



Narzędzia w testowaniu

Radosław
Kowal
17.05.2020

Agenda



- 1) Wprowadzenie do narzędzi
- 2) Zarządzanie testami i incydentami
- 3) Narzędzia pomocnicze (robienie screenshotów, generatory)
- 4) Automatyzacja
- 5) Systemy kontroli wersji
- 6) Continuous Integration
- 7) Testy wydajnościowe
- 8) Testy webservice'ów
- 9) 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

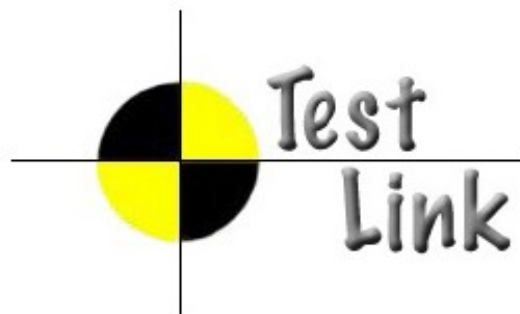
Wtyczki i konsole przeglądarkowe

Narzędzia do automatyzacji

Systemy kontroli wersji

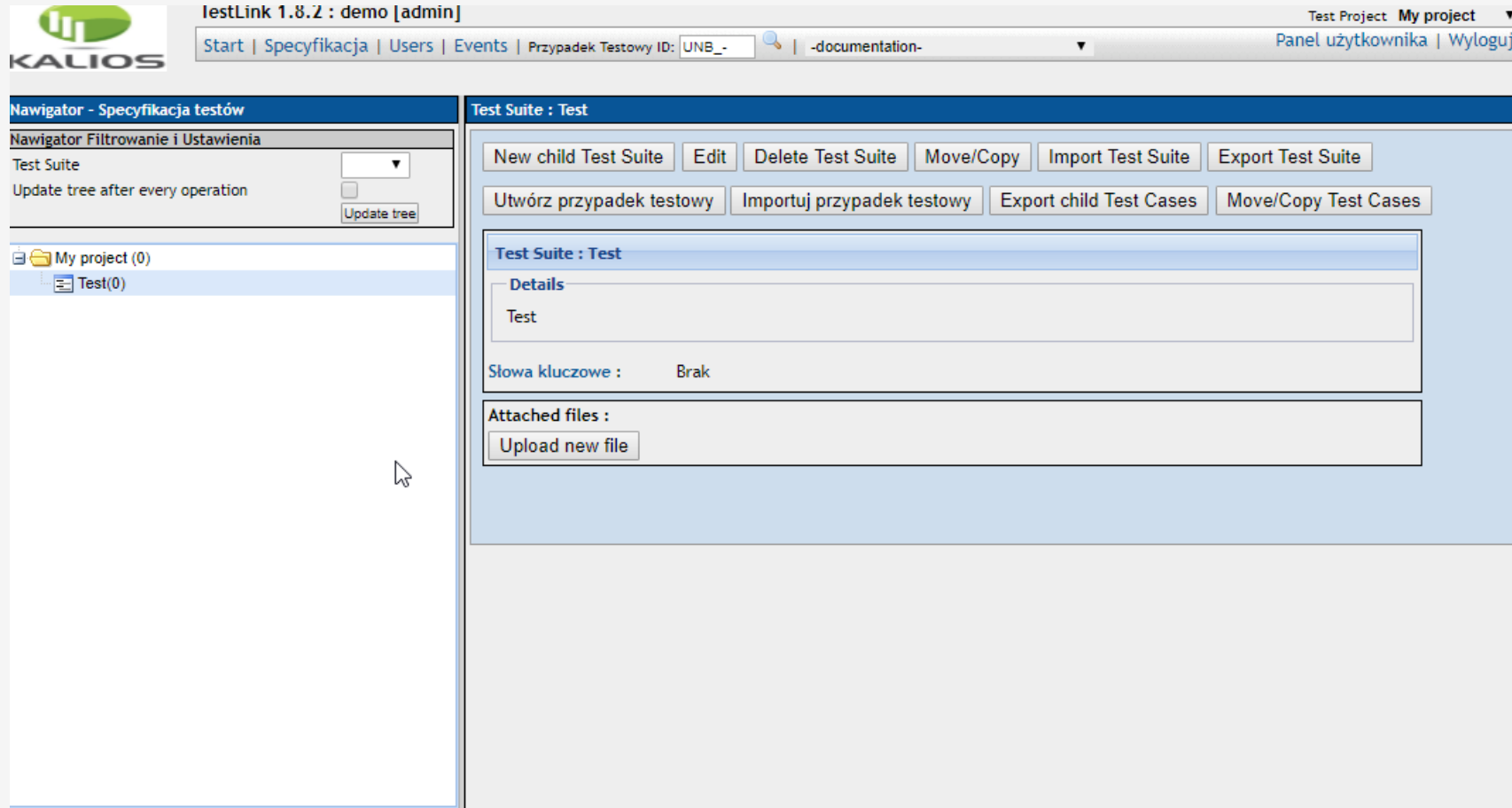
Narzędzia do Continuous Integration

Zarządzanie incydentami/testami





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





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](#)

▼ DPO -3047 **RESOLVED** 2 sub-tasks Add empty page by customer

Frontend implementation

DPO -3065

Backend implementation

DPO -3066

Disable admin login from connect request

DPO -3204



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:](#) bugzilla-4.2.1 [Component Description:](#) bugzilla-4.2.1

