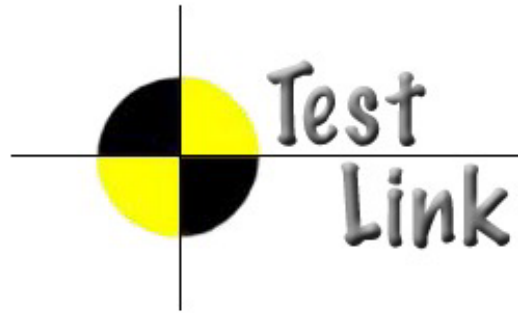
Wtyczki i konsole przeglądarkowe

Narzędzia do automatyzacji

Systemy kontroli wersji

Narzędzia do Continuous Integration

# Zarządzanie incydentami/testami





Bitnami Testlink (instalacja na własnym komputerze): <http://127.0.0.1/testlink>

testLink 1.8.2 : demo [admin]

Test Project My project

Start | Specyfikacja | Users | Events | Przypadek Testowy ID: UNE\_- | -documentation-

Panel użytkownika | Wyloguj

**Nawigator - Specyfikacja testów**

Nawigator Filtrowanie i Ustawienia

Test Suite

Update tree after every operation

Update tree

My project (0)

Test(0)

**Test Suite : Test**

New child Test Suite Edit Delete Test Suite Move/Copy Import Test Suite Export Test Suite

Utwórz przypadek testowy Importuj przypadek testowy Export child Test Cases Move/Copy Test Cases

**Test Suite : Test**

Details

Test

Słowa kluczowe : Brak

Attached files :

Upload new file



Secure | https://testerswp2.atlassian.net/browse/TES-13

Bookmarks iMacros Testing Welltok QBranch Admin QBranch Admin Environments - Well Environments - Well test Decline Cycle asda 0 Wiadomości DE4663: Program co Current cycles Current cycles Current cycles

**TESTED**  
Projekt oprogramow...

- Zaległości
- Aktywne sprinty
- Raporty
- Wydania
- Problemy** →
- Pages NOWY
- Komponenty
- Add item
- Ustawienia

TES-13

As a developer, I can update details on an item using the Detail View >> Click the "TES-13" link at the top of this card to open the detail view

Edytuj Komentarz Przydziel Do zrobienia W toku Gotowe Admin

Typ: **Błąd** Status: **DO ZROBIENIA**  
(Wyświetl przepływ pracy)

Priorytet: **Medium** Rozwiązanie: **Nierozwiązane**

Dotyczy Wersji: **Brak** Naprawione w Wersji: **Version 2.0**

Etykiety: **Brak**

Sprint: **Sample Sprint 2**

Przydzielony: **Patryk Raba**

Twórca: **Patryk Raba**

Głosy: **0**

Obserwatorzy: **0** [Obserwuj to zadanie](#)

Utworzone: **Tydzień temu**

Aktualizowane: **Tydzień temu**

**Agile**

Aktywny sprint: **Sample Sprint 2** kończy się 01/maj/18  
[Wyświetl na tablicy](#)

**Dyskusje HipChat**

Chcesz omówić ten problem? Połącz się z HipChat.

[Połącz](#) [Odrzuć](#)

**Opis**

**Editing using the Detail View**

Many of the fields in the detail view can be inline edited by simply clicking on them.  
For other fields you can open Quick Edit, select "Edit" from the cog drop-down.

**Załączniki**

Przeciągnij pliki tutaj aby je załączyć, lub [przeglądaj](#).

**Aktywność**

Wszystkie **Komentarze** Dziennik pracy Historia Zmian Działanie

**Patryk Raba** skomentował - Tydzień temu  
Joined Sample Sprint 2 7 days 9 hours 10 minutes ago



Projects / DPO

Main Board

## Sprint 108



4 days remaining

Complete sprint



Quick filters ▾

TO DO

IN PROGRESS

TESTING

DONE

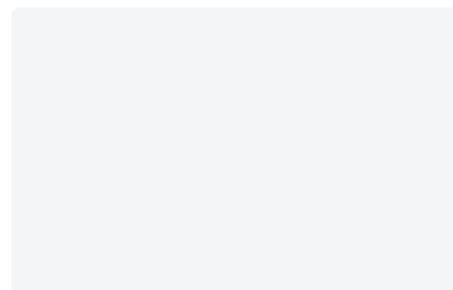
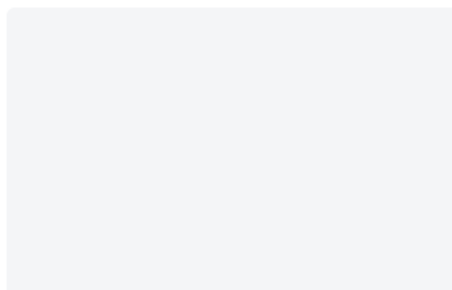
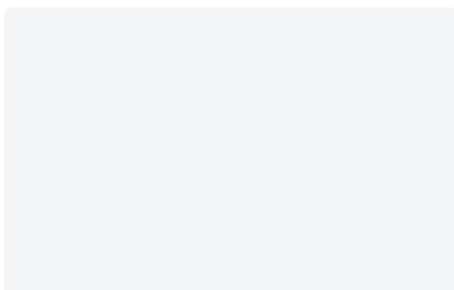
▼ DPO

-3050

REOPENED

1 sub-task Finalize authentication items

Move to Done

Disable admin login from  
connect request

DPO

-3204

▼ DPO

-3047

RESOLVED

2 sub-tasks Add empty page by customer

Frontend implementation



DPO

-3065

Backend implementation



DPO

-3066





## Sprint 6 | Android (AR27)



Pozostaje 14 dni

Ukończ sprint



15.01-29.01 Prio1: Release Candidate AR 23/24 ready (with hot fixes done). Prio2: Do as much rewrite as possible of Content Screens.



