

# BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng máy tính nâng cao

Lab 4: Security with Snyk in DevSecOps

GVHD: Đỗ Thị Phương Uyên

**1. THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT534.O21.ATTN

STT	Họ và tên	MSSV	Email
1	Hà Thị Thu Hiền	21522056	21522056@gm.uit.edu.vn

**2. NỘI DUNG THỰC HIỆN:<sup>1</sup>**

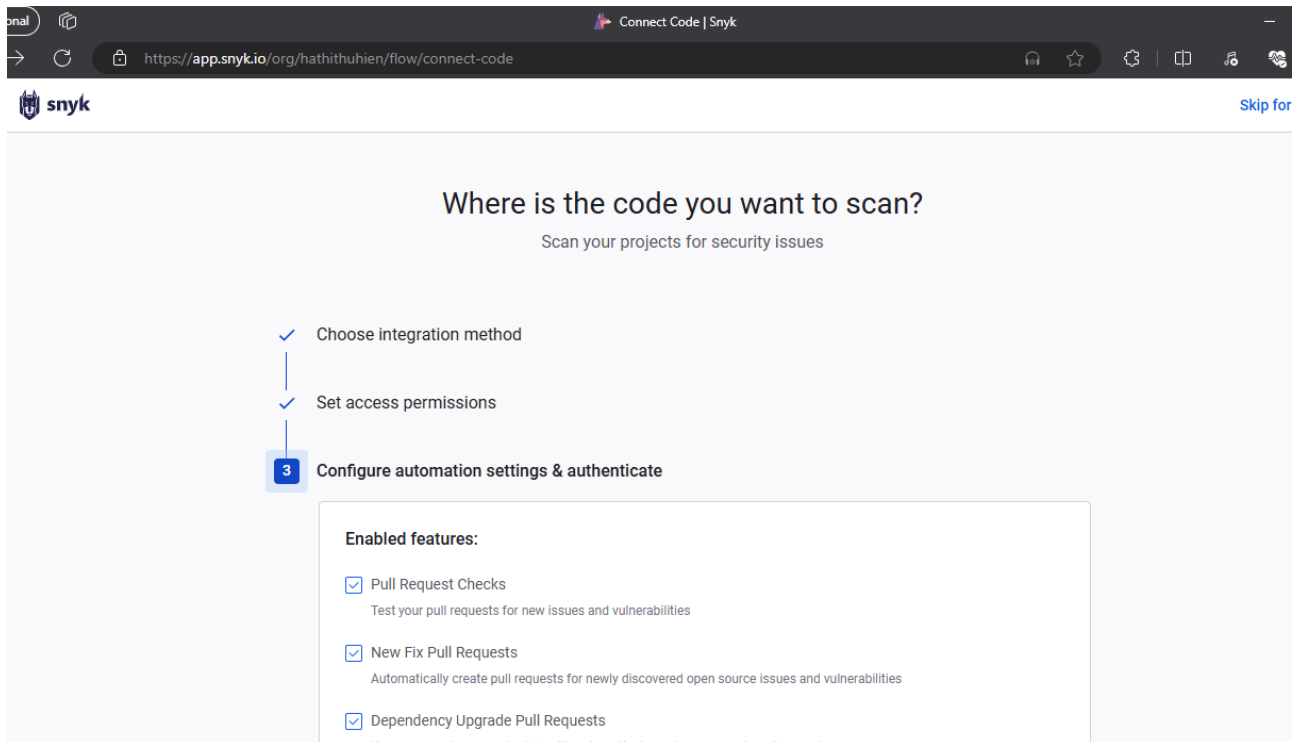
STT	Công việc	Kết quả tự đánh giá
1	Tất cả các bài tập	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

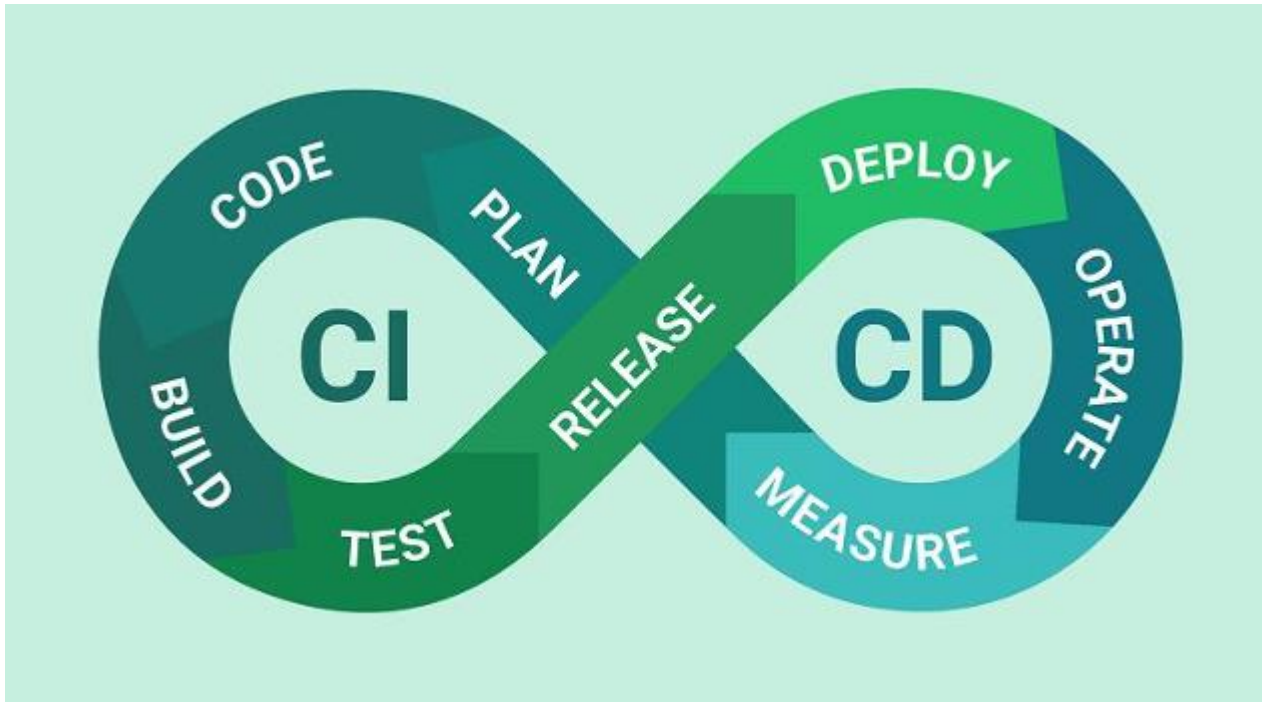
<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## 1. Task: Tạo tài khoản Snyk và GitHub



