

Alati za statičku i dinamičku analizu koda

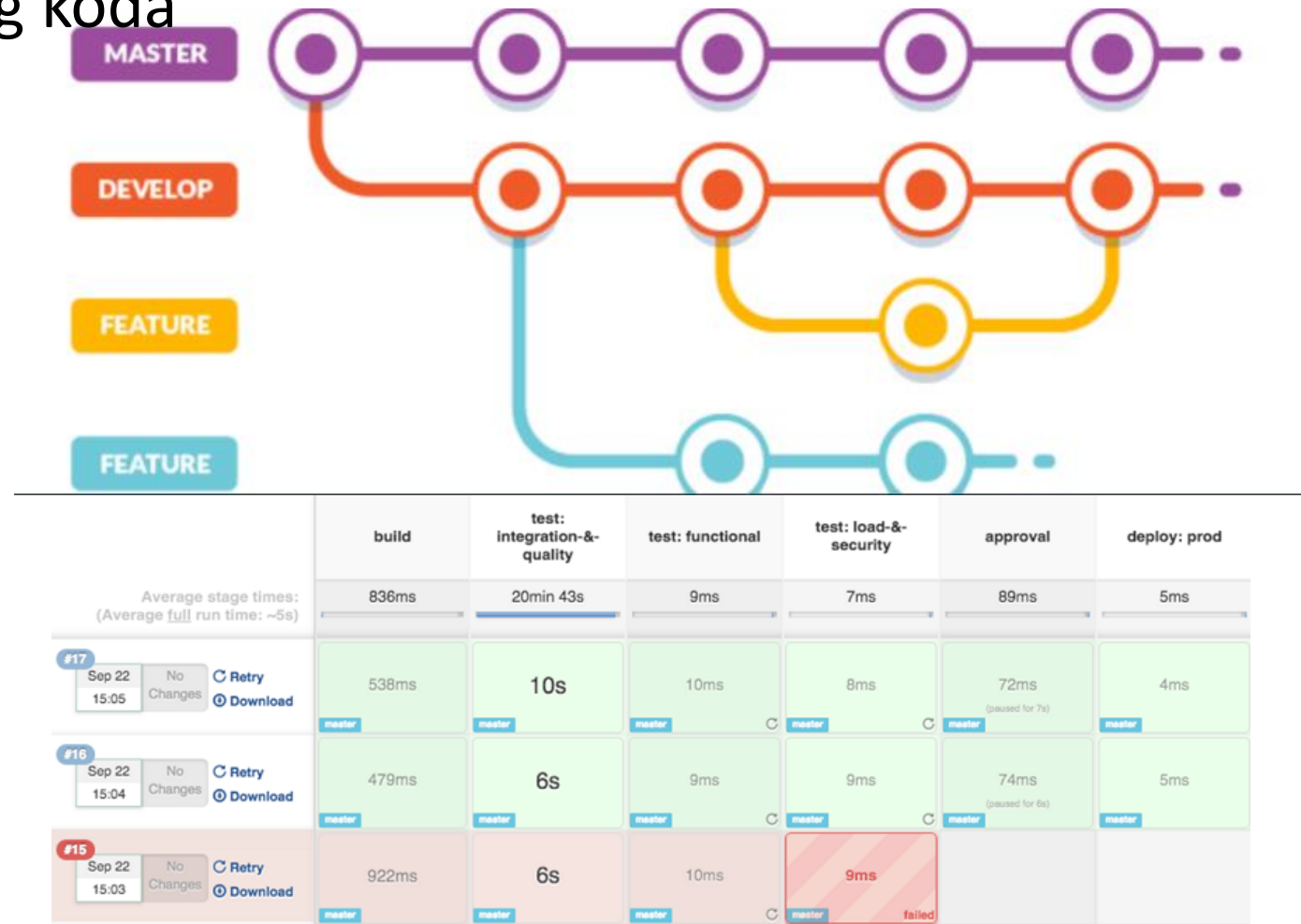


ОБАВЕШТЕЊЕ ЗА СТУДЕНТЕ

- Настава на предмету Развој безбедног софтвера подразумева изучавање различитих механизма којима се нарушава информациона безбедност и врше напади на интернет апликације и софтверске системе.
- Студенти на предмету Развој безбедног софтвера могу ове методе за потребе изучавања да користе искључиво у оквиру затвореног лабораторијског окружења које је обезбеђено за наставу на предмету Развој безбедног софтвера.
- Студенти не могу да подразумевају да су на било који начин охрабрени од стране наставника или да им се препоручује да користе ове методе који се изучавају према другим апликацијама Електротехничког факултета или апликацијама било ког трећег правног или физичког лица.
- Свака евентуална активност коју би предузео неки студент коришћењем ових метода и механизма према апликацијама које нису у оквиру лабораторије на предмету искључива је одговорност студента.

Okolnosti rada softverskog inženjera

- Veliki projekti – dosta izvornog koda
- Legacy kod
- Tim ljudi
- Verzioniranje koda
- Način puštanja u produkciju



Statička analiza koda

Statička analiza koda (ili Analiza izvornog koda) se obično izvršava kao deo revizije koda u toku implementacije softvera.

Alat ima potpun uvid u kod – White Box princip

Izvršava se ručno ili pomoću alata. Alati samo pomažu da se lakše pronađu ranjivosti.

Alati nisu savršeni.