* [Version:](#) unspecified [Severity:](#) enhancement ▼

[Hardware:](#) PC ▼

[OS:](#) Windows ▼

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

* [Summary:](#)

Description:

Attachment:



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



JIRA

Dashboards

Projects

Issues

Tests

Create

Search

FIRE / FIRE-14

Verify that the Appstore can be accessed

Comment

Attach Files

More

Execute

Add to Test Cycle(s)

Export

Details

Type: Test

Priority: Medium

Affects Version/s: None

Labels: appstore

Status: OPEN (View Workflow)

Resolution: Unresolved

Fix Version/s: None

Assignee: Unassigned

Reporter: Lana Malakova

Votes: 0

Watchers: 1 Stop watching this issue

Description

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

Test Details

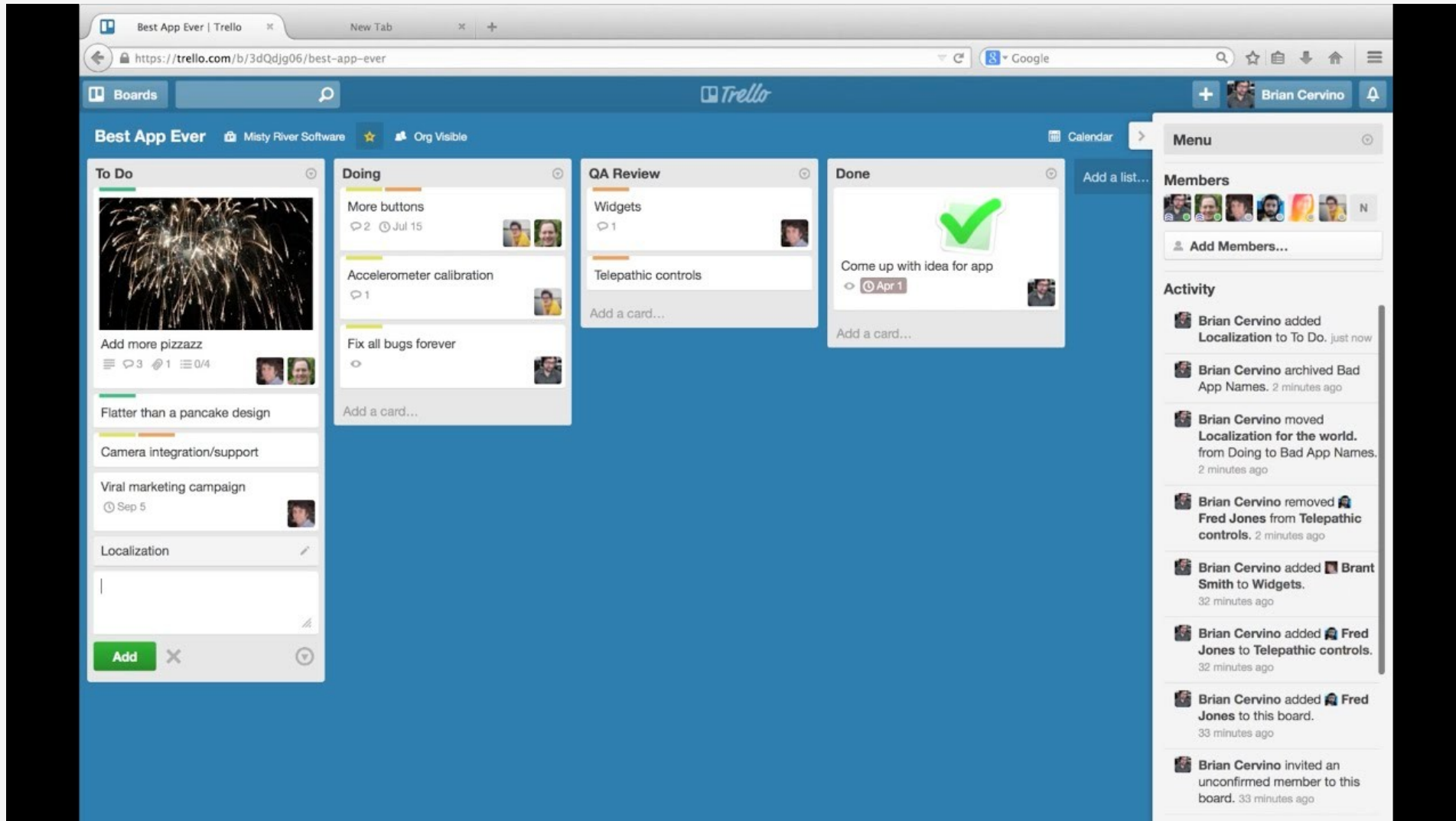
Test Step	Test Data	Test Result
1 Turn on phone. From the main screen locate the appstore icon.		Appstore icon should be present
2 Click/Tap on the icon	Single tap	The app should open