Szybkie filtry ▾

TO DO	IN PROGRESS	ON HOLD	CODE REVIEW	IN VERIFICATION	VERIFICATION DONE	DEVELOPMENT DONE
<div>Google Play - Passing the Zee5 system identifiers while</div> <div> </div> <div>AMA2-2887</div>	<div>Signed in user has access to "continue watching" items section</div> <div>CONTENT SCREE...</div> <div>  5 </div> <div>AMA2-61</div>	<div>CLONE - Add SSL certificate pins for securepayment.zee5.com</div> <div>SECURITY</div> <div> </div> <div>AMA2-2393</div>	<div>User can use JusPay payments in 2.0.1-rc.69 version</div> <div>Foundation</div> <div> </div> <div>AMA2-2521</div>	<div>Add caching support for consumption related rails</div> <div>BUILDING BLOCKS</div> <div>  5 </div> <div>AMA2-2155</div>	<div>ReWrite Search Module with Clean Architecture Principles</div> <div>CONTENT SCREE...</div> <div>  13 </div> <div>AMA2-292</div>	<div>Content must play in Landscape with Kaltura Player</div> <div>CONSUMPTION</div> <div>  5 </div> <div>AMA2-196</div>
<div>Google Play - Implement missing receipt API while app</div> <div> </div> <div>AMA2-2888</div>	<div>Rewritten Single Playback API Powered Player must be capable</div> <div>CONSUMPTION</div> <div>  5 </div> <div>AMA2-222</div>	<div>Mixpanel Implementation for Kids Safe- Enhanced Parental</div> <div>BUILDING BLOCKS</div> <div>  5</div> <div>AMA2-443</div>	<div>CLONE - User can use JusPay payments in 2.0.1-rc.69 version</div> <div>Foundation</div> <div> </div> <div>AMA2-2525</div>	<div>User should see upcoming shows in his country</div> <div>CONTENT SCREE...</div> <div>  5 </div> <div>AMA2-2712</div>	<div>Implementation of 401 Error handling in network layer of Android</div> <div>BUILDING BLOCKS</div> <div>  8 </div> <div>AMA2-527</div>	<div>AMA2-696 New cellsty...</div> <div>Unify date processing</div> <div> </div> <div>AMA2-2908</div>
<div>AMA2-61 Signed in us...</div> <div>User should the Continue Watching content on the</div> <div> </div> <div>AMA2-2972</div>	<div>Handling all Callback of IMA ads</div> <div> </div> <div>AMA2-277</div>	<div>Analysis of existing Analytics design and usage it in Search</div> <div>BUILDING BLOCKS</div> <div> </div> <div>AMA2-2657</div>	<div>User can see reminders screen</div> <div>CONTENT SCREE...</div> <div> </div> <div>AMA2-2657</div>	<div>Blocks HiPi Requests for the International IP user</div> <div> </div> <div>AMA2-2657</div>	<div>Old parental control is visible when kids safe remote flag is disabled</div> <div>SECURITY</div> <div> </div> <div>AMA2-1310</div>	<div>User must see hipi collection rails</div> <div>CONTENT SCREE...</div> <div>  5 </div> <div>AMA2-1310</div>



Before reporting a bug, please read the [bug writing guidelines](#), please look at the list of [most frequently reported bugs](#), and please [search](#) for the bug.

[Show Advanced Fields](#)

(\* = Required Field)

\* **Product:** OpenDemo.ORG **Reporter:** odoun54568

\* **Component:**

\* **Version:**  **Severity:**

**Hardware:**

**OS:**

We've made a guess at your operating system and platform. Please check them and make any corrections if necessary.

\* **Summary:**

**Description:**

**Attachment:**



0000001: Title of Issue 1 - Mantis

localhost/mantis/view.php?id=1

Report Issue

Invite Users

Testing Mantis

administrator

My View

View Issues

Report Issue

Change Log

Roadmap

Summary

Manage

View Issue Details

Send a Reminder

Jump to Notes

Jump to History

ID	Project	Category	View Status	Date Submitted	Last Update
0000001	Testing Mantis	[All Projects] Methods & Tools	public	2019-11-22 09:35	2019-11-22 09:35
Reporter	administrator	Assigned To	developer		
Priority	normal	Severity	minor	Reproducibility	always
Status	assigned	Resolution	open		
Platform	Desktop	OS	Windows	OS Version	10
Summary	0000001: Title of Issue 1				
Description	Description of Issue 1				
Steps To Reproduce	Step 1 Step 2 Step 3				
Additional Information	Additional information				
Tags	tag1 tag2				
Attach Tags	(Separate by ",") Existing tags Attach				
<div><div>Edit</div><div>Assign To: [Myself]</div><div>Change Status To: new</div><div>Monitor</div><div>Stick</div><div>Clone</div><div>Close</div><div>Move</div><div>Delete</div></div>					

Relationships

Current issue

related to

Users monitoring this issue

User List

There are no users monitoring this issue.

Username Add

Activities

administrator

© 2019-11-22 09:35

administrator

aa code artificial intelligence.jpg (35,864 bytes)



## Create New Ticket

### Properties

Summary:

Description:



You may use [WikiFormatting](#) here.

Type:

Priority:

Milestone:

Component:

Version:

Keywords:




Cc:


Owner:

☐ I have files to attach to this ticket

Preview

Create ticket

 Dashboards ▾ Projects ▾ Issues ▾ Tests ▾ **Create**   

 FIRE / FIRE-14 **Verify that the Appstore can be accessed**

Comment

Attach Files


More ▾

Execute


Add to Test Cycle(s)

Export ▾

**Details**

Type:  Test

Status: **OPEN** [\(View Workflow\)](#)

Priority:  Medium


Resolution: Unresolved


Affects Version/s: None


Fix Version/s: None


Labels: [appstore](#)

**People**

Assignee:  Unassigned

Reporter:  Lana Malakova




Votes:  0




Watchers:  [Stop watching this issue](#)




**Description**

Appstore specific tests. Needs integration with the latest build of appstore platform.

**Test Details**



Test Step	Test Data	Test Result	
1 Turn on phone. From the main screen locate the appstore icon.		Appstore icon should be present	 
2 <b>Click/Tap</b> on the icon	Single tap	The app should open	