## 2. 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?

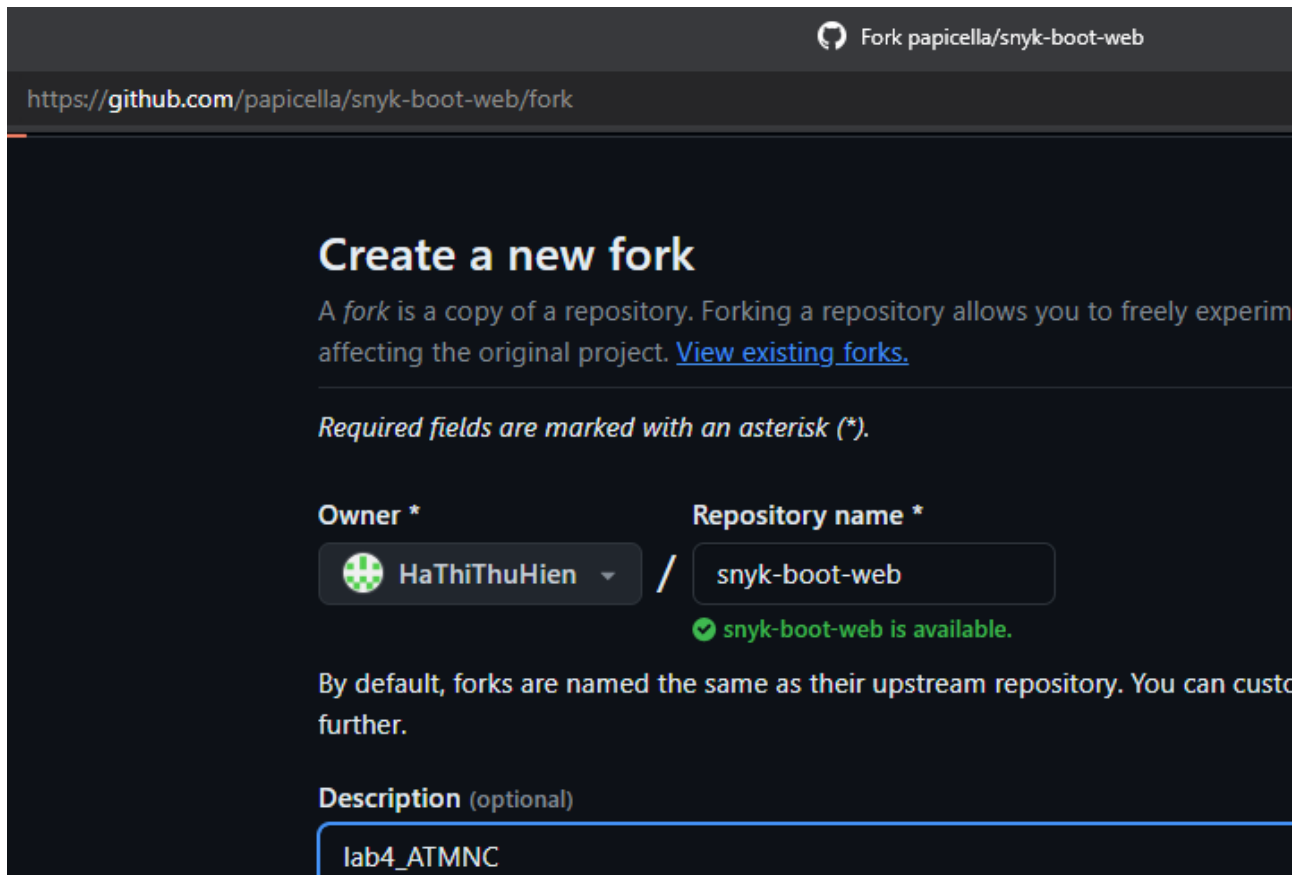


Dựa vào thông tin về các công cụ của Snyk, ta có thể dự đoán các công cụ này hỗ trợ kiểm tra, đánh giá và khắc phục các vấn đề bảo mật ở các giai đoạn sau trong quá trình phát triển phần mềm:

1. **Snyk Code (SAST) và Snyk Open Source (SCA):** Các công cụ này hỗ trợ kiểm tra mã nguồn và các gói phần mềm mã nguồn mở của bên thứ ba. Chúng có thể được sử dụng trong **giai đoạn phát triển và kiểm thử** để phát hiện các lỗ hổng bảo mật ngay từ khi mã nguồn được viết ra và sử dụng các gói phần mềm.
2. **Snyk Container:** Công cụ này tập trung vào kiểm tra cấu hình của các hình ảnh container và các lỗ hổng trên nền tảng Linux. Nó hỗ trợ phát hiện các lỗ hổng bảo mật trong **quá trình triển khai ứng dụng** thông qua containerization.
3. **Snyk Infrastructure as Code:** Công cụ này cung cấp đánh giá cho các cấu hình cơ sở hạ tầng đám mây. Nó có thể được sử dụng trong **giai đoạn triển khai và quản lý hạ tầng** để phát hiện và khắc phục các lỗ hổng bảo mật liên quan đến cấu hình hạ tầng.

Tóm lại, các công cụ của Snyk có thể hỗ trợ kiểm tra, đánh giá và khắc phục các vấn đề bảo mật ở cả giai đoạn phát triển và triển khai phần mềm, từ việc phát hiện lỗ hổng từ mã nguồn đến cấu hình hạ tầng đám mây.