Add

Test Executions

Version	Test Cycle	Status	Defects	Executed By	Executed On
Release 1.0	Mobile Testing	FAIL	110 FIRE-15	lana.malakova	02-01-2015

Trello



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.

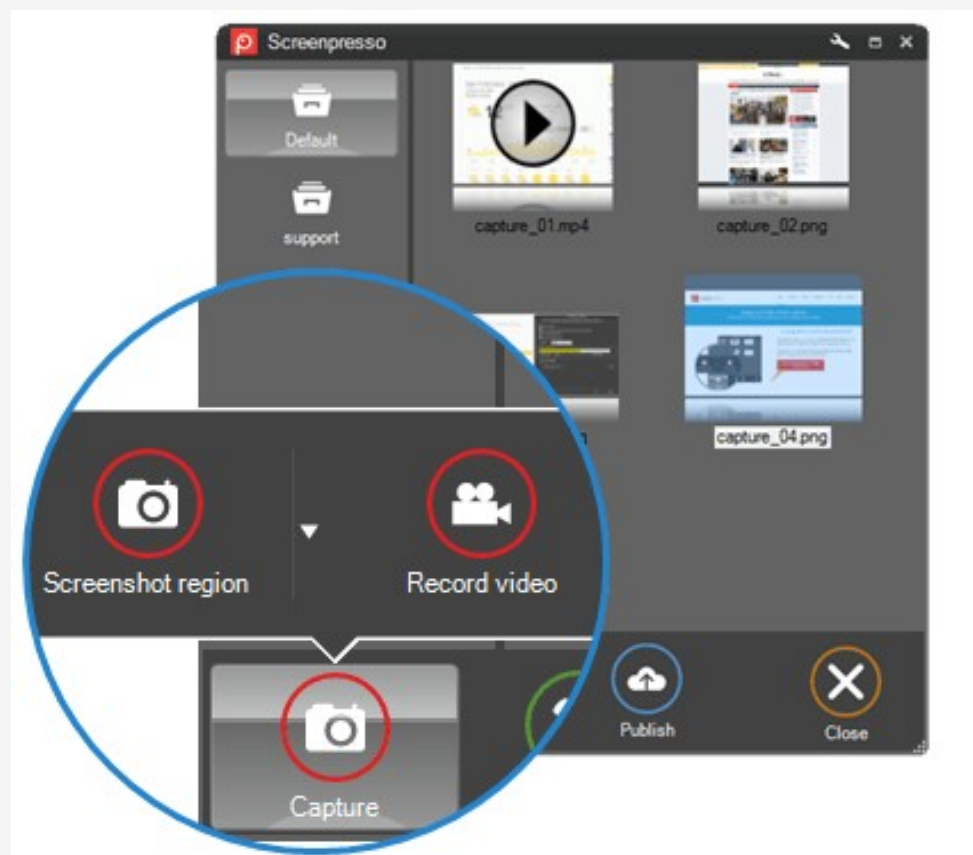
Pobierz aplikację Mr Buggy ze strony <http://mrbuggy.pl/mrbuggy1/data/MrBuggy.exe>

