Security Scanning

Tetiana Chupryna

Toruń GitLab Day, 9 Dec 2020

Tetiana

Backend Developer @ GitLab

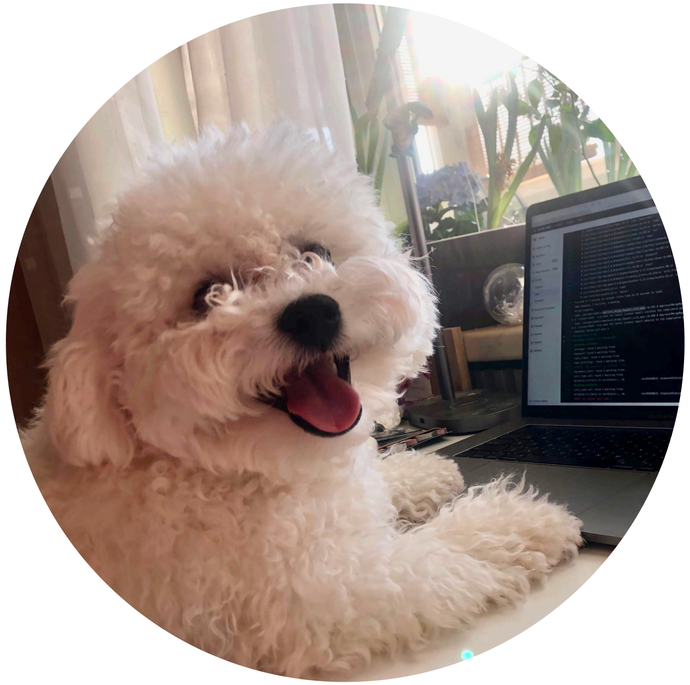
I work on Security features

I live in Kharkiv, Ukraine

Here is my dog Darcy

- lichess@brytannia
- twitter@TetianaOfficial
- gitlab@brytannia

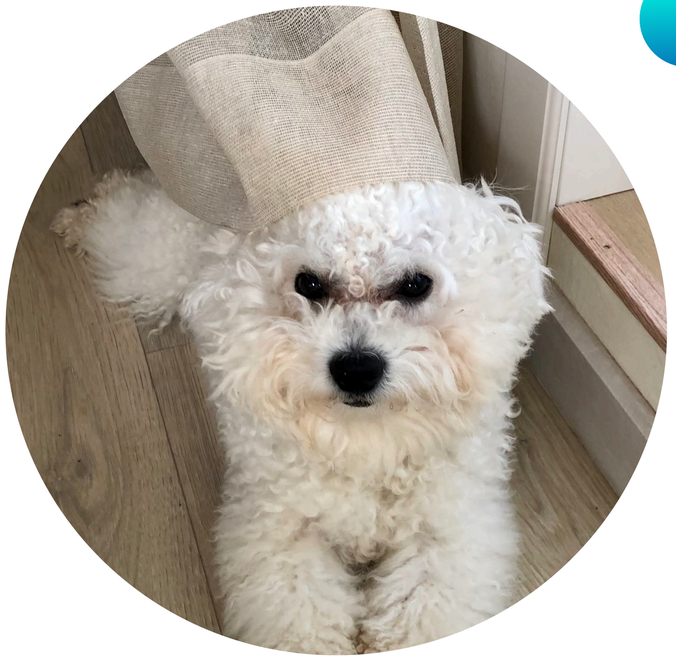
Let me tell a story



Alice

Lead Dev @ Goodboy

She uses GitLab



Bob

Hides his treats with Goodboy

Trudy

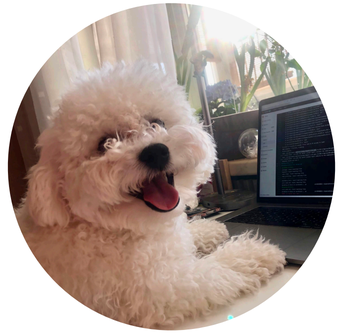
Wants to steal ALL THE TREATS

Trudy breaks the Goodboy web-site and steals hidden bones and cucumbers

Walter

Private investigator

Helps find breach and apply security fix



Why my code is vulnerable?

