



BÁO CÁO LAB 4

Môn: An toàn mạng máy tính nâng cao

GVTH: Đỗ Thị Phương Uyên

Sinh viên thực hiện	Sinh viên 1 MSSV: 21521182 Họ tên: Nguyễn Đại Nghĩa Sinh viên 2 MSSV: 21521295 Họ tên: Phạm Hoàng Phúc Sinh viên 3 MSSV: 21521848 Họ tên: Hoàng Gia Bảo Sinh viên 4 MSSV: 21521386 Họ tên: Lê Xuân Sơn
Lớp	NT534.O21.ATCL.1
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc (nếu là nhóm)	
Link Video thực hiện (nếu có yêu cầu)	



Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý...	
Điểm tự đánh giá (bắt buộc)	9 /10

BÁO CÁO CHI TIẾT

Tạo tài khoản Snyk

phamhoangphuc24092003 > Flow > Import

✓ GitHub successfully connected

Import and scan your first project

Import your code to see how Snyk surfaces issues, problematic dependencies, and vulnera

Choose from your most active repositories or [view all your repositories](#)

- ☒ hoangphuc2409/BaoMatWeb-FormValidation
- ☐ hoangphuc2409/WEBMUSSIC-main



Tạo tài khoản Github

Home

[Send feedback](#)

[Filter](#) 8

<> Start writing code

Start a new repository for hoangphuc2409

A repository contains all of your project's files, revision history, and collaborator discussion.

Repository name *

name your new repository...

☐ Public

Anyone on the internet can see this repository

☒ Private

You choose who can see and commit to this repository

Create a new repository

Introduce yourself with a profile README

Share information about yourself by creating a profile README, which appears at the top of your profile page.

hoangphuc2409 / README.md

Create

```
1 - 🙋 Hi, I'm @hoangphuc2409
2 - 👁 I'm interested in ...
3 - 📖 I'm currently learning ...
4 - 🤝 I'm looking to collaborate on ...
5 - 📧 How to reach me ...
6 - 🗨 Pronouns: ...
7 - ⚡ Fun fact: ...
8
```

Question: Dựa vào thông tin về các công cụ của Snyk, hãy dự đoán các công cụ này của Snyk hỗ trợ kiểm tra, đánh giá và khắc phục các vấn đề bảo mật ở những giai đoạn nào trong quá trình phát triển phần mềm?

Các công cụ của Snyk có thể hỗ trợ kiểm tra, đánh giá và khắc phục các vấn đề bảo mật ở các giai đoạn khác nhau trong quy trình phát triển phần mềm. Cụ thể:

+ Snyk Code (SAST) và Snyk Open Source (SCA) thường được sử dụng trong giai đoạn phát triển và kiểm thử. Chúng hỗ trợ trong việc kiểm tra mã nguồn và các gói phần mềm nguồn mở được sử dụng trong ứng dụng để phát hiện lỗ hổng bảo mật ngay từ giai đoạn phát triển.

+ Snyk Container được sử dụng trong giai đoạn triển khai và vận hành. Nó giúp kiểm tra và đánh giá bảo mật của các file Docker image hoặc các container trước khi triển khai chúng, nhằm đảm bảo an toàn và bảo mật trong môi trường triển khai.



+Snyk Infrastructure as Code thường được áp dụng trong giai đoạn thiết lập và quản lý cơ sở hạ tầng đám mây.

Fork repository từ đường dẫn <https://github.com/papicella/snyk-boot-web>


Create a new fork

A *fork* is a copy of a repository. Forking a repository allows you to freely experiment with changes without affecting the original project. [View existing forks.](#)

Required fields are marked with an asterisk ().*


Owner *

Repository name *

 hoangphuc2409

 /

snyk-boot-web


 snyk-boot-web is available.

By default, forks are named the same as their upstream repository. You can customize the name to distinguish it further.

Description (optional)