#### a. Fork sample webapp vào GitHub repository




Fork papicella/snyk-boot-web

<https://github.com/papicella/snyk-boot-web/fork>

## Create a new fork

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

*Required fields are marked with an asterisk (\*).*

**Owner \***  HaThiThuHien

**Repository name \*** snyk-boot-web

✓ snyk-boot-web is available.

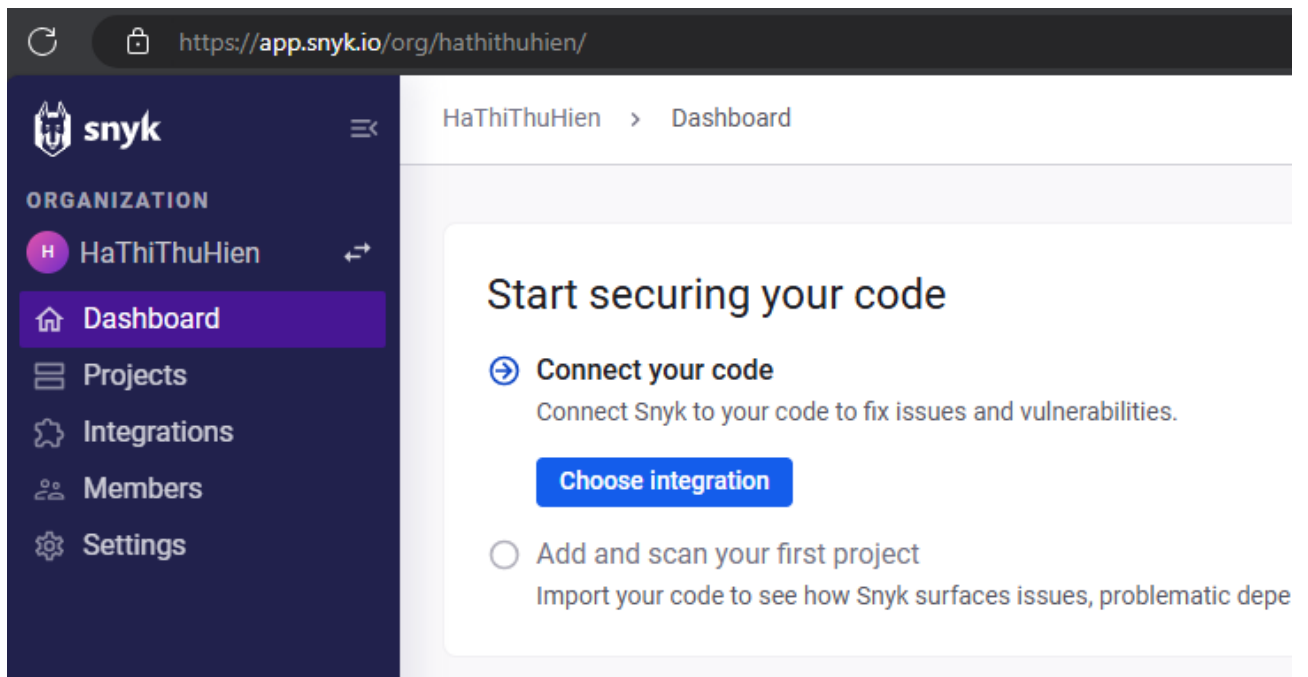
By default, forks are named the same as their upstream repository. You can customize the name further.