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

Powodzenia :)

Narzędzia do robienia screenshotów i nagrywania ekranu (Screenpresso)



Multischowek (Ditto)



The screenshot shows the Ditto application window. The title bar reads "Ditto - 1/8 - Microsoft FrontPage - C:\Documents". The main content area is a list of features, numbered 1 through 8. Item 7, "Send copied data to other computers manually or automatically", is highlighted in blue. The list items are:

- 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

At the bottom of the window, there is a status bar with a folder icon and the text: "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 ▼	COPY
----------	----------------	-------------



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

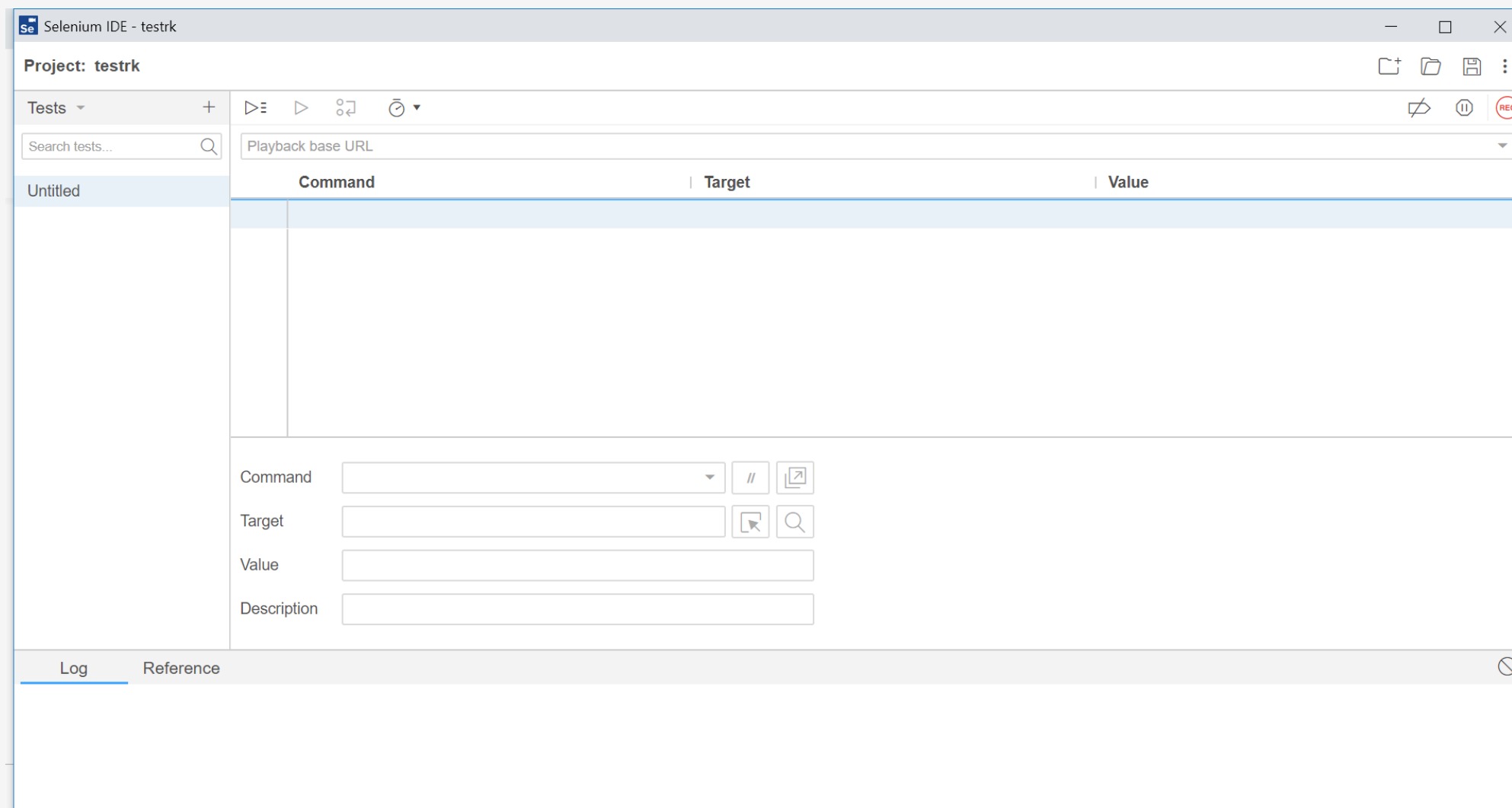
Muszą wystąpić znaki:

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

Automatyzacja (Selenium IDE)



Automatyzacja (SikuliX)



SikuliXIDE 1.1.3 - Bez tytułu

Plik Edycja Uruchom Widok Narzędzia Pomoc

Zrób zrzut ekranu Wstaw obrazek Region Location Offset Show Show in Uruchom Uruchom w zwolnionym tempie Find

Ustawienia

Znajdź

- find()
- findAll()
- wait()
- waitVanish()
- exists()


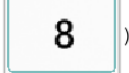

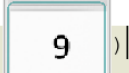
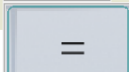
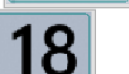
Akcje myszy

- click()
- doubleClick()
- rightClick()
- hover()
- dragDrop(,)

Akcje klawiatury

- type(text)

***Bez tytułu**

```
1 click(  )
2 type( "kalk"+Key.ENTER)
3 click(  )
4 click(  )
5 click(  )
6 click(  )
7 find(  )
8
```

Komunikat

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

SikuliXIDE 1.1.3 (2018-07-11_08:19)

(python) | R: 5 | C: 9

Praca domowa



1. Przy użyciu narzędzia Selenium IDE przeprowadź test logowania do swojej skrzynki pocztowej.
2. Przy użyciu narzędzia SikuliX sprawdź, czy $2+9-5*8=48$, a następnie czy $2+9-5*8=47$

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

The screenshot displays a GitHub repository page for 'radekkowalsda / sda' and a terminal window showing Git commands and output.

GitHub Repository Page:

- Repository: radekkowalsda / sda
- 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)