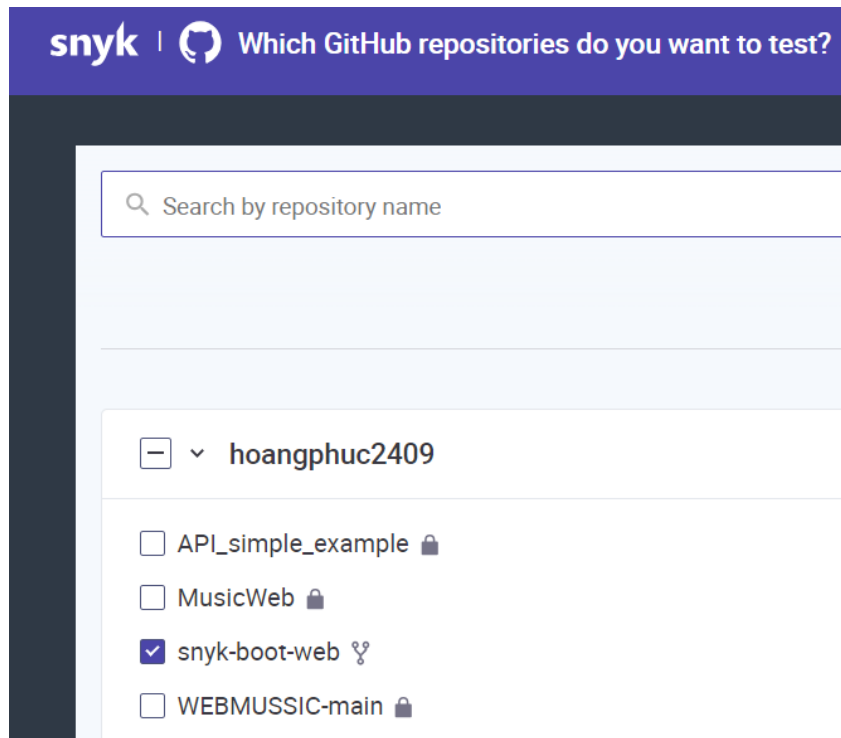
☒ Copy the master branch only

Contribute back to papicella/snyk-boot-web by adding your own branch. [Learn more.](#)

 You are creating a fork in your personal account.

Create fork

Đăng nhập tài khoản Snyk và chọn repository mà ta vừa fork về Github



Kiểm tra Snyk code và Snyk IaC đã enable hay chưa

Enable Snyk Code

To analyze your code for vulnerabilities we temporarily clone your repository. Cloned or uploaded code is cached for a maximum of 24h.

With the Snyk Free Plan, Snyk Code offers unlimited scans for public repositories.

☒ **Enabled**

After being enabled, you must import / re-import projects to Snyk Code.



ORGANIZATION SETTINGS

- General
- Integrations
- Languages
- Snyk Code
- Snyk IaC**
- Usage
- Your plan and billing
- Plans and pricing
- Licenses
- Notifications

? Snyk IaC

Your organization phamhoangphuc24092003 is using Current IaC. IaC+ — a new version of Snyk IaC — is currently in Early Access, and

Detect configuration files

Snyk can detect configuration files and report any misconfigurations

☒ Enabled

Các lỗi hỏng tìm được sau khi scan thành công

hoangphuc2409/snyk-boot-web				14	C	45	H	53	M	106	L
Project	Imported	Tested	Issues ↓								
<input type="checkbox"/> Dockerfile	6 minutes ago	6 minutes ago	11 C 23 H 19 M 80 L ...								
<input type="checkbox"/> pom.xml	6 minutes ago	6 minutes ago	3 C 21 H 24 M 6 L ...								
<input type="checkbox"/> Code analysis	6 minutes ago	6 minutes ago	0 C 1 H 1 M 0 L ...								
<input type="checkbox"/> kubernetes/snyk-boot-web-deployment-V1.yaml	6 minutes ago	6 minutes ago	0 C 0 H 3 M 5 L ...								
<input type="checkbox"/> argocd/snyk-boot-app-v1.yaml	6 minutes ago	6 minutes ago	0 C 0 H 3 M 5 L ...								
<input type="checkbox"/> argocd/snyk-iac-scan.yaml	6 minutes ago	6 minutes ago	0 C 0 H 3 M 4 L ...								
<input type="checkbox"/> terraform/main.tf	6 minutes ago	6 minutes ago	0 C 0 H 0 M 3 L ...								
<input type="checkbox"/> kubernetes/snyk-boot-web-deployment-V2.yaml	6 minutes ago	6 minutes ago	0 C 0 H 0 M 2 L ...								
<input type="checkbox"/> kubernetes/snyk-boot-web-deployment-wth-security-fixes.yaml	6 minutes ago	6 minutes ago	0 C 0 H 0 M 1 L ...								

Task: Quan sát và phân tích kết quả của việc scan trên các môi trường khác nhau: code application, container, IaC.



Code Application:

SNYK đã phát hiện một số lỗ hổng bảo mật trong mã nguồn của ứng dụng, bao gồm các phụ thuộc có chứa các phiên bản cũ không an toàn của thư viện.

The screenshot shows a code editor with a file named `pom.xml`. The editor has tabs for `Switch org`, `Overview`, `History`, and `Settings`. Below the tabs is a search bar and a list of dependencies. Each dependency row includes the dependency name, a table of security issues (C, H, M, L), and the number of paths affected.