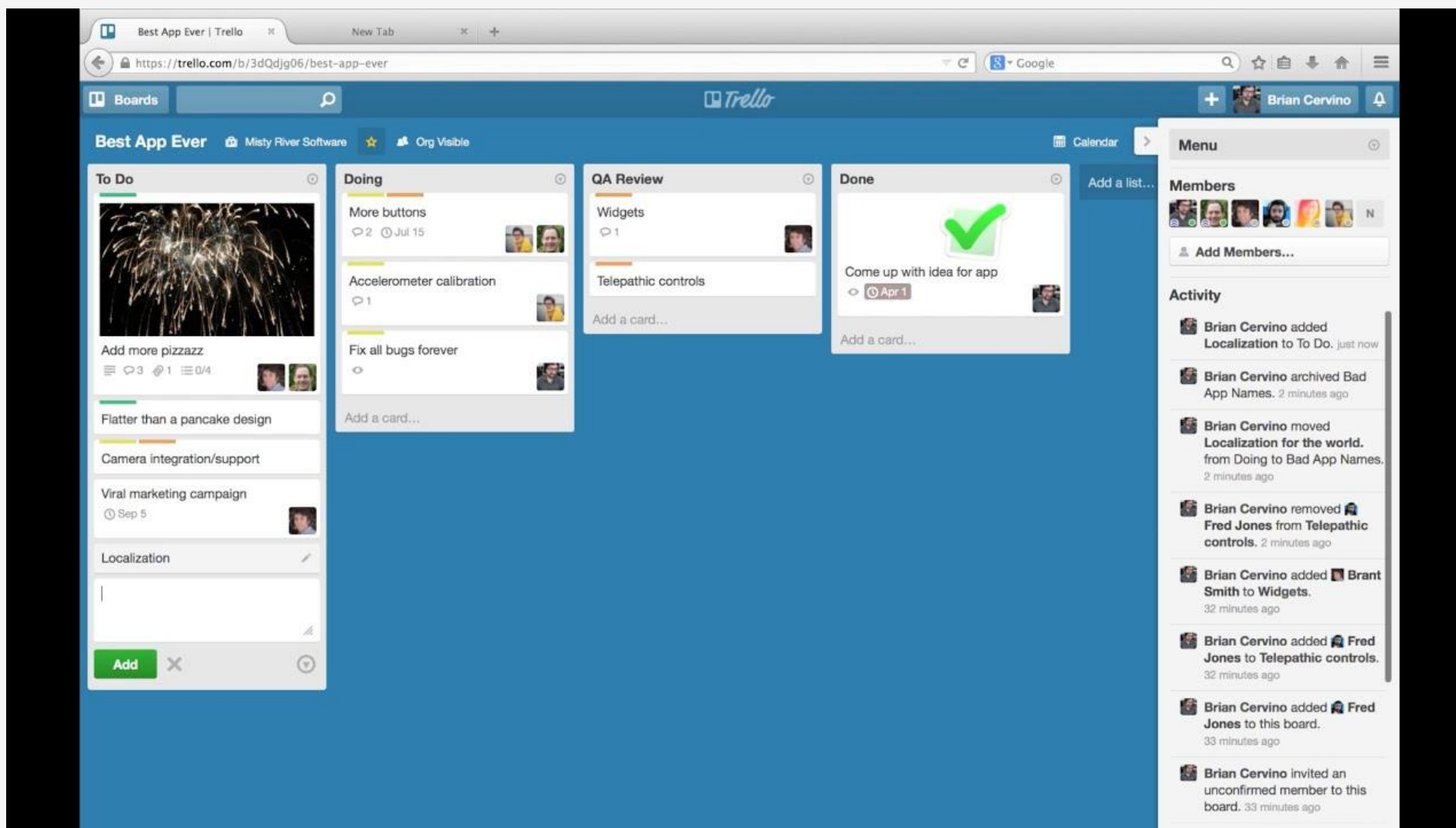


Add

**Test Executions**

Version	Test Cycle	Status	Defects	Executed By	Executed On	
Release 1.0	Mobile Testing	<b>FAIL</b>	 <a href="#">FIRE-15</a>	lana.malakova	02-01-2015 14:11	

Radosław Kowal: Prawa do korzystania z materiałów posiada Software Development Academy



# Praca domowa



Na stronie <http://www.opendemo.org/open-source-demos> podaj swój adres mailowy w sekcji Issue Tracking, dostaniesz na niego link generujący Bugzillę, Mantis i Traca.

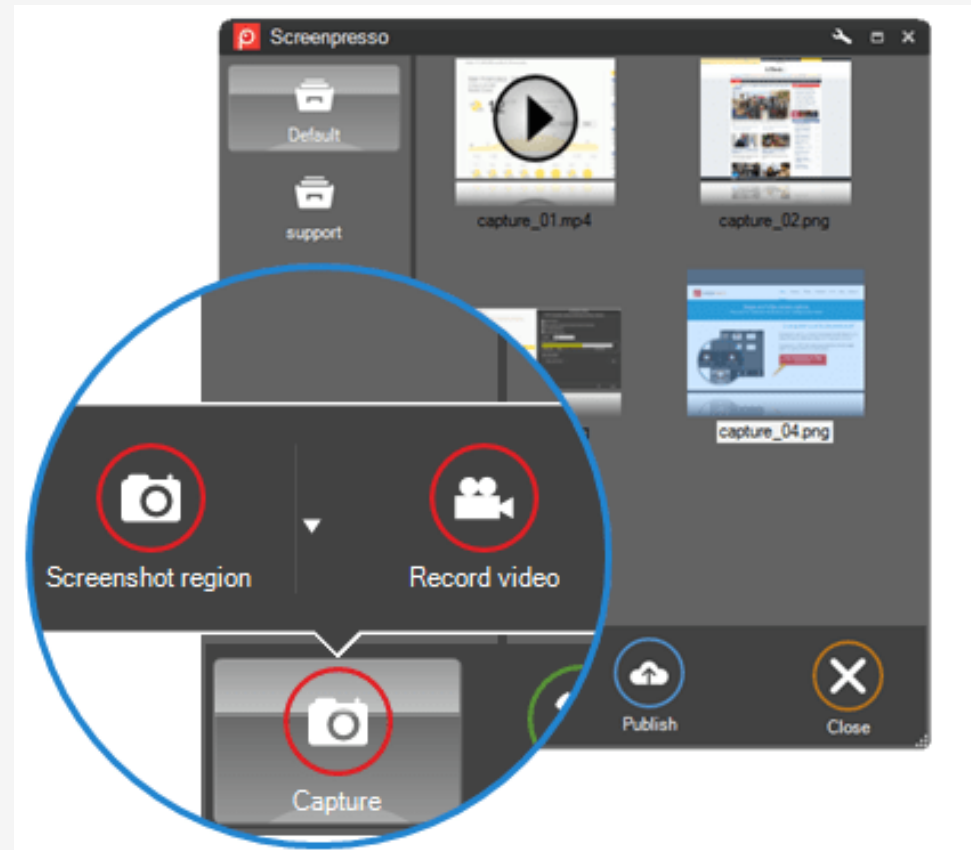
Pobierz aplikację Mr Buggy ze strony <http://mrbuggy.pl/mrbuggy1/data/MrBuggy.exe>

W aplikacjach z punktu 1 zgłoś kilka błędów. Dla ułatwienia (w końcu uczymy się obsługi samych narzędzi) znajdziesz je pod tym linkiem:

[https://docs.google.com/spreadsheets/d/1dt2\\_xVu8AXMIGKdRxuThIjb0Ldx2RJQ4Q4a9rpanOBo/pub?output=html](https://docs.google.com/spreadsheets/d/1dt2_xVu8AXMIGKdRxuThIjb0Ldx2RJQ4Q4a9rpanOBo/pub?output=html)

Powodzenia :)

# Narzędzia do robienia screenshotów i nagrywania ekranu (Screenpresso)

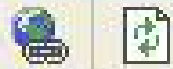




# Multischowek (Ditto)



The screenshot shows the Ditto application window. On the right side, there is a vertical blue bar with the text "Ditto - 1/8 - Microsoft FrontPage - C:\Documents & Settings\user\My Documents". The main area contains a list of features, each preceded by a number in a small box. The 7th item, "Send copied data to other computers manually or automatically", is highlighted with a blue background. At the bottom, there is a status bar with a folder icon and the text "Radosław Kowal: Prawa do korzystania z materiałów posiada Software Development Academy".

- 1  Display a thumbnail of a copied bitmap
- 2 Keep multiple computer's clipboards in sync
- 3 Ditto is a clipboard Extender
- 4 Paste into any window that excepts standard copy/paste entries
- 5 Very handy tool
- 6 Easy to use interface
- 7 Send copied data to other computers manually or automatically
- 8 Search previous copy entries

Radosław Kowal: Prawa do korzystania z materiałów posiada Software Development Academy

# Tymczasowe skrzynki pocztowe



<http://www.fakemailgenerator.com>

## YOUR FAKE E-MAIL ADDRESS IS READY

Noul1932	@teleworm.us ▼	<b>COPY</b>
----------	----------------	-------------



Waiting for e-mails...

This page will automatically show any e-mails sent to **Noul1932@teleworm.us**

# Generatory haseł



<https://generator.blulink.pl/>

### Ustawienia

Ile znaków?