Alat: Veracode

1

APPLICATION

Profile

Metadata

SANDBOXES

SCANS

In Progress

Completed

RESULTS

Results

Latest

View Report

Triage Flaws

Mitigated Flaws

DynamicDS Scan

16 Aug 2016 Dynamic

Bookmarked Reports

Dynamic Flaw Inventory

Application: DVR Demo 2

VERACODE

Dynamic Flaw Inventory

The flaw inventory is a list of all the flaws found during past scans and their current statuses.

All (50)New (4)Open and Reopened (38)Cannot Reproduce (7)Fixed (1)

1 of 1

Rows 50

Flaw ID	CWE ID and Name	Severity	Status	Date Found	Path	Details
50	80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Medium	New	16 Aug 2016	/smoketest2/app.php	View
49	327 Use of a Broken or Risky Cryptographic Algorithm	Medium	New	16 Aug 2016	/smoketest2/	View
48	829 Inclusion of Functionality from Untrusted Control Sphere	Medium	New	16 Aug 2016	/smoketest2/	View
47	16 Configuration	Informational	New	16 Aug 2016	/smoketest2/	View
46	79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium	Open	18 May 2016	/smoketest2/app.php	View
45	79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium	Open	18 May 2016	/smoketest2/app.php	View
44	80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Medium	Open	18 May 2016	/smoketest2/app.php?input=%3cscript%3e%3c%2fscript%3e%3cscript%3ephocidCallback%281811085665%29%3c%2fscript%3e%3c%2fscript%3e	View
43	526 Information Exposure Through Environmental Variables	Low	Open	11 May 2016	/smoketest2/app.php	View
42	79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium	Open	11 May 2016	/smoketest2/app.php?input=%3cscript%3e1%3b%3bphocidCallback%289039595772%29%3b1%3c%2fscript%3e	View
41	16 Configuration	Informational	Open	11 May 2016	/smoketest2/	View
40	601 URL Redirection to Untrusted Site ('Open Redirect')	Medium	Open	11 May 2016	/smoketest2/app.php	View

© Veracode, Inc. 2006 - 2016

Usage Guidelines

Responsible Disclosure Policy

Veracode Support

Last account activity on 8/19/16 10:11 AM EDT from IP: 10.130.35.181

For use under U.S. Pat. Nos. 8,365,155, 7,752,609, and 5,854,824, and patents pending.

Alat: FindSecBugs

The screenshot displays the FindSecBugs-IDEA plugin interface within an Android Studio environment. The top pane shows the project structure and the source code of `DoTransfer.java`. The bottom pane displays the 'FindSecBugs-IDEA FindBugs Analysis Results' for `InsecureBankv2`, listing 14 security items. A detailed view of the 'External File Access (Android)' bug is shown on the right, explaining the risk of writing confidential data to external storage and providing a better alternative using `Context.MODE_PRIVATE`.

FindSecBugs-IDEA FindBugs Analysis Results

- InsecureBankv2 (found 14 bug items in 59 classes) [more](#)
 - Security (14 items)
 - Static IV (2 items)
 - Cipher is susceptible to padding oracle attack (2 items)
 - Cipher with no integrity (2 items)
 - External File Access (Android) (4 items)
 - Files could be saved to external storage. (4 items)
 - WebView with JavaScript Enabled (Android) (1 item)
 - Potential Path Traversal (File Write) (2 items)
 - Broadcast (Android) (1 item)

External File Access (Android)

The application write data to external storage (potentially SD card). There are multiple security implication to this action. First, file store on SD card will be accessible to the application having the `READ_EXTERNAL_STORAGE` permission. Also, if the data persisted contains confidential information about the user, encryption would be needed.

Code at risk:

```
file file = new File(getExternalStorageDirectory() + "/Statements");
fos = new FileOutputStream(file);
fos.write(confidentialData.getBytes());
fos.flush();
```

Better alternative:

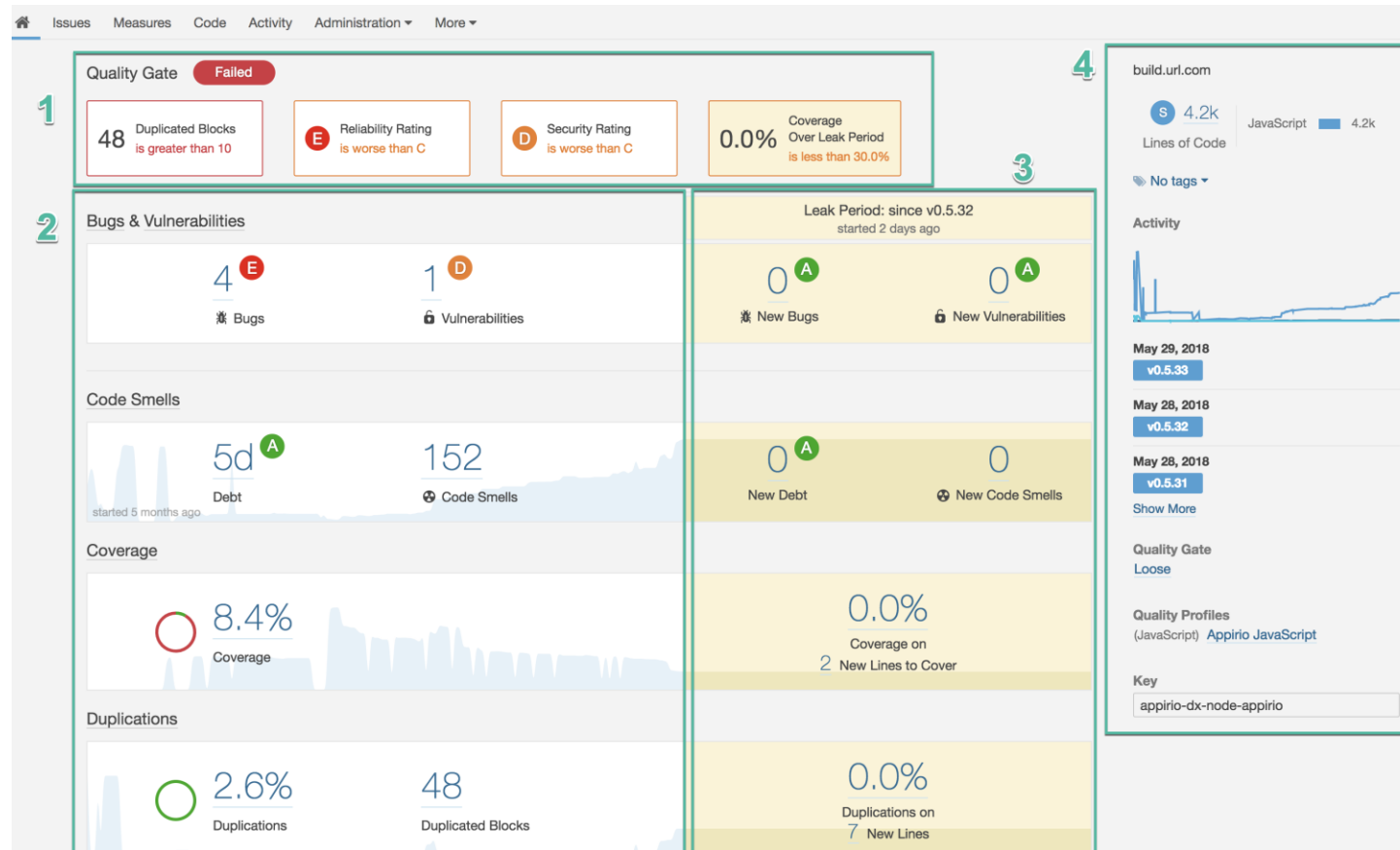
```
fos = openFileOutput(filename, Context.MODE_PRIVATE);
fos.write(string.getBytes());
```

References

CERT: DRD00-J: Do not store sensitive information on external storage [...]
[Android Official Docs Using the External Storage](#)

This gives a longer description of the detected bug pattern

Alat: SonarQube



Tumačenje izveštaja

Svaka ranjivost koju alat pronade ima reference na neku od baza ranjivosti.

Common Weakness Enumeration (CWE)

<https://cwe.mitre.org/>

Example:

CWE-89 <https://cwe.mitre.org/data/definitions/89.html>

Ograničenja

		Tačnost	
		Tačno	Netačno
Ranjivost postoji	Pozitivno	Istinski pozitivan (True Positive)	Lažno pozitivan (False Positive)
	Negativno	Istinski negativan (True Negative)	Lažno negativan (False Negative)

Ograničenja

- Lažno pozitivan
 - Pronalazak ranjivosti koja zapravo nije ranjivost.
 - Posledica: Gubitak vremena za analizu. Označavanja kao *false positive*.
- Lažno negativan
 - Ranjivost postoji, ali nije pronađena!
 - Posledica: Velika verovatnoća za propust inženjera koji analizira kod.

		Tačnost	
		Tačno	Netačno
Rezultat	Pozitivno	Istinski pozitivan (True Positive)	Lažno pozitivan (False Positive)
	Negativno	Istinski negativan (True Negative)	Lažno negativan (False Negative)

Radnje na izveštaju

TRUE POSITIVE

1. Confirm
2. Nov zadatak u listi zadataka za tim
3. Prioritizacija zadatka prema riziku koji predstavlja
4. Popravka



Radnje na izveštaju

FALSE POSITIVE

1. Resolve as false positive
2. Ostaviti komentar sa argumentacijom zašto se veruje da je FP.

Jako je važno obeležiti FP da bi se ostavio trag da je nađena ranjivost adresirana.



Radnje na izveštaju

TRUE NEGATIVE → Ništa nije prijavljeno. Nema ranjivosti, ni akcije.

FALSE NEGATIVE → Ništa nije prijavljeno.

Ranjivost postoji, ali akcija nije moguća! 😞



Demonstracija na SonarQube

Statička analiza koda

Pokretanje

Tumačenje izveštaja

1. git checkout staticka-i-dinamicka-analiza-koda
2. Start Sonar Qube server:
 - Nađite direktorijum za SonarQube
 - Uđite u bin folder
 - Odaberite distribuciju za Vaš operativni sistem
 - Startujte StartSonar.bat

```
Directory of C:\Users\pevu\Desktop\sonarqube-9.1.0.47736\sonarqube-9.1.0.47736\bin\windows-x86-64
```

```
22.11.2021. 15:51 <DIR> .
22.11.2021. 15:51 <DIR> ..
22.11.2021. 15:51 <DIR> lib
22.11.2021. 15:51      1.214 StartNTService.bat
22.11.2021. 15:51      1.371 StartSonar.bat
22.11.2021. 15:51      1.212 StopNTService.bat
22.11.2021. 15:51    220.672 wrapper.exe
          4 File(s)      224.469 bytes
          3 Dir(s)  356.756.971.520 bytes free
```

```
C:\Users\pevu\Desktop\sonarqube-9.1.0.47736\sonarqube-9.1.0.47736\bin\windows-x86-64>
```