**Description (optional)**

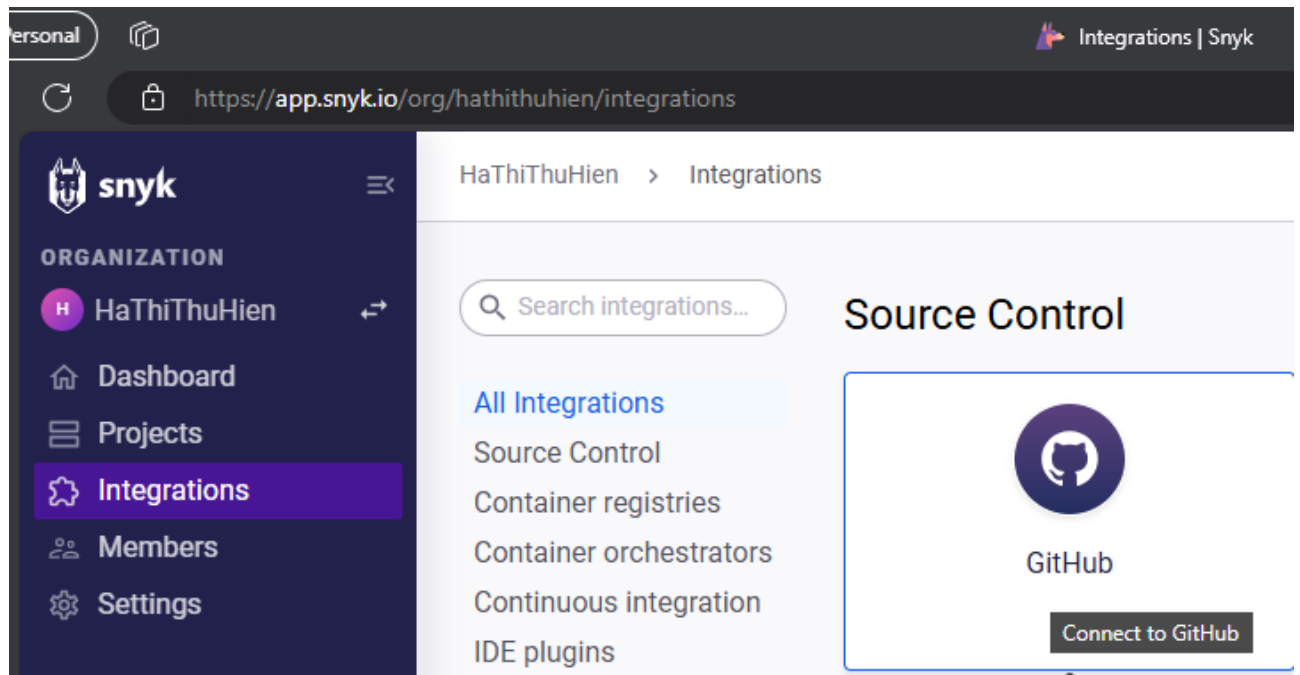
lab4\_ATMNC

### b. Cấu hình GitHub Intergration

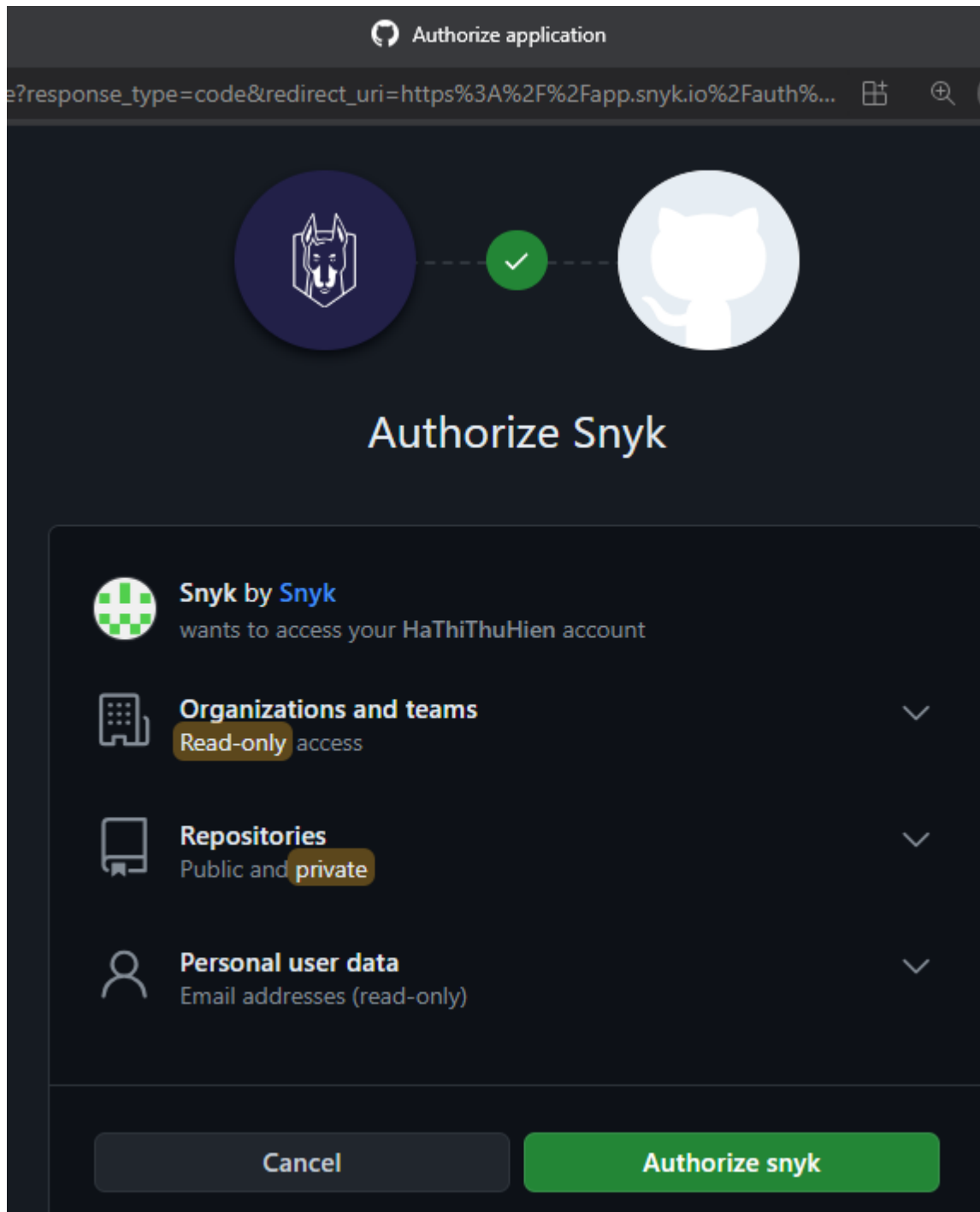
- Đăng nhập vào <http://app.snyk.io>

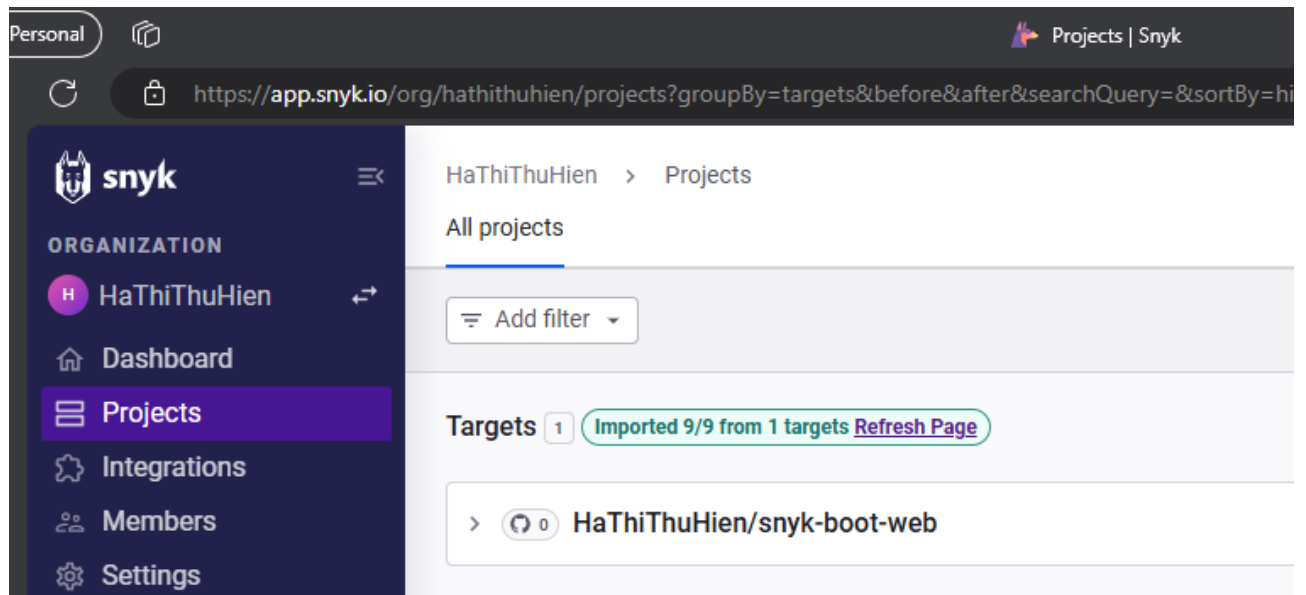


- Tại trang chủ, chọn Integrations → Source Control → GitHub



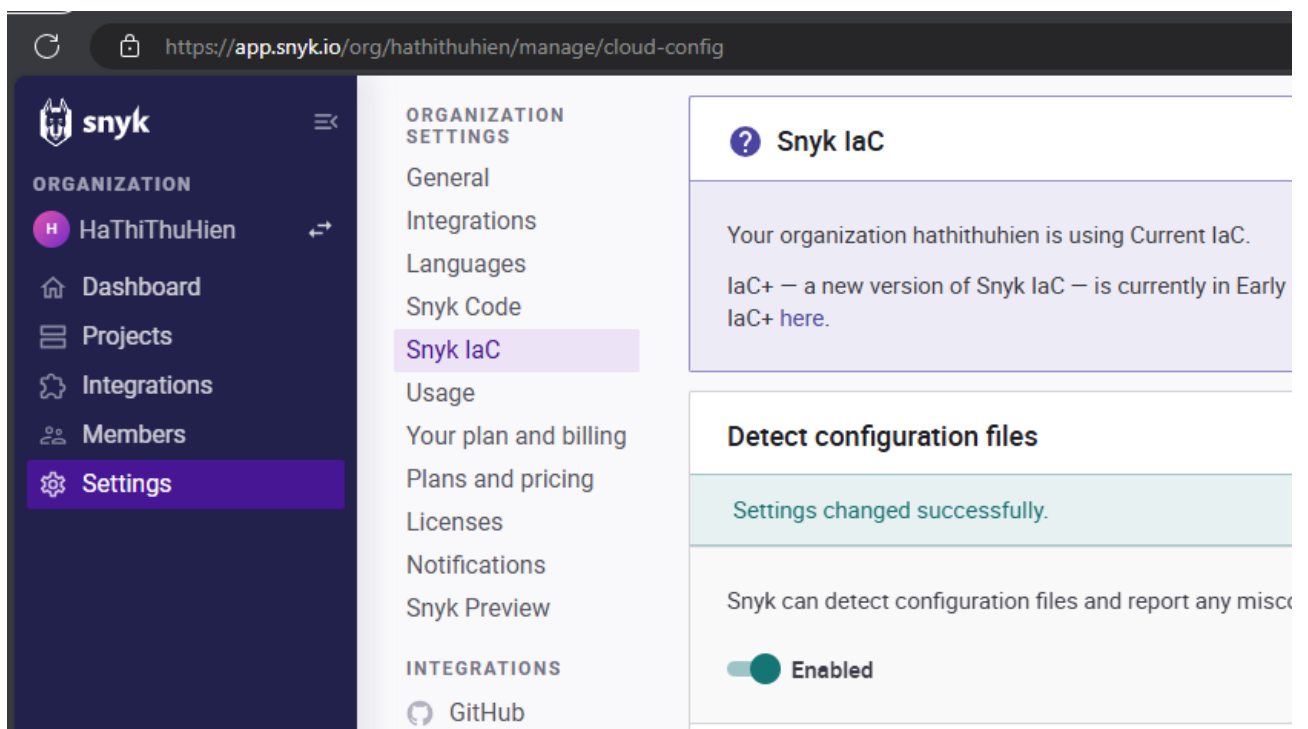
- Điền các thông tin kết nối github và Snyk





### c. Import Repository và enable Snyk Code

- Snyk đã được kết nối với GitHub account.
- Tiếp theo, chúng ta sẽ tiến hành enable Snyk Code và import Repository vào Snyk.
  - o Kiểm tra Snyk Code đã được enable chưa bằng cách truy cập vào Settings → Snyk Code. Tiến hành Enable và lưu các thay đổi.
  - o Thực hiện tương tự với Snyk IaC



- Chọn Project → Add project → GitHub

- Chọn Repo đã được fork ở bước trước và chọn Add selected repositories.

#### d. Phân tích kết quả của Snyk

- Sau khi tiến hành scan, Snyk trả về kết quả các lỗ hổng, mỗi đe dọa được tìm thấy

HaThiThuHien/snyk-boot-web				14	C	45	H	53	M	106	L	...