Ile haseł?

**Hasło zawiera:**

- ☒ małe litery: [a b c...]
- ☒ wielkie litery: [A B C...]
- ☒ cyfry: [1 2 3...]
- ☐ znaki interpunkcyjne: [: ! ?...]
- ☐ znaki specjalne: [@ # \$...]
- ☒ bez znaków podobnych: [i l O 1 0 I]

### Dodatkowe ustawienia

**Muszą wystąpić znaki:**

**Mogą wystąpić znaki:**

**Nie mogą wystąpić znaki:**

nBND4ygrow  
ryGEh6VChj  
9naUMKe3BU  
eoVtsqs8ge  
57ccbUGxXp  
gwbQRo2wP3  
RuQdoH3egH  
SKevnQQuMe  
htbSJtFbpV  
DEPUhC3JgJ  
RzTwvFLLzY  
qhS2z3TFCG  
2GLg2ukuCZ  
CUZVRU3463  
sVJKnJcEPf  
MgnYXNSGGV  
8Jgx6xRxZo  
YSJ83wgEAW  
mNc8cAmuGs  
QeAwc6uu4T  
gscrZEnFJo  
BuAe2deM7n  
DoZDjBacvC  
wcu83TcPZn  
B3gCGHfnUM

# Systemy kontroli wersji



Jest to program zapisujący zmiany zachodzące w plikach (wersje), dzięki czemu możemy przejrzeć ich historię i w razie potrzeby – przywrócić. Wszystkie te informacje są zapisywane w tzw. repozytorium projektu.

Systemy kontroli wersji umożliwiają:


Przegląd historii zmian wraz z informacją kto i kiedy je wprowadził

Przywrócenie Dowolnej wersji pliku lub nawet całego projektu

Pracę zespołową, poprzez wykorzystywanie zdalnych repozytoriów (w serwisach takich jak GitHub, BitBucket lub GitLab)



## Najpopularniejszy system kontroli wersji




[Pull requests](#)
[Issues](#)
[Marketplace](#)
[Explore](#)


[radekkowalsda / sda](#)


[Code](#)
[Issues 0](#)
[Pull requests 0](#)
[Projects 0](#)
[Wiki](#)


Branch: master ▼


Commits on Jun 30, 2019


usuniety obrazek  
 radekkowalpmi committed 38 minutes ago


obrazek  
 radekkowalpmi committed 1 hour ago


to jest mój plik  
 RKowal committed 4 hours ago

Initial commit  
 radekkowalsda committed 4 hours ago


 37391e5




 340ade0



Verified

 c4380ea



MINGW64: c:/Users/admin/Desktop/gitsda/sda

```

admin@DESKTOP-FAGJPIC MINGW64 ~/Desktop/gitsda
$ git status
fatal: not a git repository (or any of the parent directories): .git

admin@DESKTOP-FAGJPIC MINGW64 ~/Desktop/gitsda
$ cd sda/

admin@DESKTOP-FAGJPIC MINGW64 ~/Desktop/gitsda/sda (master)
$ git status
On branch master
Your branch is up to date with 'origin/master'.

Changes to be committed:
  (use "git reset HEAD <file>..." to unstage)

    new file:   obrazek.bmp

Untracked files:
  (use "git add <file>..." to include in what will be committed)

    rysunek.odg
    
```

# Git – przydatne komendy



`git clone link_do_repozytorium` – pobiera repozytorium ze zdalnego serwera (wykonujemy tylko na samym początku)

`git checkout nazwa_brancha` – zmiana gałęzi repozytorium

`git pull` – pobiera zmiany (aktualizuje repozytorium na naszym dysku)

`git commit -m 'nazwa wprowadzonych zmian'` - zatwierdza dokonane przez nas zmiany

`git push` – aktualizuje wszystkie nasze zmiany (commit'y) na zdalnym repozytorium



Repozytorium SVN służy do kontroli wersji plików niebinarnych (czyli np. pliki tekstowe, html, php, bash). Użytkownicy przechowują w nim różne wersje plików, np. skryptów PHP. Możliwe jest również wysyłanie innych plików do repozytorium. Należy jednak pamiętać, że SVN służy do kontroli wersji głównie plików tekstowych i wysyłanie innych plików mija się z celem.

# Git vs. SVN



- w SVN – jeden etap przenoszenia zmian na serwer, w Git są to dwa etapy – zapis do lokalnego repozytorium, a potem na serwer;
- pozwala to na pracę offline, a ponadto możliwe jest wysłanie nie wszystkich zmian, które dokonaliśmy;
- Git jest dużo szybszy :)



# Narzędzia developerskie przeglądarki



screenpresso

[Wszystko](#) [Grafika](#) [Filmy](#) [Wiadomości](#) [Zakupy](#) [Więcej](#)

Okolo 153 000 wyników (0,30 s)

## Screenpresso: The Ultimate Screen Capture Tool for Windows

<https://www.screenpresso.com/> [Tłumaczenie strony](#)

**Screenpresso** screen capture allows you to grab an image or video of what you see on your c  
screen, add effects, and share with anyone.

### Download

Download the NEW version for FREE.  
Available for Windows ...

[Więcej wyników z screenpresso.com »](#)

### Features

Feature tour. Discover all our  
features. Capture screenshots ...