DEPENDENCY	LATEST	LAST PUBLISHED	ISSUES	LICENSES	PATHS
ch.qos.logback.logback-classic@1.2.3			0 C 2 H 0 M 0 L		1
ch.qos.logback.logback-core@1.2.3			0 C 2 H 1 M 0 L		1
com.fasterxml.jackson.core:jackson-annotations@2.11.4			0 C 0 H 0 M 0 L		2
com.fasterxml.jackson.core:jackson-core@2.11.4			0 C 0 H 0 M 0 L		4
com.fasterxml.jackson.core:jackson-databind@2.11.4			0 C 4 H 12 M 0 L		4
com.fasterxml.jackson.datatype:jackson-datatype-jdk8@2.11.4			0 C 0 H 0 M 0 L		1
com.fasterxml.jackson.datatype:jackson-datatype-jsr310@2.11.4			0 C 0 H 0 M 0 L		1
com.fasterxml.jackson.module:jackson-module-parameter-names@2.11.4			0 C 0 H 0 M 0 L		1
com.h2database:h2@1.4.200			1 C 3 H 1 M 0 L		1
com.zaxxer:HikariCP@3.4.5			0 C 0 H 0 M 0 L		1

At the bottom of the table, there is a pagination bar with the following controls: `<<`, `<`, `1`, `2`, `3`, `4`, `>`, `>>`.



Snyk Vulnerability Database / Maven / ch.qos.logback:logback-classic

ch.qos.logback:logback-classic vulnerabilities

Direct Vulnerabilities

Known vulnerabilities in the ch.qos.logback:logback-classic package. This does not include vulnerabilities belonging to this package's dependencies.

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

VULNERABILITY	VULNERABLE VERSION
H Uncontrolled Resource Consumption ('Resource Exhaustion')	[1.2.13) [1.3.0,1.3.14) [1.4.0,1.4.14)
H Denial of Service (DoS)	[1.2.13) [1.3.0-alpha0,1.3.12) [1.4.0,1.4.12)
C Arbitrary Code Execution	[0.3,1.2.0)

Việc tích hợp SNYK vào quy trình CI/CD có thể phát hiện các vấn đề bảo mật ngay từ giai đoạn phát triển, giúp giảm thiểu rủi ro và chi phí sửa lỗi sau này.

Container:



Khi quét các image Docker, SNYK đã tìm thấy một số lỗ hổng bảo mật trong các phần mềm được cài đặt bên trong các container.

The screenshot shows the SNYK web interface for a Dockerfile scan. The top navigation bar includes the repository path 'GBaoZ/94 > Projects > GBaoZ/94/snyk-boot-web' and a link to 'Open on GitHub'. The main content area is titled 'Dockerfile' and includes tabs for 'Overview', 'History', and 'Settings'. A 'View docs' button is visible. Below the tabs, there are filters for 'Issues' (133) and 'Dependencies' (91). A search bar contains the text 'cve'. The left sidebar contains filters for 'SEVERITY' (Critical: 11, High: 23, Medium: 19, Low: 80), 'PRIORITY SCORE' (Scored between 0 - 1000), 'FIXED IN AVAILABLE' (Yes: 52, No: 81), 'COMPUTED FIXABILITY' (Fixable: 0, Partially fixable: 0, No supported fix: 133), and 'EXPLOIT MATURITY'. The main area displays a list of vulnerabilities. The first vulnerability is 'systemd/libudev1' with a score of 786, labeled as 'HIGH' and 'MATURE'. It includes details about the vulnerability (CVE-2023-26604), CVSS score (7.8), and the packages it affects. The second vulnerability is 'dpkg - Directory Traversal' with a score of 714, labeled as 'CRITICAL' and 'MATURE'. It includes details about the vulnerability (CVE-2022-1664), CVSS score (9.8), and the package it affects.

Infrastructure as Code (IaC):

SNYK đã phát hiện một số lỗ hổng bảo mật trong mã IaC, đặc biệt là trong các tệp cấu hình Terraform.



GBao294 > Projects > GBao294/snly-boot-web master

Open on GitHub

terraform/main.tf

Overview History Settings

SEVERITY

- High 0
- Medium 0
- Low 3

STATUS

- Open 3
- Ignored 0

3 of 3 issues

Sort by highest severity

S3 bucket versioning disabled

SNYK-CC-TF-124

```
6 resource "aws_s3_bucket" "s3_bucket_myapp" {
7   bucket = "myapp-prod"
8   acl = "private"
9 }
10
```

Detailed paths

- Introduced through: resource > aws_s3_bucket[s3_bucket_myapp] > versioning > enabled

Show more details

Ignore Full details

S3 server access logging is disabled

SNYK-CC-TF-45

```
6 resource "aws_s3_bucket" "s3_bucket_myapp" {
7   bucket = "myapp-prod"
8   acl = "private"
9 }
10
```

Detailed paths

- Introduced through: input > resource > aws_s3_bucket[s3_bucket_myapp] > logging