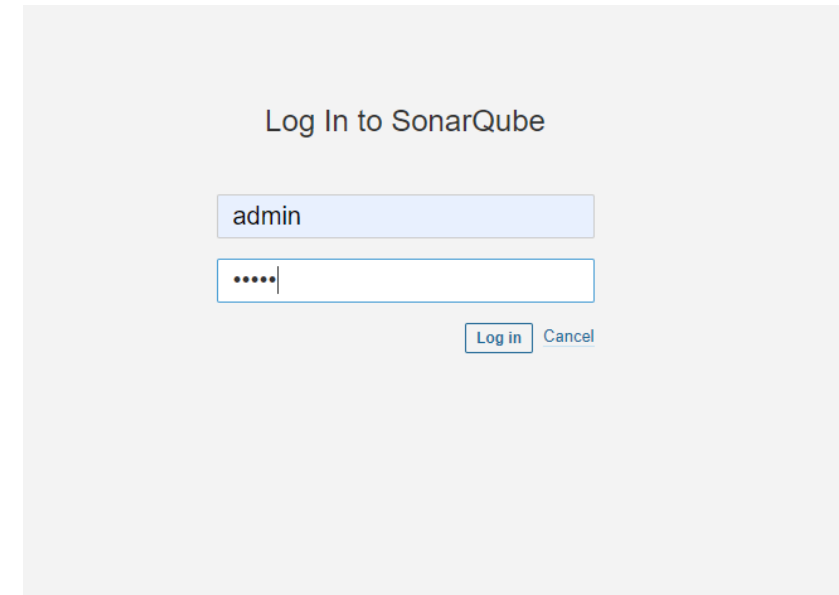
Idite na localhost:9000

Login:

User: admin

Password: admin

Morate promeniti šifru da nastavite



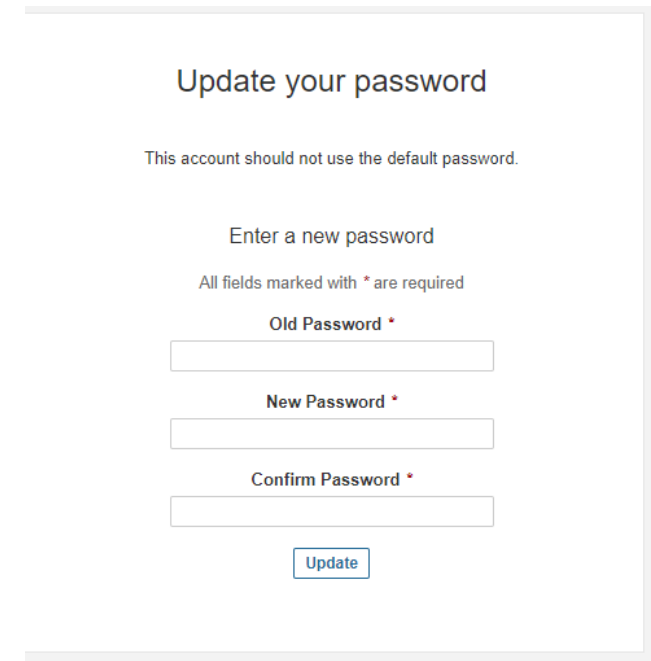
Log In to SonarQube

admin

.....

Log in Cancel

This screenshot shows the SonarQube login interface. It has a title 'Log In to SonarQube'. Below the title are two input fields: the first contains the text 'admin', and the second contains five dots, indicating a password. To the right of the password field are two buttons: 'Log in' and 'Cancel'.



Update your password

This account should not use the default password.

Enter a new password

All fields marked with * are required

Old Password *

New Password *

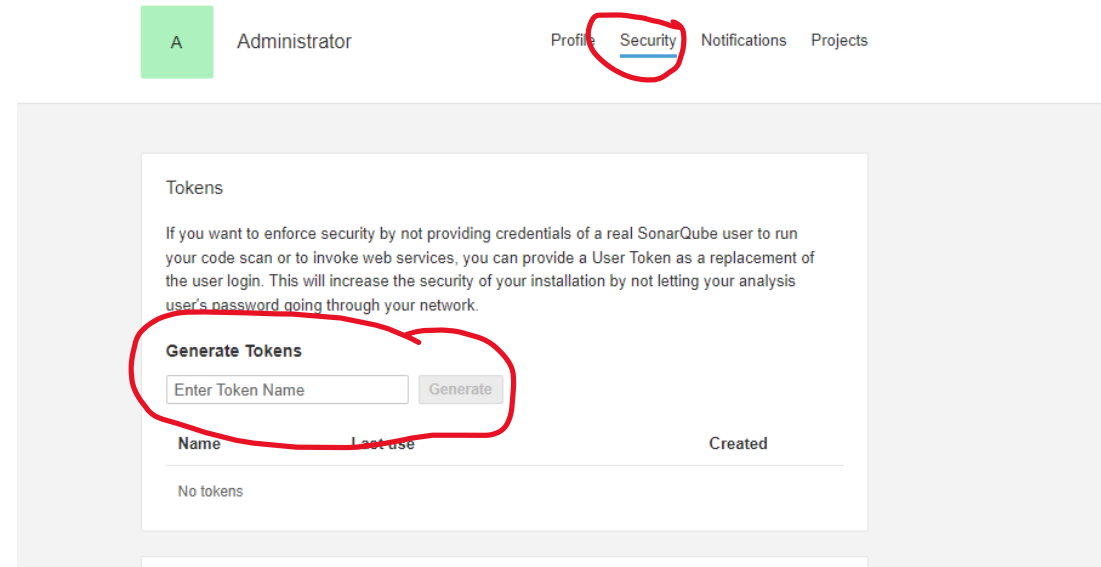
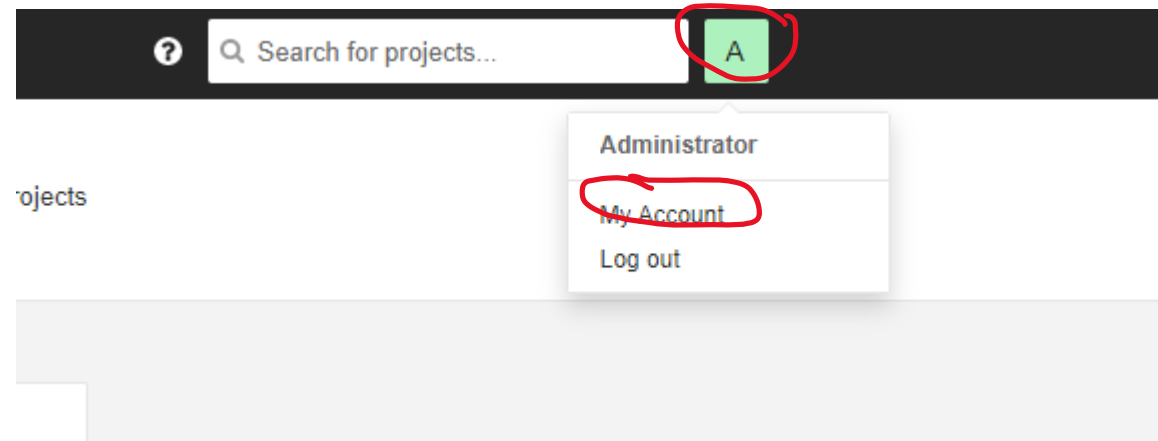
Confirm Password *