Elements Console Sources Network Performance >> 3

top Filter Default levels 3 hidden

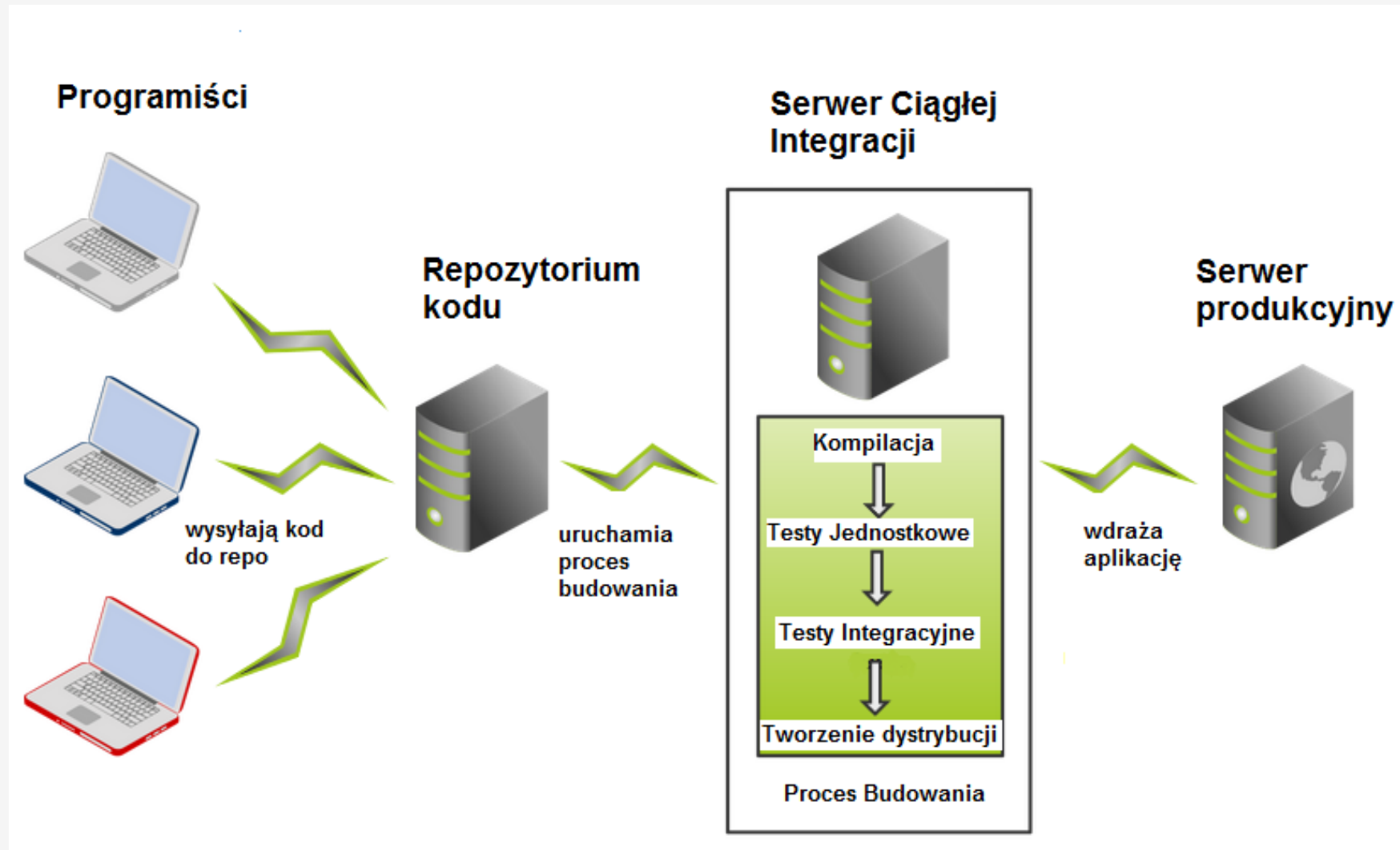
GET https://adservice.google.com/ad\_ adservice.google.com/adsid/google/ui:1  
sid/google/ui net::ERR\_BLOCKED\_BY\_CLIENT

GET https://clients5.google.com/pagead/drt/dn/dn.js (index):4  
net::ERR\_BLOCKED\_BY\_CLIENT


Uncaught ReferenceError: gbar is not defined (index):6  
at onload ((index):6)

>

# CI w procesie tworzenia oprogramowania





 **Jenkins**

search

admin | log out

Jenkins

ENABLE AUTO REFRESH

add description

New Item

People

Build History

Manage Jenkins

My Views

Credentials

Lockable Resources

New View

Build Queue











No builds in the queue.

Build Executor Status




1 Idle

2 Idle

All +

S	W	Name ↓	Last Success	Last Failure	Last Duration	
		<a href="#">Freestyle project</a>	29 sec - <a href="#">#1</a>	N/A	41 ms	
		<a href="#">Github Org project</a>	N/A	20 sec - <a href="#">log</a>	2.9 sec	
		<a href="#">Multibranch</a>	N/A	N/A	N/A	
		<a href="#">Other</a>	N/A	N/A	N/A	

Icon: [S](#) [M](#) [L](#)

[Legend](#)  [RSS for all](#)  [RSS for failures](#)  [RSS for just latest builds](#)

# Po co CI to?



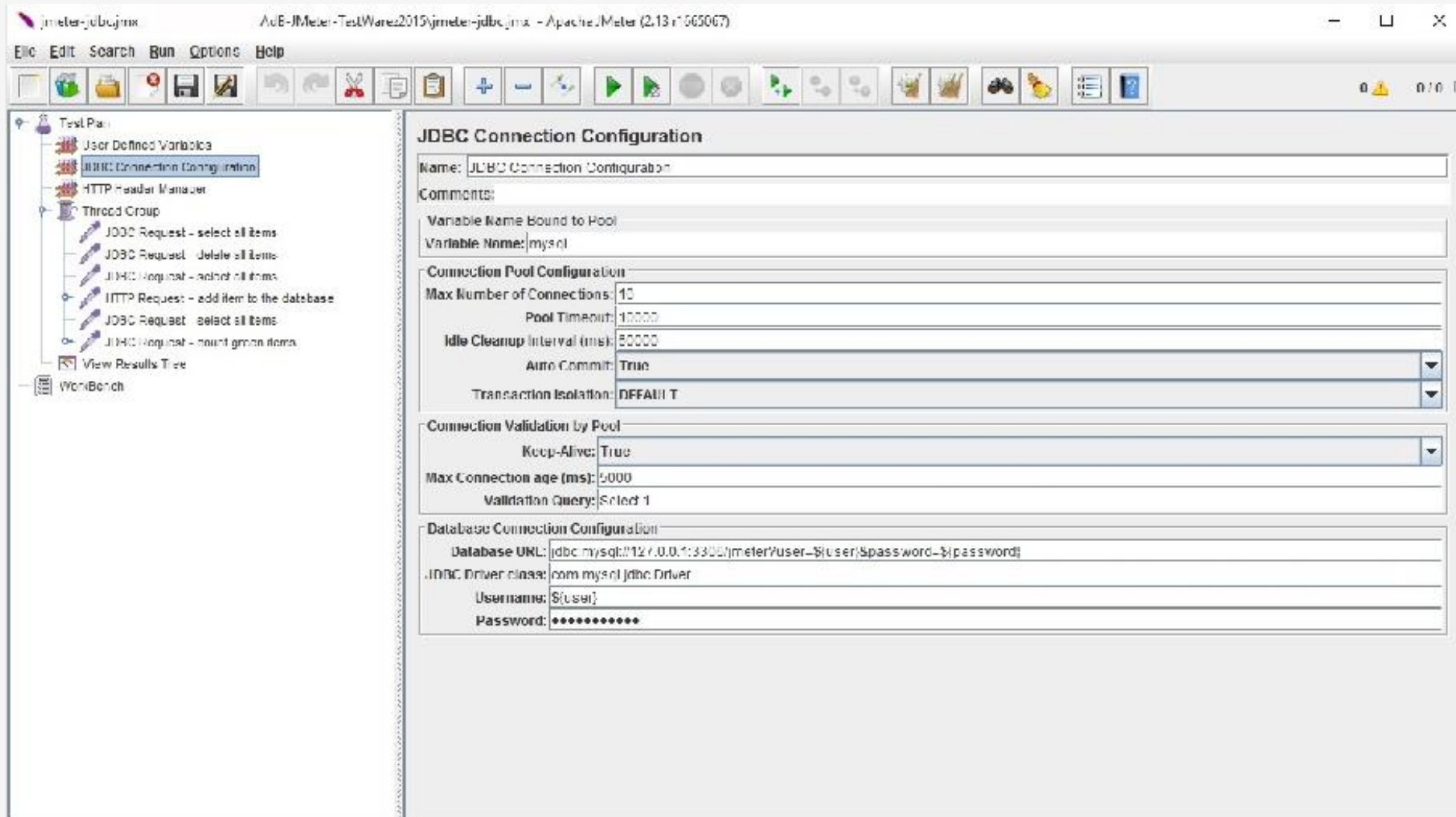
- Ciągła Integracja zmniejsza ryzyko związane z integracją na samym końcu projektu – błędy, niekompatybilność interfejsów, trudny do oszacowania czas na poskładanie całości.
- CI ułatwia naprawę błędów: ich szybkie wykrywanie sprawia, że łatwiej zlokalizować przyczynę – wiadomo, co było ostatnio modyfikowane i jaka wersja działała poprawnie.
- CI chroni przed niespodziankami wynikającymi z różnic pomiędzy środowiskiem deweloperskim a produkcyjnym (np. inne środowisko uruchomieniowe danego języka, niestandardowe biblioteki).
- CI umożliwia demonstrowanie aplikacji i konsultację z klientem w dowolnym momencie dzięki stałej dostępności ostatniej działającej wersji.
- CI ułatwia refaktoryzację (po każdej „kosmetycznej” zmianie możemy szybko sprawdzić, czy wszystko gra).
- Ciągła integracja zdejmuje z programistów obowiązek wykonywania wielu powtarzalnych, nierozwijających (a jednak trudnych!) czynności.