Terminal Window (MINGW64):

```
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 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

`git checkout nazwa_brancha` – zmiana gałęzi repozytorium

`git config --global user.name "imię"` – ustawia nazwę użytkownika

`git config --global user.email "email"` – ustawia email



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 :)

Praca domowa



1. Stwórz własne repozytorium na GitHub.
2. Dodaj kilku kolegów lub koleżanek z grupy jako contributorów
3. Stwórz plik tekstowy, w którym zapiszesz swoje imię i nazwisko (kolegów poproś o to samo)
4. Znajdź w internecie zdjęcie kota, zapisz je na dysku pod nazwą kot *TwojeImię i Nazwisko*
5. Wrzuć te pliki do swojego repozytorium
6. Poproś kolegów o wrzucenie swoich plików do Twojego repozytorium
7. „Spulluj się” u siebie
8. Pooglądaj zdjęcia :)
9. W plikach tekstowych kolegów napisz na końcu DZIĘKUJĘ :)
10. Zacommituj i „spushuj” zmiany

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_adsid/google/ui:1sid/google/ui net::ERR_BLOCKED_BY_CLIENT
- GET <https://clients5.google.com/pagead/drt/dn/dn.js> net::ERR_BLOCKED_BY_CLIENT (index):4
- Uncaught ReferenceError: gbar is not defined at onload ((index):6) (index):6

Continuous Integration (CI)



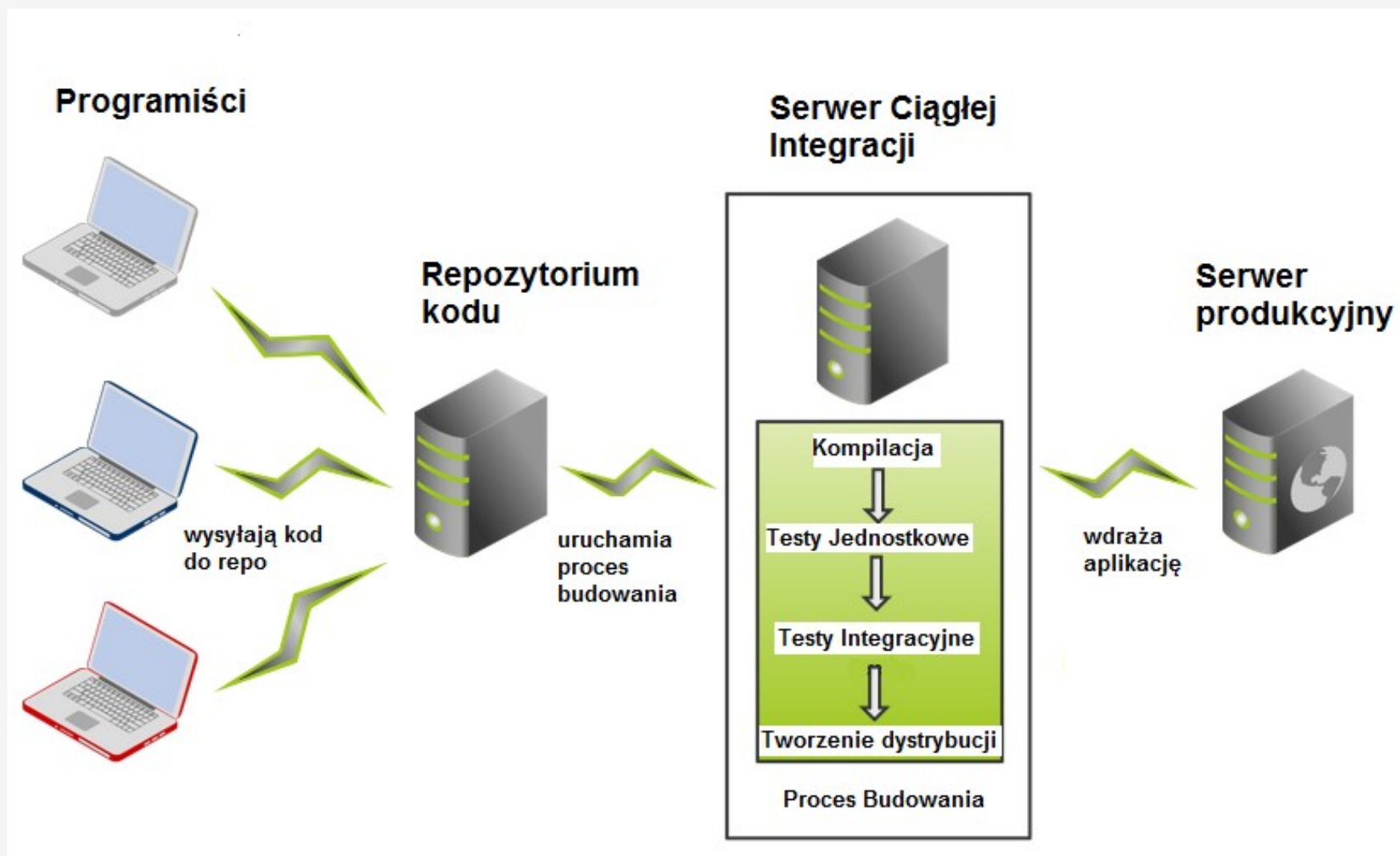
Ciągła Integracja (ang. Continuous Integration) to praktyka programistyczna, w której członkowie zespołu często scalają wyniki swojej pracy – z reguły każdy robi to przynajmniej raz dziennie. W ten sposób każdego dnia powstaje kilka zintegrowanych wersji kodu, które są sprawdzane przez automatyczny proces budowania (i testowania).