Project	Imported	Tested	Issues ↓									
<input type="checkbox"/> Dockerfile	10 minutes ago	10 minutes ago	11 C 23 H 19 M 80 L									...
<input checked="" type="checkbox"/> pom.xml	10 minutes ago	10 minutes ago	3 C 21 H 24 M 6 L									...
<input type="checkbox"/> Code analysis	10 minutes ago	10 minutes ago	0 C 1 H 1 M 0 L									...
<input type="checkbox"/> argocd/snyk-boot-app-v1.yaml	10 minutes ago	10 minutes ago	0 C 0 H 3 M 5 L									...
<input type="checkbox"/> kubernetes/snyk-boot-web-deployment-V1.yaml	10 minutes ago	10 minutes ago	0 C 0 H 3 M 5 L									...
<input type="checkbox"/> argocd/snyk-iac-scan.yaml	10 minutes ago	10 minutes ago	0 C 0 H 3 M 4 L									...
<input type="checkbox"/> terraform/main.tf	10 minutes ago	10 minutes ago	0 C 0 H 0 M 3 L									...
<input type="checkbox"/> kubernetes/snyk-boot-web-deployment-V2.yaml	10 minutes ago	10 minutes ago	0 C 0 H 0 M 2 L									...
<input type="checkbox"/> kubernetes/snyk-boot-web-deployment-wth-security-fixes.yaml	10 minutes ago	10 minutes ago	0 C 0 H 0 M 1 L									...