Show more details

Ignore Full details

S3 bucket MFA delete control disabled

SNYK-CC-TF-127

```
6 resource "aws_s3_bucket" "s3_bucket_myapp" {
7   bucket = "myapp-prod"
8   acl = "private"
9 }
```



GBao294 > Projects > GBao294/snyk-boot-web [master] [Open on GitHub](#)

terraform/main.tf

Overview History Settings

Created Mon 6th May 2024 | Snapshot taken by snyk.io 20 minutes ago | Retest now

IMPORTED BY
baohoanggia9@gmail.com

LIFECYCLE
Add a value

Issues 3

SEVERITY
☐ High 0
☐ Medium 0
☐ Low 3

STATUS
☒ Open 3
☐ Ignored 0

S3 bucket versioning disabled [SNYK-CC-TF-124](#)

```
1 provider "aws" {  
2   region = "eu-west-1"  
3   shared_credentials_file = "${HOME}/.aws/credentials"  
4 }  
5  
6 resource "aws_s3_bucket" "s3_bucket_myapp" {  
7   bucket = "myapp-prod"  
8   acl = "private"  
9 }  
10  
11 resource "aws_s3_bucket_object" "s3_bucket_object_myapp" {  
12   bucket = aws_s3_bucket.s3_bucket_myapp.id  
13   key = "beanstalk/myapp"  
14   source = "target/snyk-boot-web-0.0.1-SNAPSHOT.jar"  
15 }  
16  
17 resource "aws_elastic_beanstalk_application" "beanstalk_myapp" {  
18   name = "myapp"  
19   description = "Snyk Boot Web Application"  
20 }  
21  
22 resource "aws_elastic_beanstalk_application_version" "beanstalk_myapp_version" {
```

Detailed paths
Introduced through: resource: aws_s3_bucket[s3_bucket_myapp] › versioning › enabled
[Show more details](#)

BUSINESS CRITICALITY
Add a value

Sort by highest severity

Task: Dùng tính năng Snyk Pull Request để fix các lỗ hổng được tìm thấy

Mở file pom.xml để quan sát các lỗ hổng



▼ 9 hoangphuc2409/snyk-boot-web

☐ Dockerfile

☐ pom.xml

☐ Code analysis

☐ kubernetes/snyk-boot-web-deployment-V1.yaml

Chọn một lỗ hổng và nhấn Fix this vulnerability

hoangphuc2409/snyk-boot-web master

[Open on GitHub](#)

54
0
0

C org.apache.logging.log4j:log4j-core- Remote Code Execution (RCE) [🔗](#)

VULNERABILITY | ...

SCORE
879

Introduced through	org.apache.logging.log4j:log4j-core@2.15.0	Exploit maturity	MATURE
Fixed in	org.apache.logging.log4j:log4j-core@2.3.1, @2.12.2, @2.16.0		

Show more detail ▼

[Learn about this type of vulnerability](#)

Ignore Fix this vulnerability

Chọn lỗ hổng cần khắc phục



- ☐ **C** Remote Code Execution (RCE) in com.h2database:h2
- ☐ **M** Information Exposure in com.h2database:h2
- ☒ **C** Remote Code Execution (RCE) in org.apache.logging.log4j:log4j-core
- ☐ **M** Arbitrary Code Execution in org.apache.logging.log4j:log4j-core
- ☐ **M** Improper Input Validation in org.apache.tomcat.embed:tomcat-embed-core

Nhấn Open a Fix PR

Issues with no fix

No upgrade or patch is currently available for these issues:

- H** Remote Code Execution (RCE) in com.h2database:h2

Open a PR with upgrades and patches to address the selected issues.

Open a Fix PR

Khi này, một pull request sẽ được tạo ra



Conversation 0 Commits 1 Checks 0 Files changed 1

hoangphuc2409 commented 3 minutes ago Owner

This PR was automatically created by Snyk using the credentials of a real user.

Snyk has created this PR to fix one or more vulnerable packages in the `maven` dependencies of this project.

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
 - pom.xml

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Upgrade	Breaking Change	Exploit Maturity
C	879/1000 Why? Mature exploit, Has a fix available, CVSS 9	Remote Code Execution (RCE) SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2320014	<code>org.apache.logging.log4j:log4j-core:2.15.0 -> 2.16.0</code>	No	Mature

Sau khi xác nhận không có xung đột, tiến hành merge pull request

Add more commits by pushing to the `snyk-fix-f93b4f250aae56ad2ae93e7305015065` branch on `hoangphuc2409/snyk-boot-web`.

Require approval from specific reviewers before merging

[Rulesets](#) ensure specific people approve pull requests before they're merged.

Add rule

✓ All checks have passed

2 successful checks

Show all checks

✓ This branch has no conflicts with the base branch

Merging can be performed automatically.