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.

CI w procesie tworzenia oprogramowania



Jenkins



 **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	
		Freestyle project	29 sec - #1	N/A	41 ms	
		Github Org project	N/A	20 sec - log	2.9 sec	
		Multibranch	N/A	N/A	N/A	
		Other	N/A	N/A	N/A	

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

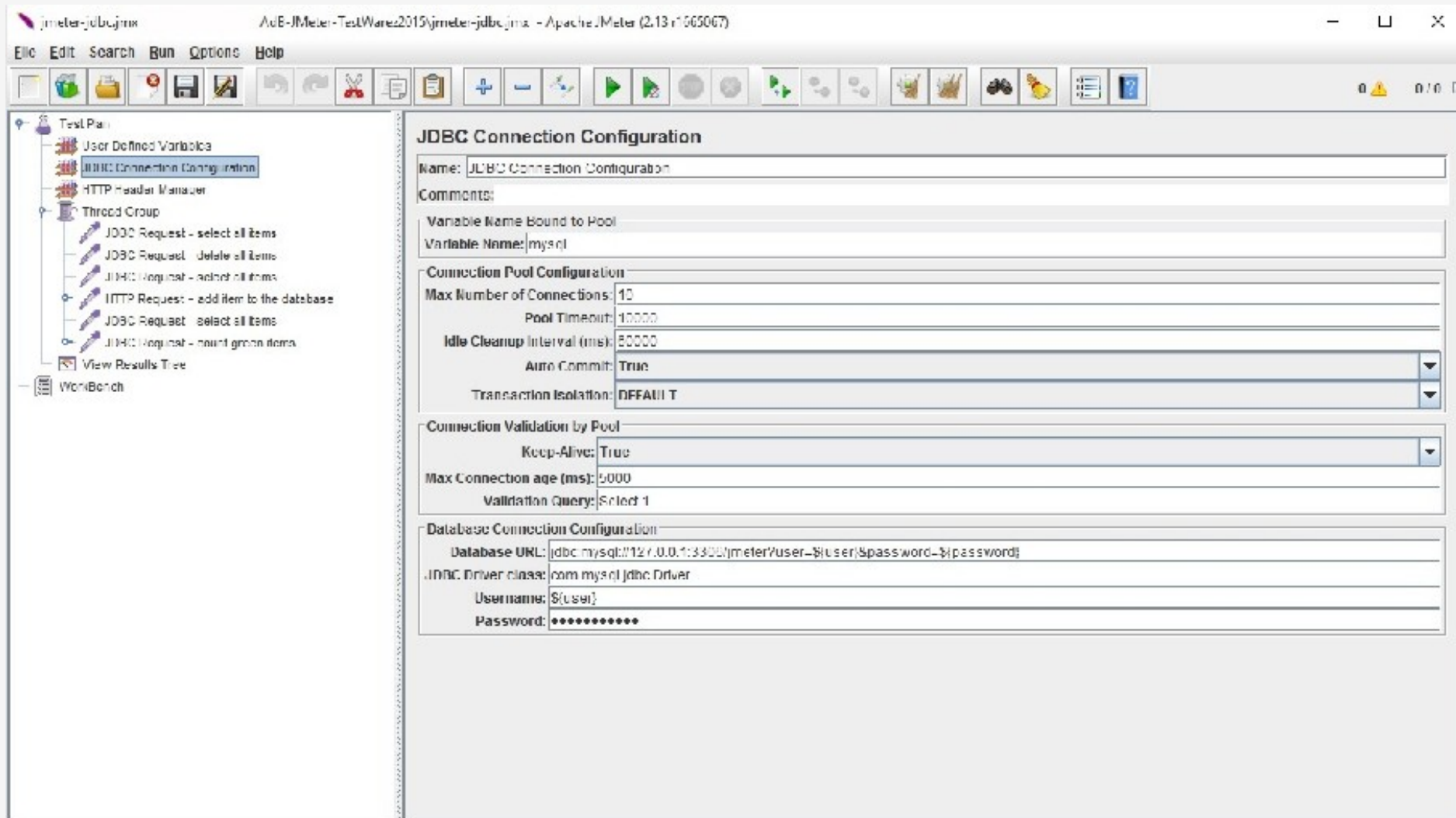
[Legend](#)  [RSS for all](#)  [RSS for failures](#)  [RSS for just latest builds](#)

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



1. jest darmowym narzędziem do wykonywania testów wydajnościowych,
2. działa na systemach Windows, Linux oraz MacOS,
3. został napisany głównie w języku Scala i jest oparty o AKKA i NETTY,
4. dzięki zastosowanym rozwiązaniom posiada asynchroniczną architekturę, wprowadza model aktora, który jest zorientowany na wysyłanie wiadomości zamiast tworzenia dedykowanych wątków, pozwalając na generowanie większych obciążeń,
5. 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 (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 request is configured with the method 'GET' and the URL 'https://jsonplaceholder.typicode.com/users'. The 'Send' button is visible. Below the request configuration, there are tabs for 'Params', 'Authorization', 'Headers (10)', 'Body', 'Pre-request Script', and 'Tests'. The 'Params' tab is active, showing a table for 'Query Params' with columns 'KEY', 'VALUE', and 'DESCRIPTION'. The 'Body' tab is also visible, showing the response in 'JSON' format. The response status is '200 OK', with a time of '310 ms' and a size of '6.14 KB'. The response body is a JSON array containing one user object.