945000000000$

World economy lost due to hacker attacks in 2020 *(McAfee report)*

96%

had security incidents

Application security is important, and even more important

Attack vectors

- Hardware
- Software
- Fishing

4 of the 6 top attacks were application based

Security scanners

- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Dependency Scanning
- Container Scanning
- Fuzz testing
- Secret Detection

SAST

White box

- Testing from inside out
- Tools are technology dependent
- Similar to code quality but for security
- In GitLab Core since 13.3

DAST

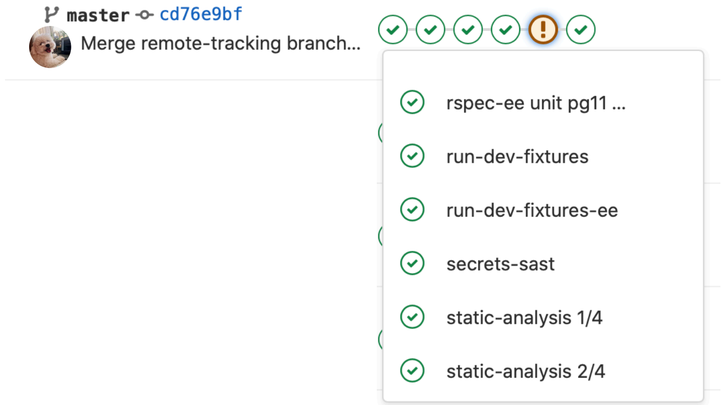
Black box

- Testing from outside
- Live attack on staging
- HTTP - lingua-franca
- GitLab Ultimate

gitlab_ci.yml

```
include:
  - template: SAST.gitlab-ci.yml
  - template: DAST.gitlab-ci.yml

variables:
  DAST_WEBSITE: https://staging.goodboy.com
```



Pipeline view

Pipeline | Needs | Jobs 3 | Tests 0 | **Security** | Licenses 0

Severity All severities

Scanner SAST

Hide dismissed

Severity	Vulnerability	Identifier	Scanner
Unknown	The cookie is missing security flag Secure WebGoat/App_Code/CookieManager.cs	SCS0008	SAST GitLab
Unknown	The cookie is missing security flag HttpOnly WebGoat/App_Code/CookieManager.cs	SCS0009	SAST GitLab
Unknown	Weak hashing function WebGoat/Content/EncryptVSEncode.aspx.cs	SCS0006	SAST GitLab
Unknown	Potential XSS vulnerability WebGoat/Content/ForgotPassword.aspx.cs	SCS0029	SAST GitLab
Unknown	The cookie is missing security flag Secure WebGoat/Content/ForgotPassword.aspx.cs	SCS0008	SAST GitLab

Vulnerability report

Vulnerability Report

Export

The Vulnerability Report shows the results of the last successful pipeline run on the default branch.

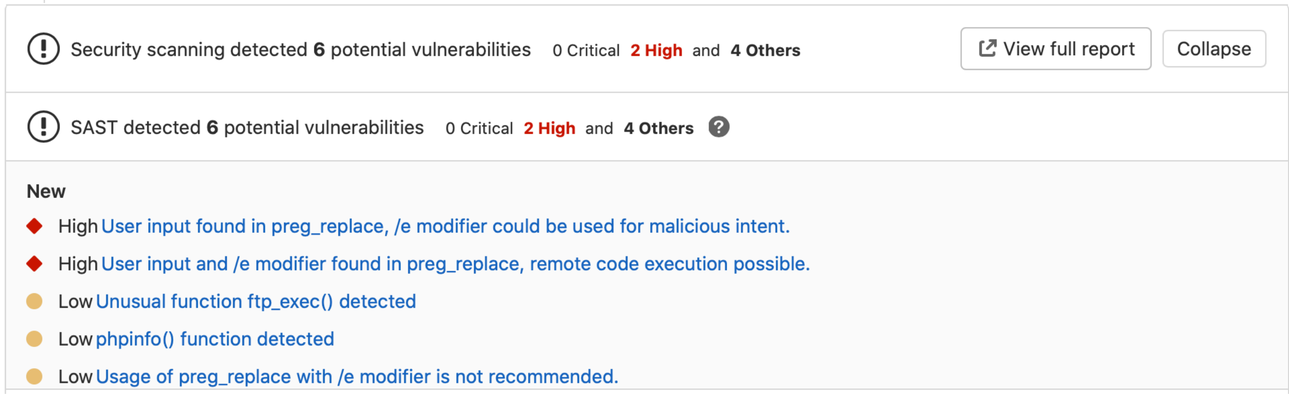
Last updated 1 day ago #225824769 1 failed security job