Merge pull request

You can also [open this in GitHub Desktop](#) or view [command line instructions](#).



Merge pull request thành công



Pull request successfully merged and closed

You're all set—the `snyk-fix-f93b4f250...` branch can be safely deleted.

Delete branch

Kiểm tra lại file pom.xml, ta thấy số lượng cảnh báo đã giảm (3 critical -> 2 critical)

Targets 1

hoangphuc2409/snyk-boot-web

13C45H53M106L...

Project

Imported

Tested

Issues ↓

Dockerfile

28 minutes ago

28 minutes ago

11C23H19M80L...

Mpom.xml

28 minutes ago

a minute ago

2C21H24M6L...

Code analysis

28 minutes ago

28 minutes ago

0C1H1M0L...

Task: Cài đặt Snyk CLI, sử dụng các công cụ của Snyk để scan và xuất report thành file HTML

Cài đặt Snyk CLI

```
D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>npm install -g snyk
changed 38 packages in 26s

12 packages are looking for funding
  run `npm fund` for details
```

Ủy quyền cho Snyk CLI

```
D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>snyk auth
Now redirecting you to our auth page, go ahead and log in,
and once the auth is complete, return to this prompt and you'll
be ready to start using snyk.

If you can't wait use this url:
https://app.snyk.io/login?token=022451cd-5a8e-4e6c-b8c5-36eaea7f0ca1&utm_medium=cli&utm_source=cli&utm_campaign=CLI_V1_PLUGIN&utm_campaign_content=1.1291.0&os=windows_nt&docker=false

Your account has been authenticated. Snyk is now ready to be used.
```



snyk



Authenticated

Your account has been authenticated. Snyk is now ready to be used.

Clone nội dung Web app về máy

```
PS D:\Web and App development\Lab 4 DevSecOps> git clone https://github.com/papicella/snyk-boot-web
Cloning into 'snyk-boot-web'...
remote: Enumerating objects: 367, done.
remote: Counting objects: 100% (3/3), done.
```

Thực hiện scan với câu lệnh snyk test

```
D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>snyk test --all-projects
Testing D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web...
Organization:   hoangphuc2409
Package manager: npm
Target file:    package-lock.json
Project name:   package.json
Open source:    no
Project path:   D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web
Licenses:       enabled

[+] Tested D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web for known issues, no vulnerable paths found.

Next steps:
- Run 'snyk monitor' to be notified about new related vulnerabilities.
- Run 'snyk test' as part of your CI/test.

-----
Testing D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web...
Tested 40 dependencies for known issues, found 54 issues, 54 vulnerable paths.

Issues to fix by upgrading:

Upgrade com.h2database:h2@1.4.200 to com.h2database:h2@2.2.220 to fix
[+] Information Exposure [Medium Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-3146851] in com.h2database:h2@1.4.200
  introduced by com.h2database:h2@1.4.200
[+] Remote Code Execution (RCE) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-2331071] in com.h2database:h2@1.4.200
  introduced by com.h2database:h2@1.4.200
[+] XML External Entity (XXE) Injection [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-1769238] in com.h2database:h2@1.4.200
  introduced by com.h2database:h2@1.4.200
[+] Remote Code Execution (RCE) [Critical Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-2348247] in com.h2database:h2@1.4.200
  introduced by com.h2database:h2@1.4.200

Upgrade org.apache.logging.log4j:log4j-core@2.15.0 to org.apache.logging.log4j:log4j-core@2.17.1 to fix
[+] Arbitrary Code Execution [Medium Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2327339] in org.apache.logging.log4j:log4j-core@2.15.0
  introduced by org.apache.logging.log4j:log4j-core@2.15.0
[+] Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2321524] in org.apache.logging.log4j:log4j-core@2.15.0
  introduced by org.apache.logging.log4j:log4j-core@2.15.0
[+] Remote Code Execution (RCE) [Critical Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2328014] in org.apache.logging.log4j:log4j-core@2.15.0
  introduced by org.apache.logging.log4j:log4j-core@2.15.0

Upgrade org.springframework.boot:spring-boot-actuator@2.3.10.RELEASE to org.springframework.boot:spring-boot-actuator@2.7.18 to fix
[+] Improper Handling of Case Sensitivity [Low Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-2689634] in org.springframework:spring-context@5.2.14.RELEASE
  introduced by org.springframework.boot:spring-boot-actuator@2.3.10.RELEASE > org.springframework.boot:spring-boot@2.3.10.RELEASE > org.springframework:spring-context@5.2.14.RELEASE
[+] Denial of Service (DoS) [Medium Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORKBOOT-6226862] in org.springframework.boot:spring-boot-actuator@2.3.10.RELEASE
```




```
SE > ch.qos.logback:logback-classic@1.2.3 > ch.qos.logback:logback-core@1.2.3
  [Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-CHQOSLOGBACK-6094942] in ch.qos.logback:logback-classic@
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter@2.3.10.RELEASE
SE > ch.qos.logback:logback-classic@1.2.3
  [Uncontrolled Resource Consumption ('Resource Exhaustion') [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-CHQOSLOGBACK-6097492]
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter@2.3.10.RELEASE
SE > ch.qos.logback:logback-classic@1.2.3
  [Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGYAML-2806360] in org.yaml:snakeyaml@1.26
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter@2.3.10.RELEASE
  [Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGYAML-6056527] in org.yaml:snakeyaml@1.26
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter@2.3.10.RELEASE
  [Improper Input Validation [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-6092281] in org.apache.tomcat.embed
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter-tomcat@2.3.10.RELEASE
  [Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-5953331] in org.apache.tomcat.embed
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter-tomcat@2.3.10.RELEASE
  [Improper Input Validation [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-3225086] in org.apache.tomcat.embed
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter-tomcat@2.3.10.RELEASE
  [Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORKBOOT-5564390] in org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter@2.3.10.RELEASE
  [Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMFASTERXMLJACKSONCORE-2421244] in com.fasterxml.jackson.core:jackson-core@2.3.10.RELEASE
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter-json@2.3.10.RELEASE
  [Privilege Escalation [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHETOMCATEMBED-2414084] in org.apache.tomcat.embed:tomcat-embed-core@2.3.10.RELEASE
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter-tomcat@2.3.10.RELEASE
  [Improper Input Validation [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGGLASSFISH-1297098] in org.glassfish:jakarta.ee@3.0.1
introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE > org.springframework.boot:spring-boot-starter-tomcat@2.3.10.RELEASE
  [Remote Code Execution [Critical Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORK-2436751] in org.springframework:spring-web@5.2.14.RELEASE > org.springframework:spring-web@5.2.14.RELEASE > org.springframework:spring-web@5.2.14.RELEASE

Issues with no direct upgrade or patch:
  [Remote Code Execution (RCE) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-31685] in com.h2database:h2@1.4.200
introduced by com.h2database:h2@1.4.200
No upgrade or patch available

Organization:    hoangphuc2409
Package manager: maven
Target file:    pom.xml
Project name:    com.example:snyk-boot-web
Open source:    no
Project path:    D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web
Licenses:       enabled

Tested 2 projects, 1 contained vulnerable paths.
```