```
[{"id": 1, "name": "Leanne Graham", "username": "Bret", "email": "Sincere@april.biz", "address": {"street": "Kulas Light", "suite": "Apt. 556", "city": "Gwenborough", "zipcode": "92998-3874"}}
```

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

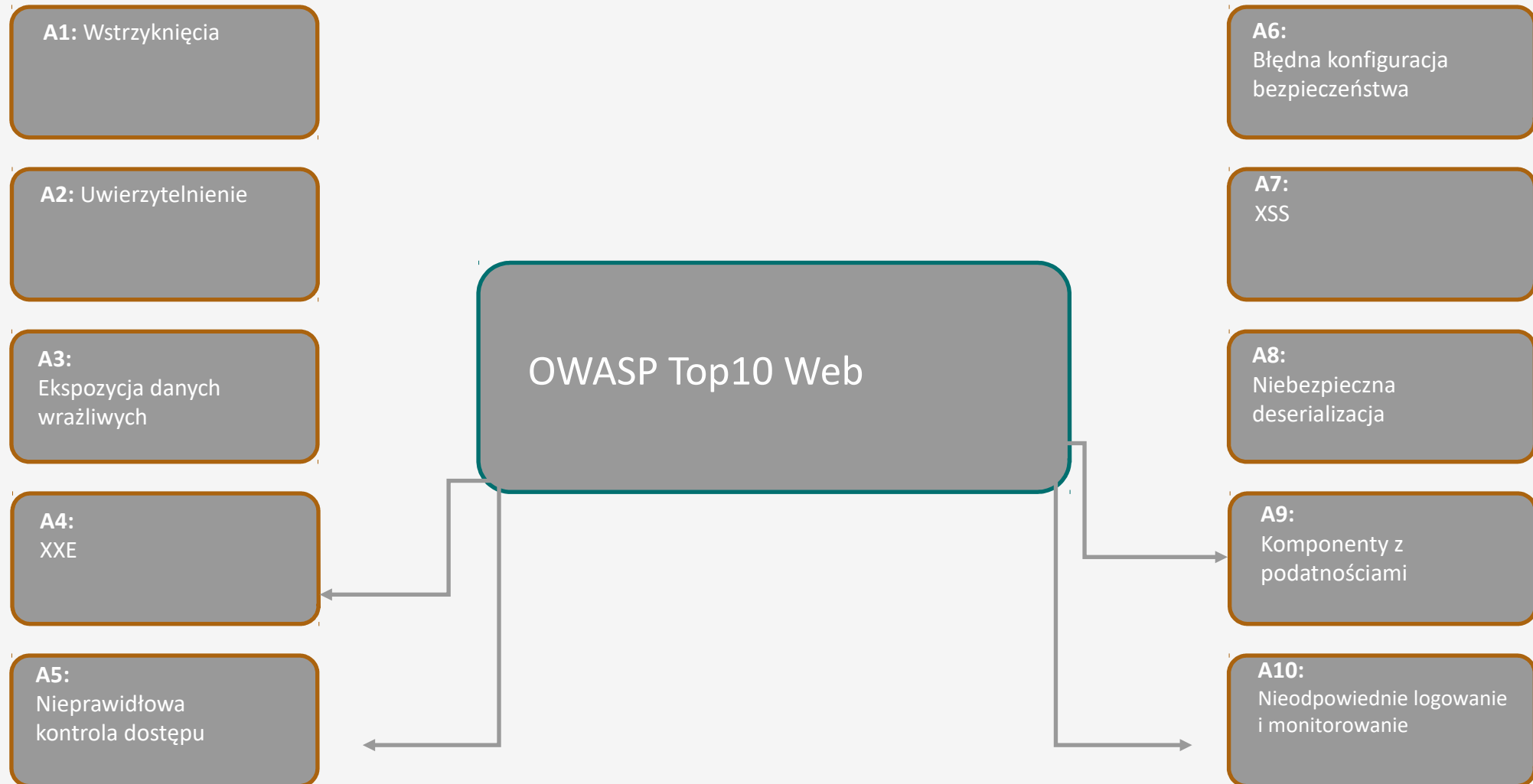


OWASP Top10 - IoT



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.

OWASP Top10 Web



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, niezałatane 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.

OWASP Top10 Web



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.

OWASP Top10 Web



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 niezłałatana, 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

Penetration Testing Execution Standard



Zwięzłe opisy zagrożeń i elementów istotnych podczas testów

- Dzieli testy na 7 etapów:
 - ✓ **Przygotowanie**
 - ✓ **Gromadzenie informacji**
 - ✓ **Modelowanie zagrożeń**
 - ✓ **Analiza podatności**
 - ✓ **Eksploracja**
 - ✓ **Post-eksploracja**
 - ✓ **Raportowanie**
- **Niektóre rozdziały nie są ukończone!**

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 ta aplikacja**)
- *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