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

Dựa trên kết quả của quá trình quét trên các môi trường khác nhau như mã nguồn ứng dụng, container và cấu hình cơ sở hạ tầng như Infrastructure as Code (IaC), chúng ta có thể rút ra một số nhận định sau:

#### a) Mã nguồn ứng dụng (Code analysis):

- Đầu tiên, ta có thể nhận thấy rằng code analysis phát hiện 1 lỗ hổng High và 1 lỗ hổng medium, click vào để xem rõ hơn.
- Đầu tiên, các lỗ hổng sẽ được hiển thị một cách ngắn gọn, lỗ hổng sẽ được sắp xếp theo priority score, thuộc CWE nào, vulnerability types, và dưới các lỗ hổng sẽ có các lời cảnh báo về việc code không được an toàn.



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

Code Analysis

Overview
History
Settings

SEVERITY

High

1

Medium

1

Low

0

PRIORITY SCORE

Scored between 0 - 1000

STATUS

Open

2

Ignored

0

LANGUAGES

Java

2

2 of 2 issues

Group by none Sort by highest severity

H

SQL Injection

SNYK CODE | CWE-89

SCORE 800

25

26

27

28

29

}

@GetMapping(produces = "application/json", path = "/all/{lastName}")

public List<Customer> getAllCustomersByLastName(@PathVariable String lastName) {

return customerService.getAllByLastName(lastName);

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.

[src/main/java/com/example/snykbootweb/jdbc/CustomerRest.java](#)
7 steps in 2 files

[Learn about this type of vulnerability and how to fix it](#)

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

Code Analysis

Overview
History
Settings

VULNERABILITY TYPES

Use of Hardcoded Credentials

1

SQL Injection

1

M

Use of Hardcoded Credentials

SNYK CODE | CWE-798 + 1 MORE

SCORE 550

5

6

7

8

@Service

public class DatabaseService {

private String userName = "admin";

private String password = "shwhehe67whd!";

Do not hardcode passwords in code. Found hardcoded password used in here.

[src/main/java/com/example/snykbootweb/DatabaseService.java](#)
1 step in 1 file

- Khi click vào detail thì ta có thể thấy rõ hơn về data flow của lỗ hổng và các fix chúng để tránh khỏi các cuộc tấn công, hiểu rõ được các cuộc tấn công diễn ra như thế nào và cách chống lại chúng.

HaThiThuHien > [Projects](#) > [HaThiThuHien/snyk-boot-web](#) master

[Open on GitHub](#)

## Code Analysis

Overview History Settings

### SQL Injection

SNYK CODE | [CWE-89](#)

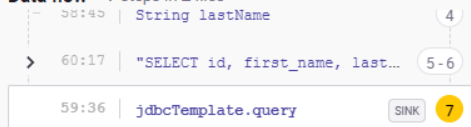
Data flow

Fix analysis

X

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.

Data flow - 7 steps in 2 files



Find out how to remediate this issue through our [Fix analysis](#)

[src/main/java/com/example/snykbootweb/jdbc/CustomerService.java](#)

```

53
54     return customers;
55
56 }
57
58 public List<Customer> getAllByLastName (String lastName) {
59     List<Customer> customers = jdbcTemplate.query(
60         "SELECT id, first_name, last_name FROM customers WHERE
61         (rs, rowNum) -> new Customer((int) rs.getLong("id"),
62         rs.getString("first_
63         rs.getString("last_
64
65     return customers;
  
```

[Ignore](#)

HaThiThuHien > [Projects](#) > [HaThiThuHien/snyk-boot-web](#) master

[Open on GitHub](#)

## Code Analysis

Overview History Settings

### SQL Injection

SNYK CODE | [CWE-89](#)

Data flow

Fix analysis

X

In an SQL injection attack, the user can submit an SQL query directly to the database, gaining access without providing appropriate credentials. Attackers can then view, export, modify, and delete confidential information; change passwords and other authentication information; and possibly gain access to other systems within the network. This is one of the most commonly exploited categories of vulnerability, but can largely be avoided through good coding practices.

#### Best practices for prevention

- Avoid passing user-entered parameters directly to the SQL server.
- Avoid using string concatenation to build SQL queries from user-entered

[apache/incubator-brooklyn](#)

```

50 stmt.execute("INSERT INTO MESSAGES valu
50 stmt.execute("INSERT INTO MESSAGES valu
51
52 //better escaping and security
53
54 //this essentially does StringE
55
56 request.getParameter("name").re
57
58 ", "+
59
60 request.getParameter("message")
61
62 ", "+request.getParameter("me
63 ");
  
```

[Ignore](#)

## b) Container (Dockerfile):

- Nhìn qua thì ta thấy lỗi hổng ở Dockerfile khá nhiều.

[Dockerfile](#)

an hour ago

an hour ago

11 C 23 H 19 M 80 L

- Bao gồm các lỗi hổng ở mức độ: 11 Critical, 23 High, 19 Medium, 80 Low.