# Testy wydajnościowe



- Testy wydajnościowe są przeprowadzane w celu oceny stopnia spełnienia wymagań wydajnościowych przez system lub moduł.
- Istnieje kilka rodzajów wymagań wydajnościowych:
  - wymagania na szybkość przetwarzania,
  - wymagania na równoległość przetwarzania,
  - wymagania na wielkość obsługiwanych danych.
- Testy wydajnościowe przeprowadza się zwykle w dwóch sytuacjach: na granicy wymagania wydajnościowego oraz powyżej wymagania wydajnościowego. W tym drugim przypadku testy są nazywane przeciążeniowymi.

# JMeter



# Gatling



jest darmowym narzędziem do wykonywania testów wydajnościowych,  
działa na systemach Windows, Linux oraz MacOS,  
został napisany głównie w języku Scala i jest oparty o AKKA i NETTY,  
dzięki zastosowanym rozwiązaniom posiada asynchroniczną architekturę, wprowadza model aktora,  
który jest zorientowany na wysyłanie wiadomości zamiast tworzenia dedykowanych wątków, pozwalając  
na generowanie większych obciążeń,  
skrypty testowe są pisane w Scali, przy czym wystarczy podstawowa znajomość tego języka, gdyż  
skrypty są tworzone z wykorzystaniem łatwego w użyciu DSL (Domain Specific Language), przez co  
tworzenie i późniejsze zrozumienie skryptów jest proste,

# Testy webservice



Usługi sieciowe (ang. webservice) to mechanizmy, które pozwalają na komunikację klienta z serwerem. Klient, czyli użytkownik, chciałby wyświetlić swoje ulubione restauracje na mapie - aby to zrobić, musi wysłać do serwera odpowiednie żądanie (ang. request). Jeśli żądanie jest prawidłowe, użytkownik otrzyma odpowiedź (ang. response) w odpowiednim formacie. Błędnie sformułowane zapytanie lub brak zasobu na serwerze spowoduje odpowiednie akcje informujące o niepowodzeniu.

REST (ang. Representational State Transfer) opiera się na konkretnych adresach URL, które poniekąd działają jak identyfikatory. Na dany adres URL zostaje wysłane zapytanie na serwer, następnie serwer przetwarza nasze zapytanie i dostajemy odpowiedź. Wyróżnia się 7 podstawowych metod do komunikacji.



# Testy webservice (Postman)



Postman służy głównie do wysyłania żądań różnego typu:

- GET
- POST
- PUT
- DELETE

Są to cztery najbardziej popularne żądania wysyłane przy pomocy REST API.

Po każdym z wysłanych żądań, wysyłany jest kod odpowiedzi w postaci trzycyfrowego numeru. Pierwsza liczba kodu odpowiedzi definiuje rodzaj komunikatu. Są to odpowiednio:

Kody informacyjne - rozpoczynające się od 1, np. 101, 111

Kody powodzenia - rozpoczynające się od 2, np. 200, 201

Kody przekierowania - rozpoczynające się od 3, np. 301, 306

Kody błędu aplikacji klienta - rozpoczynające się od 4, np. 404

Kody błędu serwera HTTP - rozpoczynające się od 5, np. 500, 501

# Testy webservice (Postman)



The screenshot shows the Postman application window. The top bar includes the Postman logo, menu items (File, Edit, View, Help), and buttons for 'New', 'Import', 'Runner', 'My Workspace', and 'Invite'. The left sidebar shows a 'Filter' search bar and tabs for 'History', 'Collections', and 'APIs BETA'. The 'History' tab is active, showing a list of requests from 'Today' and 'Yesterday'. The main panel displays a GET request to 'https://jsonplaceholder.typicode.com/users'. The 'Send' button is highlighted. Below the request, the 'Query Params' section is empty. The 'Body' section shows the response in 'Pretty' format, which is a JSON array containing one user object.

```
1 [
2   {
3     "id": 1,
4     "name": "Leanne Graham",
5     "username": "Bret",
6     "email": "Sincere@april.biz",
7     "address": {
8       "street": "Kulas Light",
9       "suite": "Apt. 556",
10      "city": "Gwenborough",
11      "zipcode": "92998-3874",
```

Status: 200 OK Time: 310 ms Size: 6.14 KB Download

# Testy webservice (Swagger UI)



[https://petstore.swagger.io/?\\_ga=2.166840766.1007213295.1590004620-467914185.1590004620#/](https://petstore.swagger.io/?_ga=2.166840766.1007213295.1590004620-467914185.1590004620#/)

SWAGGERhub  
SMARTBEAR

TradeshowD... | SamplePets... | 1.0.0 OAS3

PRIVATE UNPUBLISHED

Editor Split UI

Last Saved: 12:46:55 pm May 4, 2018 VALID Save

<https://virtserver.swaggerhub.com/TradeshowDemos/SamplePetstoreAPI/1.0.0>

pet Everything about your Pets Find out more: <http://swagger.io>

- POST /pet Add a new pet to the store
- PUT /pet Update an existing pet
- GET /pet/findByStatus Finds Pets by status
- GET /pet/findByTags Finds Pets by tags
- GET /pet/{petId} Find pet by ID
- POST /pet/{petId} Updates a pet in the store with form data
- DELETE /pet/{petId} Deletes a pet
- POST /pet/{petId}/uploadImage uploads an image

store Access to Petstore orders

# Testy bezpieczeństwa



Testy bezpieczeństwa są kolejnym typem testów niefunkcjonalnych. Testy bezpieczeństwa są kluczowe dla niektórych typów aplikacji — szczególnie dla aplikacji przechowujących dane poufne. Testy bezpieczeństwa mogą być wymuszone poprzez umowę czy uwarunkowania prawne. Obecnie widać coraz większy nacisk na testy bezpieczeństwa, osoba zajmująca się testami bezpieczeństwa nazywana jest Pentesterem lub Testerem bezpieczeństwa. Zazwyczaj zajmuje się tylko tym jednym typem testów. Podstawowe testy bezpieczeństwa można wykonać ręcznie, ale bardziej zaawansowane jak np. analiza pakietów sieciowych, jest możliwa tylko i wyłącznie przy pomocy narzędzi.