Sử dụng Snyk Code để scan mã nguồn



```
D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>snyk code test

Testing D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web ...

[Medium] Use of Hardcoded Credentials
Path: src/main/java/com/example/snykbootweb/DatabaseService.java, line 8
Info: Do not hardcode passwords in code. Found hardcoded password used in here.

[High] SQL Injection
Path: src/main/java/com/example/snykbootweb/jdbc/CustomRest.java, line 29
Info: Unsanitized input from the request URL flows into query, where it is used in an SQL query. This may result in an SQL Injection vulnerability.

Test completed

Organization:   hoangphuc2409
Test type:     Static code analysis
Project path:  D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web

Summary:

2 Code issues found
1 [High]  1 [Medium]

D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>
```

Cài đặt plugin để xuất file html

```
D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>npm install snyk-to-html -g

added 23 packages in 4s

1 package is looking for funding
  run `npm fund` for details

D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>snyk test --json | snyk-to-html -o results.html
Vulnerability snapshot saved at results.html

D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>snyk test --all-projects --json | snyk-to-html -o results.html
Vulnerability snapshot saved at results.html

D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web>
```

Kết quả

	.dccache	5/4/2024 11:45 AM	DCCACHE File	2 KB
	.deepsource	5/4/2024 11:18 AM	Toml Source File	1 KB
	build-container	5/4/2024 11:18 AM	Shell Script	1 KB
	Dockerfile	5/4/2024 11:18 AM	File	1 KB
	package	5/4/2024 11:21 AM	JSON Source File	1 KB
	package-lock	5/4/2024 11:21 AM	JSON Source File	1 KB
	pom	5/4/2024 11:18 AM	Microsoft Edge HT...	3 KB
	README	5/4/2024 11:18 AM	Markdown Source ...	3 KB
	results	5/4/2024 11:49 AM	Chrome HTML Do...	258 KB



File D:/Web%20and%20App%20development/Lab%204%20DevSecOps/snyk-boot-web/results.html

Th... Paraphrasing Tool... Search results for E... YouTube Free Vectors, Stock... Bộ sưu tập - Sandra... Welcome to Cloud... ChatGPT - Poe Dashboard | Hacker...

snyk

Snyk test report

May 4th 2024, 4:49:21 am (UTC+00:00)

Scanned the following paths:

- D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web\package-lock.json (npm)
- D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web\pom.xml (maven)

54 known vulnerabilities | 54 vulnerable dependency paths | 40 dependencies

CRITICAL SEVERITY

Remote Code Execution

- Manifest file: D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web > pom.xml
- Package Manager: maven
- Vulnerable module: org.springframework:spring-beans
- Introduced through: com.example:snyk-boot-web@0.0.1-SNAPSHOT, org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE and others

Task: Cài đặt Snyk plugin/extension vào IDE đang sử dụng và quan sát kết quả scan

Cài đặt Snyk extension trên VScode

EXTENSIONS: MARKETPLACE

Snyk

Snyk Security
Easily find and fix vulnerabilities in your code, open so...
Snyk

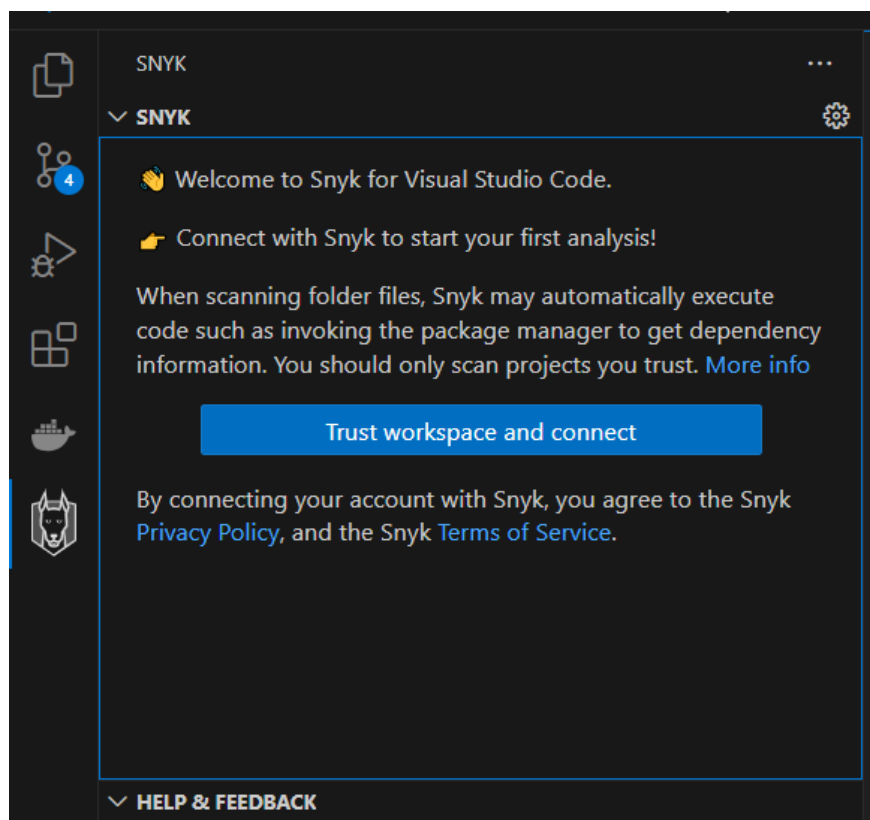
(Preview) Snyk Security
This is a preview release for functionality that is not yet...
Snyk