- Click vào để xem trong Dockerfile có gì

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

### Dockerfile

Overview History Settings

	BASE IMAGE	VULNERABILITIES	SEVERITY	
<b>Current image</b>	openjdk:11.0.13-slim-buster	133	11 C 23 H 19 M 80 L	
<b>Minor upgrades</b>	openjdk:11.0.14.1-slim-buster	129	11 C 20 H 18 M 80 L	<a href="#">Open a fix PR</a>
<b>Major upgrades</b>	openjdk:21-slim-buster	93	2 C 6 H 7 M 78 L	<a href="#">Open a fix PR</a>
<b>Alternative upgrades</b>	openjdk:23-ea-18-jdk-oraclelinux8	18	0 C 9 H 9 M 0 L	<a href="#">Open a fix PR</a>
	openjdk:23-ea-17-jdk-oraclelinux8	20	0 C 9 H 11 M 0 L	<a href="#">Open a fix PR</a>
	openjdk:23-ea-16-jdk-oraclelinux8	27	0 C 9 H 18 M 0 L	<a href="#">Open a fix PR</a>
	openjdk:23-ea-15-jdk-oraclelinux8	27	0 C 9 H 18 M 0 L	<a href="#">Open a fix PR</a>

- Ta thấy tools phân tích các lỗ hổng ở các base image với current image và các phiên bản upgrades, bên cạnh đó ta có thể thấy phần Open a fix PR thì nó sẽ hiển thị như sau:

Personal [\[Snyk\] Security upgrade openjdk from 11.0.13-slim-buster to 11.0.14.1-slim-buster by HaThiThuHien · Pull Request #1 · HaThiThuHien/snyk-boot-web](#)

[https://github.com/HaThiThuHien/snyk-boot-web/pull/1](#)

HaThiThuHien / **snyk-boot-web**

<> Code **Pull requests 1** Actions Projects Wiki Security Insights Settings

### [Snyk] Security upgrade openjdk from 11.0.13-slim-buster to 11.0.14.1-slim-buster #1

[Open](#) HaThiThuHien wants to merge 1 commit into `master` from `snyk-fix-986e00e08dd5ae3c3d7be89296b73c57`

Conversation 0 Commits 1 Checks 0 Files changed 1

**HaThiThuHien** commented 3 minutes ago Owner

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

Keeping your Docker base image up-to-date means you'll benefit from security fixes in the latest version of your chosen image.

**Changes included in this PR**

- Dockerfile

**Reviewers**

No reviews

Still in progress? [Convert to draft](#)

**Assignees**

No one—[assign yourself](#)

**Labels**

None yet

hal [Snyk] Security upgrade openjdk from 11.0.13-slim-buster to 11.0.14.1-slim-buster by HaThiThuHien · Pull Request #1 · HaThiT

https://github.com/HaThiThuHien/snyk-boot-web/pull/1

**Open** [Snyk] Security upgrade openjdk from 11.0.13-slim-buster to 11.0.14.1-slim-buster #1  
HaThiThuHien wants to merge 1 commit into `master` from `snyk-fix-986e00e08dd5ae3c...`

Some of the most important vulnerabilities in your base image include:

Severity	Priority Score / 1000	Issue	Exploit Maturity
C	714	Use After Free <a href="#">SNYK-DEBIAN10-GLIBC-1296899</a>	No Known Exploit
C	714	Integer Overflow or Wraparound <a href="#">SNYK-DEBIAN10-GLIBC-1315333</a>	No Known Exploit
C	714	Off-by-one Error <a href="#">SNYK-DEBIAN10-LIBTASN16-3061094</a>	No Known Exploit
H	786	<a href="#">CVE-2023-26604</a> <a href="#">SNYK-DEBIAN10-SYSTEMD-3339153</a>	Mature
H	786	<a href="#">CVE-2023-26604</a> <a href="#">SNYK-DEBIAN10-SYSTEMD-3339153</a>	Mature

**Note:** You are seeing this because you or someone else with access to this repository has authorized Snyk to open fix PRs.

- Click vào Issue ta sẽ thấy [Snyk Vulnerability Database](#) , xem được những rủi ro, cảnh báo và cách fix

Personal Use After Free in glibc | CVE-2021-33574 | Snyk

https://security.snyk.io/vuln/SNYK-DEBIAN10-GLIBC-1296899

**snyk** | SECURITY Developer Tools About Snyk

Snyk Vulnerability Database > Linux > debian > debian:10 > glibc

**Use After Free**  
Affecting `glibc` package, versions <2.28-10+deb10u2

INTRODUCED: 26 MAY 2021 CVE-2021-33574 CWE-416

**How to fix?**  
Upgrade `Debian:10 glibc` to version 2.28-10+deb10u2 or higher.

**NVD Description**  
Note: Versions mentioned in the description apply only to the upstream `glibc` package and not the `glibc` package as distributed by `Debian`. See [How to fix?](#) for `Debian:10` relevant fixed versions and status.

**Snyk CVSS**

Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

**9.8**  
CRITICAL

- Lướt xuống dưới phần Dockerfile thì cũng sẽ thấy các vấn đề cụ thể được liệt kê ra:

The screenshot shows the Snyk interface for a Dockerfile. The top navigation bar includes 'HaThiThuHien', 'Projects', and 'HaThiThuHien/snyk-boot-web' with a 'master' branch selector. The 'Dockerfile' section is active, with tabs for 'Overview', 'History', and 'Settings'. The 'Issues' tab is selected, showing 133 issues. A sidebar on the left allows filtering by severity (Critical: 11, High: 23, Medium: 19, Low: 80) and priority score (0-1000). A search bar is at the top right. A notification banner at the top right suggests reducing the backlog of vulnerabilities using prioritized fix pull requests. The main content area displays a list of vulnerabilities, with the first one being 'systemd/libudev1 - CVE-2023-26604' with a score of 786. Below this, a detailed view of the vulnerability is shown, including its introduction through 'systemd/libudev1@241-7~deb10u8' and 'systemd/libsystemd0@241-7~deb10u8', its fix in 'systemd/libudev1@241-7~deb10u9' and '@241-7~deb10u9', and its exploit maturity as 'MATURE'. The detailed view also includes 'Detailed paths' showing the introduction through 'openjdk@11.0.13-slim-buster' and 'systemd/libudev1@241-7~deb10u8', and 'Security information' listing factors contributing to the scoring: 'Snyk: CVSS 7.8 - High Severity', 'NVD: CVSS 7.8 - High Severity', and 'Debian Security Rating: Not yet assigned'.

- Sẽ có những thông tin về lỗ hổng chi tiết và thông tin bảo mật, nhìn cũng có phần giống với code analysis.