# Testy bezpieczeństwa (OWASP)



OWASP - globalna, profesjonalna fundacja, działająca charytatywnie (non-profit), otwarta dla każdego, kto interesuje się zabezpieczeniami w oprogramowaniu



# OWASP

Open Web Application  
Security Project

# OWASP Top10



OWASP Top10 - web

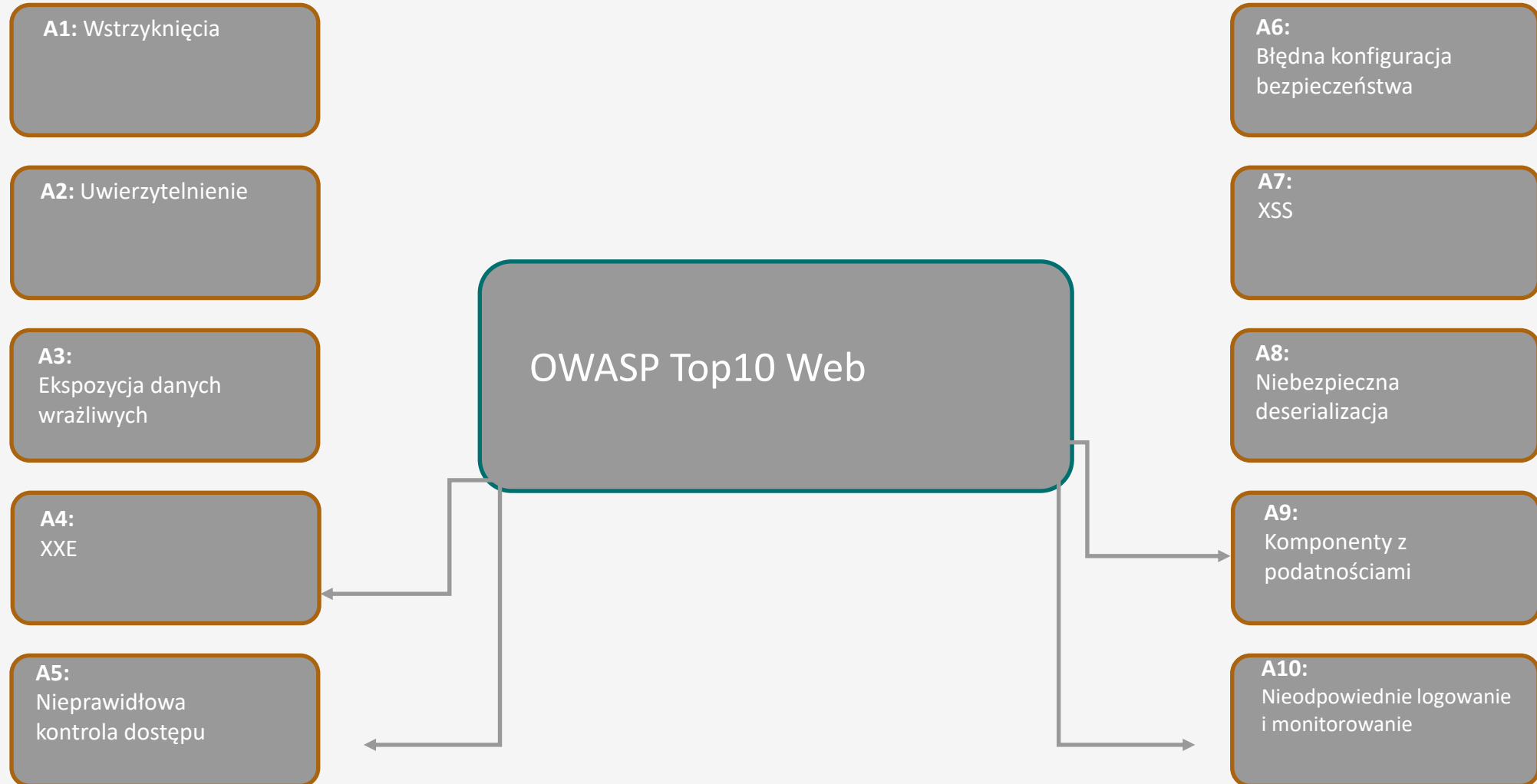


OWASP Top10 - IoT



OWASP Top10 - mobile

# OWASP Top10 Web



# OWASP Top10 Web



**Wstrzyknięcia** - jeżeli w aplikacji nie zostanie zastosowane odpowiednie filtrowanie danych, to atakujący będzie mógł przesłać exploit w formie tekstowej wykorzystujący odpowiednią składnię docelowego interpretera. Wartości zostaną potraktowane jak polecenia, co może skutkować nieautoryzowanym dostępem do poufnych informacji, a nawet przejęciem kontroli nad atakowanym systemem.

**Wadliwa obsługa uwierzytelniania i sesji** - poprawne wdrożenie funkcji związanych z uwierzytelnianiem i obsługą sesji w aplikacji nie jest łatwe. Atakujący może wykorzystać nie tylko odkryte przez siebie usterki techniczne w implementacji lub konfiguracji oprogramowania, ale też błędy projektowe i organizacyjne. Konsekwencje ataku bywają zwykle poważne i obejmują uzyskanie nieautoryzowanego dostępu do sesji, przejęcie haseł lub tokenów, wykonanie poleceń na prawach zalogowanego użytkownika itp.



# OWASP Top10 Web



**Cross-Site Scripting (XSS) – skrypty międzyserwisowe** - Luki XSS, w przeciwieństwie do wspomnianych wyżej wstrzyknięć, nie mają wpływu na logikę aplikacji po stronie serwera, pozwalają za to atakującemu na wykonywanie złośliwych skryptów w przeglądarce ofiary. Dzieje się tak, gdy aplikacja pobiera niezaufane dane i wysyła je do przeglądarki bez wcześniejszej walidacji. Skutkiem wykorzystania błędów tego typu może być np. przechwycenie sesji zalogowanego użytkownika, dynamiczna podmiana zawartości strony, jak również hostowanie złośliwego oprogramowania z wykorzystaniem zaatakowanej aplikacji.

**Insecure Direct Object References** – W aplikacjach, w których występują różne poziomy uprawnienie, zdarzają się problemy wynikające z możliwości bezpośredniego dostępu do różnych obiektów w systemie (takich jak pliki, katalogi czy klucze bazy danych). Brak zdefiniowanych reguł dostępności sprawia, że atakujący może odpowiednio manipulować odwołaniami w celu dostania się do poufnych danych. Przykładowo, jeśli aplikacja nie sprawdza uprawnień użytkownika na poziomie funkcji przyjmującej identyfikator obiektu, a te tworzone są w przewidywalny sposób, to znajomość identyfikatora będzie wystarczająca, by móc wykonać takie same operacje na obiekcie jak uprawniony użytkownik.