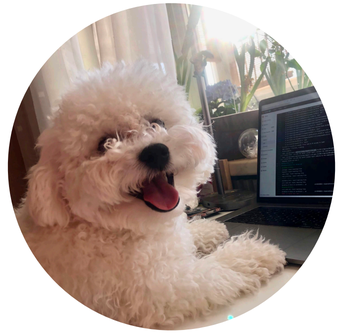
Critical	High	Medium	Low	Info	Unknown
2	0	0	26	5	1938

Status Detected +1 more | **Severity** All severities | **Scanner** DAST +1 more

Detected	Status	↓ Severity	Description	Identifier	Scanner	Activity
2020-05-27	Detected	Critical	Password in URL `docker-compose-custom.yml (line: 7)`	TruffleHog rule ID Password in URL	SAST	
2020-05-27	Detected	Critical	Password in URL `.gitlab-ci.yml (line: 123)`	TruffleHog rule ID Password in URL	SAST	
2020-02-23	Detected	Low	Cookie Without SameSite Attribute	CWE-16 + 2 more	DAST	
2020-02-23	Detected	Low	Cookie Without SameSite Attribute	CWE-16 + 2 more	DAST	
2020-01-19	Detected	Low	Absence of Anti-CSRF Tokens	Absence of Anti-CSRF Tokens + 2 more	DAST	
2020-01-19	Detected	Low	Absence of Anti-CSRF Tokens	Absence of Anti-CSRF Tokens + 2 more	DAST	
2020-01-19	Detected	Low	Absence of Anti-CSRF Tokens	Absence of Anti-CSRF Tokens + 2 more	DAST	

Merge Request View





Now my application is secure!

Now I can use the app!

No!

Let me introduce Heidi

Heidi

Lead Dev @ Tag-o-war

Her library uses Alice

Dependency scanning

Part of Composition Analysis

- Checking for vulnerabilities in dependency packages
- Tools are technology dependent
- In GitLab Ultimate

gitlab_ci.yml

```
include:
  - template: SAST.gitlab-ci.yml
  - template: DAST.gitlab-ci.yml
  - template: Dependency-Scanning.gitlab-ci.yml

variables:
  DAST_WEBSITE: https://staging.goodboy.com
```