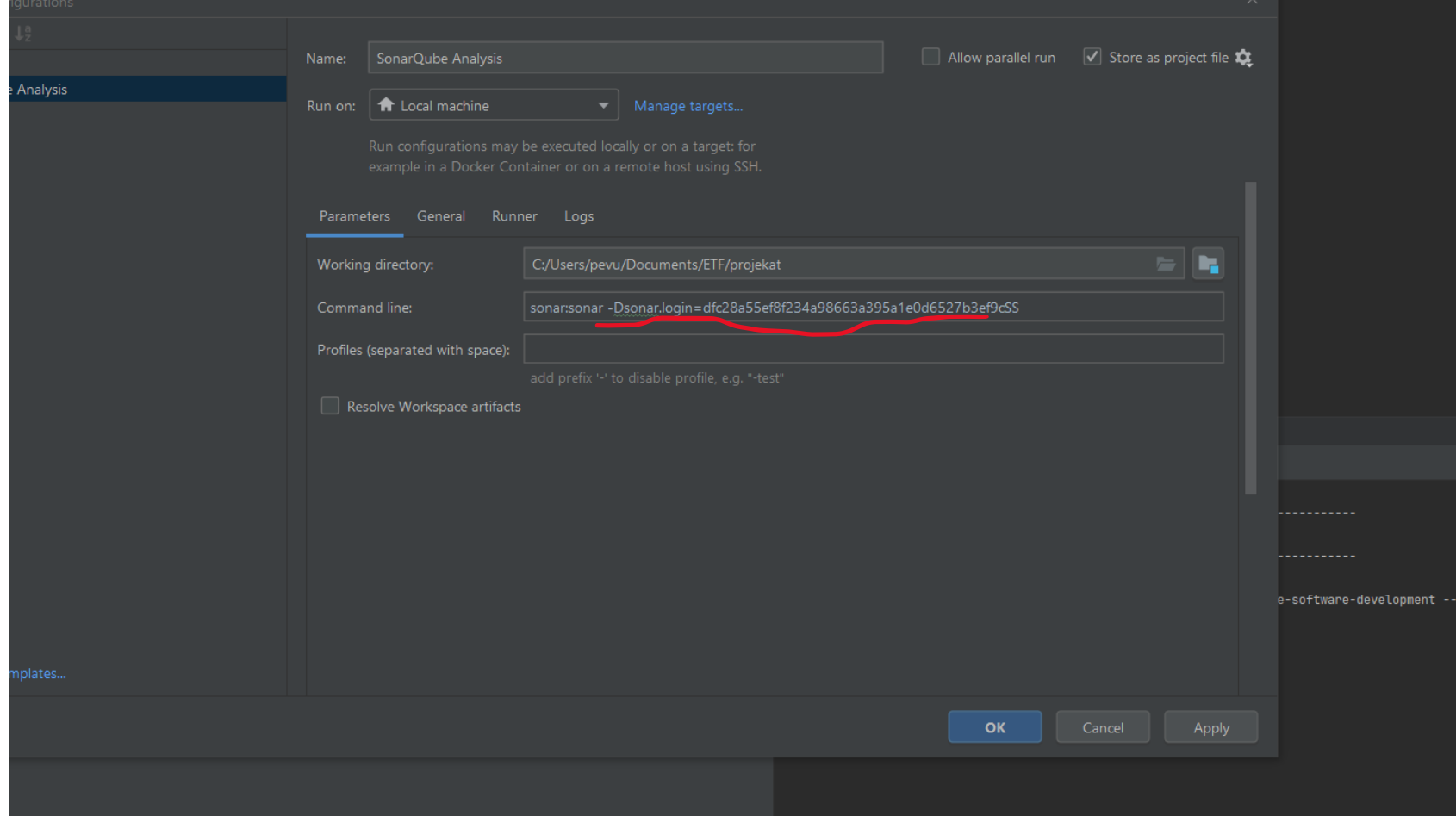
Update

This screenshot shows the SonarQube password update interface. It has a title 'Update your password'. Below the title is a message: 'This account should not use the default password.' followed by the instruction 'Enter a new password'. Below this is a note: 'All fields marked with * are required'. There are three input fields, each with a label above it: 'Old Password *', 'New Password *', and 'Confirm Password *'. At the bottom of the form is an 'Update' button.