**Security Misconfiguration – niepoprawna konfiguracja** - błędy konfiguracji zabezpieczeń mogą wystąpić w każdej warstwie aplikacji – nie tylko w jej własnym kodzie, ale też w innych elementach składających się na całość systemu, m.in. w użytych przez programistów bibliotekach i frameworkach, silnikach baz danych, serwerach aplikacyjnych czy urządzeniach sieciowych. Atakujący wykorzystuje zwykle domyślne konta, nieużywane strony, niezaktualizowane podatności lub niezabezpieczone pliki i katalogi, by uzyskać nieautoryzowany dostęp do danych. Może się zdarzyć, że umożliwi mu to całkowite przejęcie kontroli nad zaatakowanym systemem.

**Sensitive Data Exposure – nieodpowiednie zabezpieczenie poufnych danych** - omawiając to zagrożenie, należy przede wszystkim wspomnieć o niewystarczających zabezpieczeniach kryptograficznych i niewłaściwym zabezpieczeniu wymiany danych. Wciąż wiele aplikacji przechowuje poufne dane (takie jak hasła użytkowników czy numery kart kredytowych), używając błędnie zaimplementowanej enkrypcji lub hashowania bez tzw. salta. W wyniku ataku może dojść do kradzieży takich danych i ich ujawnienia. Równie często aplikacje przesyłają w sieci dane, nie dbając o ich poufność i integralność. Mogą np. stosować wygasłe certyfikaty lub zbyt słabe algorytmy szyfrowania, co stwarza szerokie pole do nadużyć.



**Missing Function Level Access Control – nieodpowiednia kontrola uprawnień – użytkowników** - aplikacje często obsługują zapytania do stron bez odpowiedniej walidacji. Nie sprawdzanie, czy dana osoba powinna mieć dostęp do żądanej strony, pozwala atakującemu na wykonywanie akcji bez uwierzytelnienia lub z prawami innego użytkownika. Głównym celem tego typu ataków są oczywiście funkcje administracyjne.

**Cross-Site Request Forgery (CSRF) – fałszowanie żądań** - podatność ta często bywa mylona z XSS, ponieważ tak jak ona pozwala zaatakować przeglądarkę użytkownika, nie część serwerową aplikacji webowej. W tym przypadku celem atakującego jest wykorzystanie uprawnień ofiary do wykonania interesujących go nieautoryzowanych akcji. Odbywa się to dzięki podmienionym zapytaniom HTTP. Powodzenie ataku zależy od tego, czy atakujący jest w stanie przewidzieć, jak powinno wyglądać żądanie, które zostanie zaakceptowane przez serwer.



**Using Components with Known Vulnerabilities – używanie komponentów ze znanymi podatnościami** - zdecydowana większość powstających obecnie aplikacji bazuje na gotowych już bibliotekach i frameworkach, które – jak każde oprogramowanie – mogą mieć błędy. W teorii można temu zaradzić, instalując udostępniane przez producentów poprawki. Często jednak okazuje się, że zaktualizowane komponenty nie będą współdziałać z tymi, które nie otrzymały łatek. W efekcie aplikacja pozostaje niezaktualizowana, co pozwala na przeprowadzanie mniej lub bardziej wyrafinowanych ataków.

**Unvalidated Redirects and Forwards – nieodpowiednia walidacja przekierowań** - Ostatnie zagrożenie w zestawieniu OWASP dotyczy sytuacji, w których aplikacje webowe przekierowują użytkownika na inne strony, wykorzystując niezaufane dane. Przy braku odpowiedniej walidacji atakujący może dodać do oryginalnego odnośnika ciąg znaków, który zaprowadzi ofiarę na stronę ze złośliwym oprogramowaniem albo wyłudzącą poufne dane. Powyżej opisane błędy należą do najbardziej krytycznych i najczęściej wykorzystywanych, dlatego warto je mieć na uwadze, tworząc i zabezpieczając własne aplikacje internetowe.

# OWASP Testing Guide



Obszerne opisy testowania aplikacji zarówno w ujęciu **black box** jak i **white/grey box**

**Dobrze się czyta**

Dzieli przeprowadzane testy na 2 fazy: **pasywną i aktywną**

Stanowi kompendium wiedzy o testach bezpieczeństwa i poza metodologią wykonywania testów może być źródłem szerokiej wiedzy z zakresu testów.

[https://www.owasp.org/index.php/OWASP\\_Testing\\_Guide\\_v4\\_Table\\_of\\_Contents](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)

# Penetration Testing Execution Standard



Zwięzłe opisy zagrożeń i elementów istotnych podczas testów

- Dzieli testy na 7 etapów:

- ✓ Przygotowanie
- ✓ Gromadzenie informacji
- ✓ Modelowanie zagrożeń
- ✓ Analiza podatności
- ✓ Eksploatacja
- ✓ Post-eksploatacja
- ✓ Raportowanie

- Niektóre rozdziały nie są ukończone!

[http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page)



# Terminologia



## ATAK

- *Wektor ataku*: czynnik, który umożliwia przeprowadzenie ataku (jeżeli np. atakujemy **aplikację internetową**, to wektorem jest np. **framework, który wykorzystuje tę aplikację**)
- *Exploit*: wykorzystanie istniejącej w oprogramowaniu podatności w celu zaburzenia działania aplikacji lub wyrządzenia szkód użytkownikom aplikacji

## CEL

- *Powierzchnia ataku*: Opisuje, co potencjalnie jest narażone na atak (jeżeli np. wystawiamy do sieci 10 portów serwera, to powierzchnią ataku jest te 10 portów.)
- *Podatność*: słaby punkt aplikacji, który może zostać wykorzystany w ataku (np. **XSS**, czy **nieaktualny Windows** z luką EternalBlue)



# Terminologia (CIA)



## CONFIDENTIALITY INTEGRITY AVAILABILITY

### •poufność

czy odpowiednie osoby mają dostęp do odpowiednich danych?

### •integralność

czy dane są spójne i godne zaufania?

## AVAILABILITY

### •dostępność

czy aplikacja jest dostępna dla uprawnionych użytkowników (czy nie jest awaryjna)?



# Terminologia (AAA)



## AUTHENTICATION

### •**uwierzytelnienie**

kim jesteś?

## AUTHORIZATION

### •**autoryzacja**

czy masz prawo do  
tego działania

## ACCOUNTING

### •**rozliczanie**

jak wykorzystać te  
zasoby?

# Przygotowanie i przeprowadzenie testów bezpieczeństwa - przykład



1. Przygotowanie środowiska lub ustalenie z administratorem, czy testy mogą być wykonywane na zwykłym środowisku testowym
2. Ustalenie trybu testów
3. Uzyskanie dostępów do kont z odpowiednimi zestawami uprawnień
4. Identyfikacja potencjalnych zagrożeń
5. Weryfikacja i próba wykorzystania podatności do przeprowadzenia ataku
6. Stworzenie raportu z analizą krytyczności zagrożeń i sugerowanymi poprawkami



# PYTANIA?

[kowal.radek@gmail.com](mailto:kowal.radek@gmail.com)

[www.linkedin.com/in/radoslaw-kowal](https://www.linkedin.com/in/radoslaw-kowal)