Extension: Snyk Security

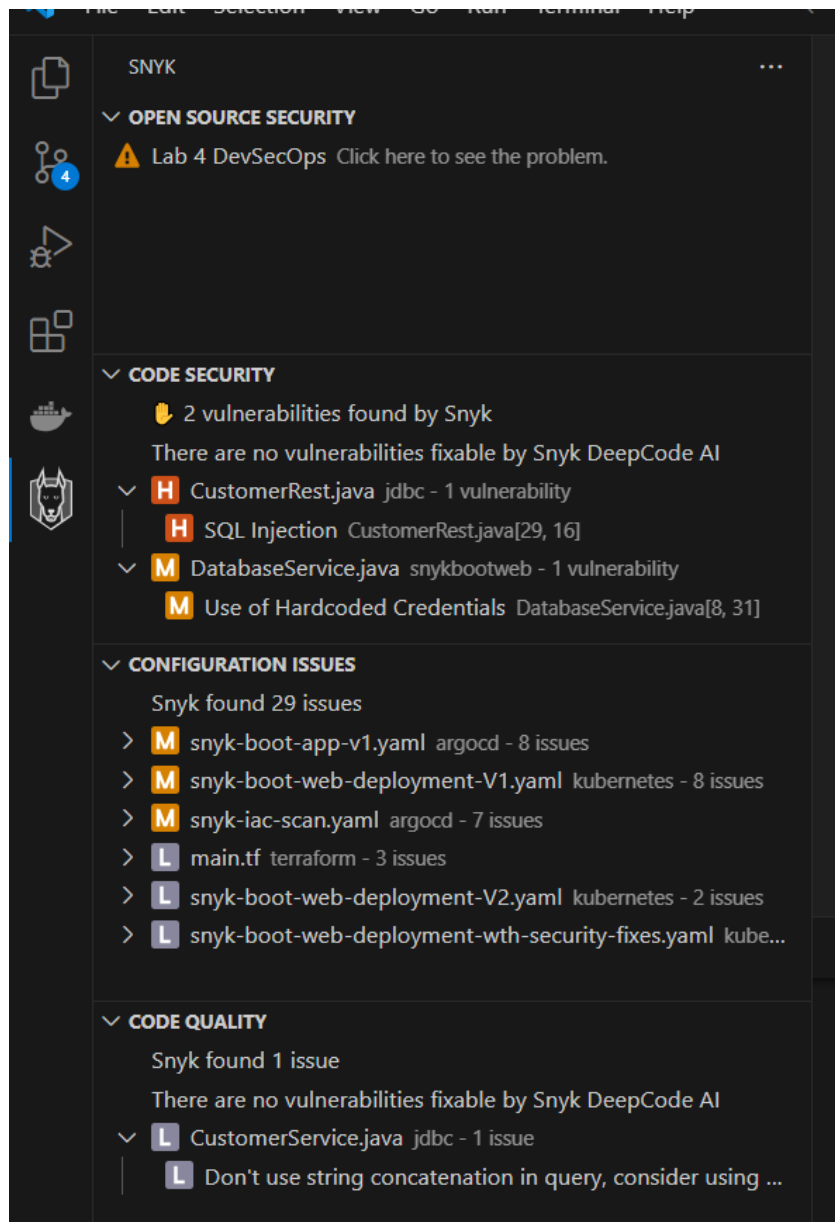
Snyk Security v2.6.1
Snyk snyk.io | 183,129 | ★★★★★ (29)
Easily find and fix vulnerabilities in your code, open so...
Disable Uninstall
This extension is enabled globally.

DETAILS FEATURES CHANGELOG

Chọn Trust workspace and connect



Kết quả sau khi scan



Bonus: Tạo một pre-commit hook gọi Snyk CLI để scan repository
Vào mục `.git/hooks` và tạo file `pre-commit.sh`



```
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> code .git/hooks
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> code .git/hooks
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> code .git/hooks/pre-commit
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> 
```

Nội dung file pre-commit

```
→ Lab 4 DevSecOps
pre-commit x
snyk-boot-web > .git > hooks > pre-commit
1  #!/usr/bin/env bash
2
3  RED='\033[1;31m' # Bold red
4  NC='\033[0m' # No Color
5
6  # Snyk command examples
7  #snyk test --severity-threshold=high
8  #snyk iac test --severity-threshold=high
9  #snyk code test --severity-threshold=high
10
11 if ! [ -x "$(command -v snyk)" ]
12 then
13     echo -e "${RED}Snyk could not be found. Please make sure Snyk is installed properly.\nDocumentation can be found
14     exit 1
15 fi
16
17 snyk test --all-projects --severity-threshold=high
18 snyk code test --severity-threshold=high
```

Kết quả

```
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> git init
Reinitialized existing Git repository in D:/Web and App development/Lab 4 DevSecOps/snyk-boot-web/.git/
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> git add .
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> git commit -m "test pre-commit hook Snyk CLI"

Testing D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web...

Organization:    hoangphuc2409
Package manager: npm
Target file:     package-lock.json
```



```
✓ Tested D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web for known issues, no vulnerable paths found.
```

```
Next steps:
```

- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.

```
-----  
Testing D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web...
```

```
Tested 40 dependencies for known issues, found 24 issues, 24 vulnerable paths.
```

```
Issues to fix by upgrading:
```

```
Upgrade com.h2database:h2@1.4.200 to com.h2database:h2@2.1.210 to fix  
X Remote Code Execution (RCE) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-com.h2database:h2@1.4.200  
introduced by com.h2database:h2@1.4.200  
X XML External Entity (XXE) Injection [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-com.h2database:h2@1.4.200  
introduced by com.h2database:h2@1.4.200  
X Remote Code Execution (RCE) [Critical Severity][https://security.snyk.io/vuln/SNYK-JAVA-com.h2database:h2@1.4.200
```

```
✓ Test completed
```

```
Organization:    hoangphuc2409  
Test type:       Static code analysis  
Project path:    D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web
```

```
Summary:
```

```
1 Code issues found  
1 [High]
```

```
PS D:\Web and App development\Lab 4 DevSecOps\snyk-boot-web> █
```



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM

KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

BỘ MÔN AN TOÀN THÔNG TIN



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM

KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

BỘ MÔN AN TOÀN THÔNG TIN