Kliknite na nalog > My Account

Zatim Security i generišite novi token





U SonarQube run konfiguraciji dodajte parametre :

sonar:sonar

-Dsonar.projectKey=<ime projekta u Sonaru>

-Dsonar.host.url =<url sonar servera>

-Dsonar.login=<key koji ste generisali na sonaru>

Koraci

Safe = False Positive

Ensure that string concatenation is required and safe for this SQL query.

Add Comment

Get Permalink

Category SQL Injection

Review priority HIGH

Assignee Not assigned

Select a status...

src/.../secursoftwaredevelopment/repository/CarRepository

```
26
27 public Car findById(String id) {
28     String sqlQuery = "SELECT id, price,
29     try (Connection connection = dataSource
30         Statement statement = connection
31         ResultSet rs = statement.execute
32         if (rs.next()) {
33             return createCar(rs);
34         }
35     } catch (SQLException e) {
36         e.printStackTrace();
```

To review

- ☒ This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

Fixed

- ☐ The code has been modified to follow recommended secure coding practices.

Safe

- ☐ The code is not at risk and doesn't need to be modified.

Add a comment (Optional)

Markdown Help : ***Bold*** ```Code``` * Bulleted point

What's the risk?

Are you at risk?

How can you fix it?

Change status

Samostalni rad

Opis

- Analizirajte izveštaj
- Obeležite False Positive stavke i ostavite komentar na njih u SonarQube
 - U zavisnosti od okruženja i početnog stanja trebalo bi da bude 1-6 false positive
- Vreme: **15 minuta**

Dinamička analiza

Alati za dinamičko testiranje

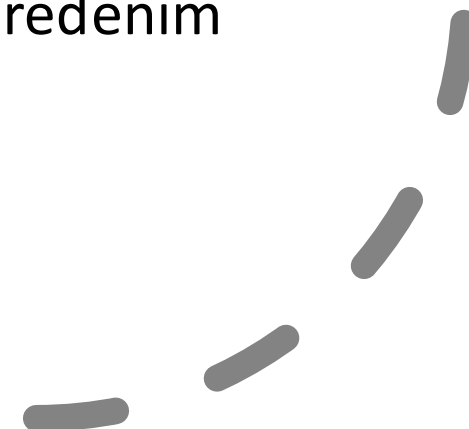
Alati koji automatski analiziraju i pronalaze ranjivosti nad aplikacijama dok rade (runtime). Nemaju pristup izvornom kodu (black box princip).

Nekada se koriste u Manual Penetration Testing operacijama.

Šalju zlonamerne unose kako bi pronašli ranjivost.

Analiziraju

- Validaciju ulaza i izlaza
- Aplikacione probleme povezane sa određenim ranjivostima
- Greške u konfiguraciji servera



1

APPLICATION

Profile

Metadata

SANDBOXES

SCANS

In Progress

Completed

RESULTS

Results Latest

View Report

Triage Flaws

Mitigated Flaws

DynamicDS Scan 16 Aug 2016 Dynamic

Bookmarked Reports

Dynamic Flaw Inventory

Application: DVR Demo 2

Dynamic Flaw Inventory

The flaw inventory is a list of all the flaws found during past scans and their current statuses.

All (50)
New (4)
Open and Reopened (38)
Cannot Reproduce (7)
Fixed (1)

Flaw ID	CWE ID and Name	Severity	Status	Date Found	Path	Details
50	80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Medium	New	16 Aug 2016	/smoketest2/app.php	View
49	327 Use of a Broken or Risky Cryptographic Algorithm	Medium	New	16 Aug 2016	/smoketest2/	View
48	829 Inclusion of Functionality from Untrusted Control Sphere	Medium	New	16 Aug 2016	/smoketest2/	View
47	16 Configuration	Informational	New	16 Aug 2016	/smoketest2/	View
46	79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium	Open	18 May 2016	/smoketest2/app.php	View
45	79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium	Open	18 May 2016	/smoketest2/app.php	View
44	80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Medium	Open	18 May 2016	/smoketest2/app.php?input=%3cscript%3e%3c%2fscript%3e%3cscript%3epholicidCallback%28181108566%29%3c%2fscript%3e%3c%2fscript%3e	View
43	526 Information Exposure Through Environmental Variables	Low	Open	11 May 2016	/smoketest2/app.php	View
42	79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium	Open	11 May 2016	/smoketest2/app.php?input=%3cscript%3e1%3b%3bpholicidCallback%289039595772%29%3b1%3c%2fscript%3e	View
41	16 Configuration	Informational	Open	11 May 2016	/smoketest2/	View
40	601 URL Redirection to Untrusted Site ('Open Redirect')	Medium	Open	11 May 2016	/smoketest2/app.php	View