Dependency list

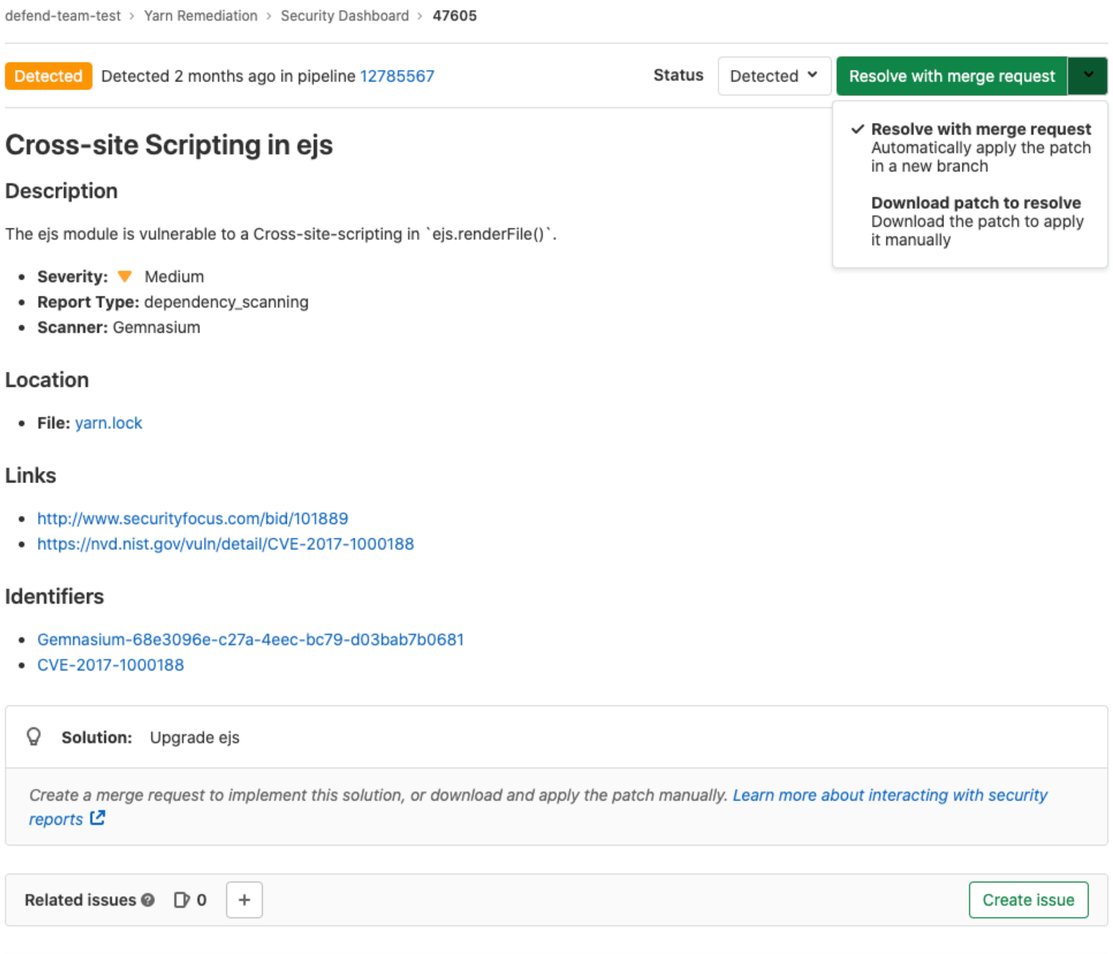
Dependencies

Based on the latest successful scan • 1 day ago

Severity | Export

Component	Packager	Location	License	
com.fasterxml.jackson.core/jackson-databind 2.9.2	Java (Maven)	pom.xml		9 vulnerabilities detected
Critical	Deserialization of Untrusted Data in com.fasterxml.jackson.core/jackson-databind			
Critical	Server-Side Request Forgery (SSRF) in com.fasterxml.jackson.core/jackson-databind			
Critical	Improper Input Validation in com.fasterxml.jackson.core/jackson-databind			
Critical	Improper Restriction of XML External Entity Reference in com.fasterxml.jackson.core/jackson-databind			
High	Deserialization of Untrusted Data in com.fasterxml.jackson.core/jackson-databind			
High	Information Exposure in com.fasterxml.jackson.core/jackson-databind			
Medium	Improper Input Validation in com.fasterxml.jackson.core/jackson-databind			
Medium	Information Disclosure in com.fasterxml.jackson.core/jackson-databind			
Medium	Deserialization of Untrusted Data in com.fasterxml.jackson.core/jackson-databind			
org.apache.geode/geode-core 1.1.1	Java (Maven)	pom.xml		9 vulnerabilities detected
org.jgroups/jgroups 3.6.10.Final	Java (Maven)	pom.xml		1 vulnerability detected
commons-beanutils/commons-beanutils 1.8.3	Java (Maven)	pom.xml		2 vulnerabilities detected
io.netty/netty 3.9.1.Final	Java (Maven)	pom.xml		1 vulnerability detected
antlr/antlr 2.7.7	Java (Maven)	pom.xml		
com.fasterxml.jackson.core/jackson-annotations 2.9.0	Java (Maven)	pom.xml		
com.fasterxml.jackson.core/jackson-core 2.9.2	Java (Maven)	pom.xml		
com.github.stephenc.findbugs/findbugs-annotations 1.3.9-1	Java (Maven)	pom.xml		

Automatical Remediation



Alice, your application is secure!

Oh no!
However, I have a last attempt.
Bob, when is your Birthday?

Alice has to make security checks as a part of her daily life

Security is not a state, it’s a process

Security is a collective responsibility

DevSecOps

GitLab is constantly improving Security tools and brings new features every month.

Stay safe

Dziękuję bardzo.