Alat: Fortify

APPLICATIONS

DASHBOARD

REPORTS

ADMINISTRATION

23

DYLAN

Your Applications

Managed 62

Discovered 830

Ignored 296

Search Text

+ NEW APPLICATION

62 found

Display: 25 50 100

expand all

collapse all

NAME

PRODUCTION RISK & POLICY COMPLIANCE

SCAN & SECURITY STATUS

MOST RECENT CHANGE

PGAdmin

1 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

08/17/2017

New Monitoring Vulnerabilities Detected

Advantage Online Banking

2 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

11/01/2017

New Static Vulnerabilities Detected

Demo App for Deletion

5 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

10/31/2017

New Static Vulnerabilities Detected

everywhere.com

4 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

08/11/2017

Release Failing Security Policy

Cobol Sample

2 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

04/28/2017

New Dynamic Vulnerabilities Detected

Zero

2 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

08/24/2017

New Monitoring Vulnerabilities Detected

Custom Banking App

1 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

MOBILE

NETWORK

MONITORING

APP DEF

01/18/2017

New Mobile Vulnerabilities Detected

emea.hpford.com

1 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

06/23/2017

New Monitoring Vulnerabilities Detected

Drupal

1 RELEASES

Business Criticality: HIGH

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

08/11/2017

Release Failing Security Policy

Microservices App

6 RELEASES

Business Criticality: MEDIUM

FAIL

CRITICAL

HIGH

MEDIUM

LOW

STATIC

DYNAMIC

NETWORK

MONITORING

APP DEF

08/15/2017

Release Failing Security Policy

SORT

Production Risk

AGENCY

(Not Set)

Acme

Coders Inc

DevStarz

Internal Team

Pinnacle

APPLICATION DEFENDER

APPLICATION MONITORING

APPLICATION TYPE

BUSINESS CRITICALITY

BUSINESS UNIT

COMPLIANCE REQUIREMENT

DYNAMIC SCAN STATUS

MOBILE SCAN STATUS

MOST RECENT CHANGE

PASS/FAIL

REGION

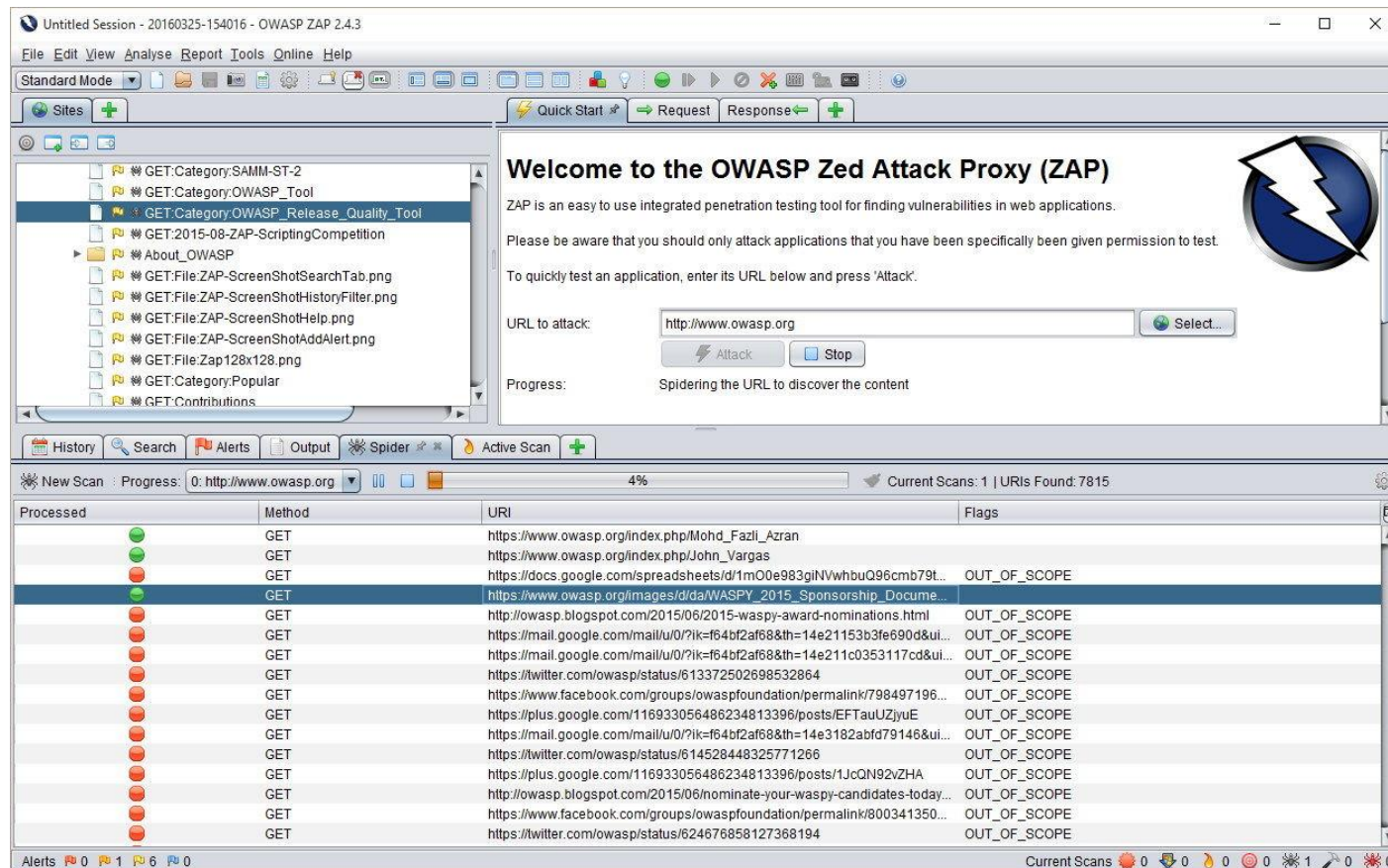
SCAN TYPE

STAR RATING

STATIC SCAN STATUS

SVP

Alat: OWASP ZAP - <https://www.zaproxy.org/download/>



Ograničenja

- Ista kao za statičku analizu koda
- Dobri alati treba da uključuju i fuzz testing
 - Slanje nasumičnih i loše formiranih podataka u velikoj količini
 - Pronalazi slabosti u RegExu, buffer overflow, integer overflow...

		Tačnost	
		Tačno	Netačno
Rezultat	Pozitivno	Istinski pozitivan (True Positive)	Lažno pozitivan (False Positive)
	Negativno	Istinski negativan (True Negative)	Lažno negativan (False Negative)

Tumačenje izveštaja OWASP ZAP

- Description

Kratak opis kako se ranjivost ispoljava u aplikaciji

- Solution

Preporuka za popravku

- Reference

Reference koje detaljno objašnjavaju napad i kako da se popravi

<https://cwe.mitre.org/index.html>

Primer: **Cross-site Scripting CWE**

<https://cwe.mitre.org/data/definitions/79.html>

Demonstracija

Dinamičko testiranje

OWASP ZAP – Inicijalni scan

Ovim detektujemo eksterne dostupne stranice koje ne zahtevaju login.


1. Pokrenite aplikaciju, kliknite ikonicu OWASP ZAP
2. Automated Scan
3. URL to attack: **http://localhost:8080/ > Attack**
4. Sites > http://localhost:8080 (right click) > Include in Context > Default Context > OK

OWASP ZAP – Podešavanje logina

1. POST:perform-login(password,username) (**right click**) > Flag as Context > Form-based Auth Login Request
2. Login Request POST Data postaviti na **username={%username%}&password={%password%}**
3. Otvorite sekciju **Users**
4. **Add** > **Username: bruce, password: wayne** > Click **Add** > **OK**

OWASP ZAP – Podešavanje logina

Configure Authentication Method

Login Form Target URL *:
  Select...

Login Request POST Data (if any):

Username Parameter *: Password Parameter *:






Session Properties

- ▼ Session
 - General
 - Exclude from Proxy
 - Exclude from Scanner
 - Exclude from Spider
- ▼ Contexts
 - ▼ 1:Default Context
 - 1: Include in Context
 - 1: Exclude from Context
 - 1: Structure
 - 1: Technology
 - 1: Authentication
 - 1: Users**
 - 1: Forced User

1: Users

Users which can be used for various operations for this context.

Enabled	ID	Name
<input checked="" type="checkbox"/>	14	bruce

 Add...
 Modify...
 Remove
 Enable All
 Disable All

OWASP ZAP – Scan

1. Default Context (**right click**) > **Spider**
2. Set **User** na **bruce** > **Start scan**
3. Default Context (**right click**) > **Active Scan**
4. Set **User** na **bruce** > **Start scan**
5. Kad završi scan > **Alerts tab** u donjem odeljku
6. U meniju Report > Generate HTML Report

OWASP ZAP – Svi koraci

1. **Pokrenite aplikaciju**
2. Kliknite ikonicu OWASP ZAP
3. Automated Scan
4. URL to attack: `http://localhost:8080/` > **Attack**
5. Sites > <http://localhost:8080> (**right click**) > Include in Context > Default Context > OK
6. POST:perform-login(password,username) (**right click**) > Flag as Context > Form-based Auth Login Request
7. Login Request postaviti na `username={%username%}&password={%password%}`
8. Otvorite sekciju **Users**
9. **Add** > Username: **bruce**, password: **wayne** > Click **Add** > **OK**
10. Default Context (**right click**) > **Spider**
11. Set **User** na **bruce** > **Start scan**
12. Default Context (**right click**) > **Active Scan**
13. Set **User** na **bruce** > **Start scan**
14. Kad završi scan > **Alerts tab** u donjem odeljku
15. U meniju Report > Generate HTML Report

Priprema za samostalni rad

1. Instalirajte OWASP ZAP (<https://www.zaproxy.org/download/>)
2. Otvorite IntelliJ Idea
3. U terminalu izvršite **git checkout staticka-i-dinamicka-analiza-koda**
4. Zatim **git reset --hard**
5. Pokrenite aplikaciju

Tumačenje rezultata

- koristite <https://www.zaproxy.org/docs/alerts/> za identifikaciju propusta
- Vreme rada 15 min

Koliko često koristiti alate?

Koliko često koristiti alate?

- Treba odrediti učestalost izvršavanja analiza i uvek ih se držati
- Period treba da bude tako određen da ispunjava sledeće uslove
 - Da ne opterećuje budžet projekta
 - Da ne utiče na učinak tima
 - Da ne opterećuje tim motivaciono
 - Da smanjuje rizik

Da li je static/dynamic analiza dovoljna?



Manual Penetration Testing

Manual Penetration Testing

Planiranje

- Obim i strategija zadatka
- Obim se zasniva na postojećim sigurnosnim polisama i standardima
- Dogovor sa klijentom i **potpisivanje ugovora**

Analiza

- Sakupljanje informacija
- Skeniranje i ispitivanje ulaza (portovi, APIs, stranice...)
- Potraga za ranjivostima

Napad

Napad (sledeći slajd)

Izveštaj

- Nalazi sa koracima za reprodukciju
- Definisanje rizici i uticaja
- Preporuke i rešenja

TOP SECRET

Manual Penetration Testing

Faze napada:

1. Zadobijanje pristupa

Eksploatisanje ranjivosti radi zadobijanja pristupa

2. Održavanje pristupa

Instaliranje trajnog prisustva (trojanac, otvaranje portova itd.)

3. Eksploatisanje

Narušavanje poverljivosti, integriteta i dostupnosti

4. Sakupljanje dokaza

Koriste se pri pravljenju izveštaja