### c) Infrastructure as Code (IaC) (argocd/snyk-iac-scan.yaml, terraform/main.tf):

- Xem qua argocd/snyk-iac-scan.yaml

The screenshot shows the Snyk web interface for the repository `HaThiThuHien/snyk-boot-web` on the `master` branch. The `argocd/snyk-iac-scan.yaml` file is selected. The interface displays a list of issues, with 7 issues found. The first issue is a Medium severity problem titled "Container is running without privilege escalation control" (SNYK-CC-K8S-9). The issue details show a configuration snippet for a container named `snyk-cli` using the `snyk/snyk-cli:npm` image. The `command` is `["/bin/sh", "-c"]` and the `args` include `git clone https://github.com/papicella/snyk-boot-web;`. The issue is currently open.

#### Detailed paths

- Introduced through: [DocId: 0] › spec › template › spec › containers[snyk-cli] › securityContext › allowPrivilegeEscalation

Show less details ^

#### This issue is...

`allowPrivilegeEscalation` attribute is not set to `false`

#### The impact of this is...

Processes could elevate current privileges via known vectors, for example SUID binaries

#### You can resolve it by...

Set `spec.containers.initContainers.securityContext.allowPrivilegeEscalation` to `false`

- Tiếp theo, cùng xem qua terraform/main.tf

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

terraform/main.tf

Overview History Settings

Issues 3

SEVERITY

- ☐ High 0
- ☐ Medium 0
- ☐ Low 3

STATUS

- ☒ Open 3
- ☐ Ignored 0

3 of 3 issues Sort by highest severity

**L 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 less details

**This issue is...**

S3 bucket versioning is disabled

**The impact of this is...**

Changes or deletion of objects will not be reversible

**You can resolve it by...**

For AWS provider < v4.0.0, set `versioning.enabled` attribute to `true`. For AWS provider >= v4.0.0, add `aws_s3_bucket_versioning` resource.

- Cả 2 loại đều liệt kê ra các lỗi hổng ở các mức độ, chi tiết ở code và cách fix chúng, nhìn sơ bộ thì nó khá đơn giản hơn so với code analysis và dockerfile. Và các lỗi hổng ở phần này cũng ít hơn nhiều và tính ảnh hưởng cũng thấp hơn nhiều.

#### d) Tổng kết:

- Các vấn đề bảo mật được phát hiện chủ yếu tập trung ở Dockerfile và các tệp IaC, cho thấy cần phải tập trung vào việc cải thiện bảo mật cho các phần này.
- Đặc biệt, các vấn đề cấp cao (Critical) cần được xử lý ưu tiên để đảm bảo an toàn và bảo mật của hệ thống.

**e. Fix các lỗ hổng bảo mật bằng tính năng Snyk Pull Request**

- Ở bước này, chúng ta đã có thử tìm hiểu và trình bày ở trên, nhưng để tìm hiểu rõ hơn về vấn đề này trong task sau

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

- Mở file pom.xml để quan sát lại các lỗ hổng bảo mật đã được tìm thấy.
- Chọn một lỗ hổng bảo mật và chọn Fix this vulnerability.

The screenshot displays the Snyk web application interface for a project named 'HaThiThuHien/snyk-boot-web'. The file 'pom.xml' is selected, showing 54 issues. The interface includes a sidebar with navigation links (Dashboard, Projects, Integrations, Members, Settings) and a top bar with project details. The main content area features filters for severity (Critical, High, Medium, Low) and priority score (0-1000). A prominent message states: 'NEW Did you know... You can reduce the backlog of existing vulnerabilities at a manageable pace with prioritized fix pull requests - enable for your GitHub integration.' Below this, a vulnerability for 'org.springframework:spring-beans' is shown with a score of 919 and a severity of 'Remote Code Execution'.



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

**M** pom.xml

Overview History Settings

log4j

**Fix these vulnerabilities**

3 of 54 issues Sort by highest priority score

**SEVERITY**

<input type="checkbox"/> Critical	3
<input type="checkbox"/> High	21
<input type="checkbox"/> Medium	24
<input type="checkbox"/> Low	6

**PRIORITY SCORE**

Scored between 0 - 1000

**"FIXED IN" AVAILABLE**

<input type="checkbox"/> Yes	53
<input type="checkbox"/> No	1

**COMPUTED FIXABILITY**

**org.apache.logging.log4j:log4j-core** - Remote Code Execution (RCE) SCORE 879

VULNERABILITY

- CWE-94
- CVE-2021-45046
- CVSS 9
- SNYK-JAVA-ORGAPACHELOGGING-LOG4J-2320014

Introduced through

Fixed in

Exploit maturity

- Chọn những lỗ hổng cần khắc phục và chọn Open PR Fix để tạo một pull request mới.

HaThiThuHien > Fix > Fc118e48 F298 403a Bd2a E40e4b61b9cf

## Open a Fix PR

HaThiThuHien/snyk-boot-web:pom.xml

[Back to project](#)

### Issues with a fix

An upgrade is available to fix these issues:

- ☐ **H** **Denial of Service (DoS)** in ch.qos.logback:logback-classic
- ☐ **H** **Uncontrolled Resource Consumption ('Resource Exhaustion')** in ch.qos.logback:logback-classic
- ☐ **H** **Denial of Service (DoS)** in ch.qos.logback:logback-core
- ☐ **H** **Uncontrolled Resource Consumption ('Resource Exhaustion')** in ch.qos.logback:logback-core
- ☐ **H** **Denial of Service (DoS)** in com.fasterxml.jackson.core:jackson-databind

HaThiThuHien commented now

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) <a href="#">SNYK-JAVA-ORGAPACHELOGGINGLOG4</a>	org.apache.logging.log4j:log4j-core: 2.15.0 -> 2.16.0	No	Mature

- Lúc này, một pull request mới đã được tạo, chúng ta có thể chọn các tab Conversation, Commits, Checks, Files changed để xem thông tin chi tiết về Pull Request này.
- Sau khi kiểm tra và xác nhận không có xung đột gì, tiến hành merge pull request

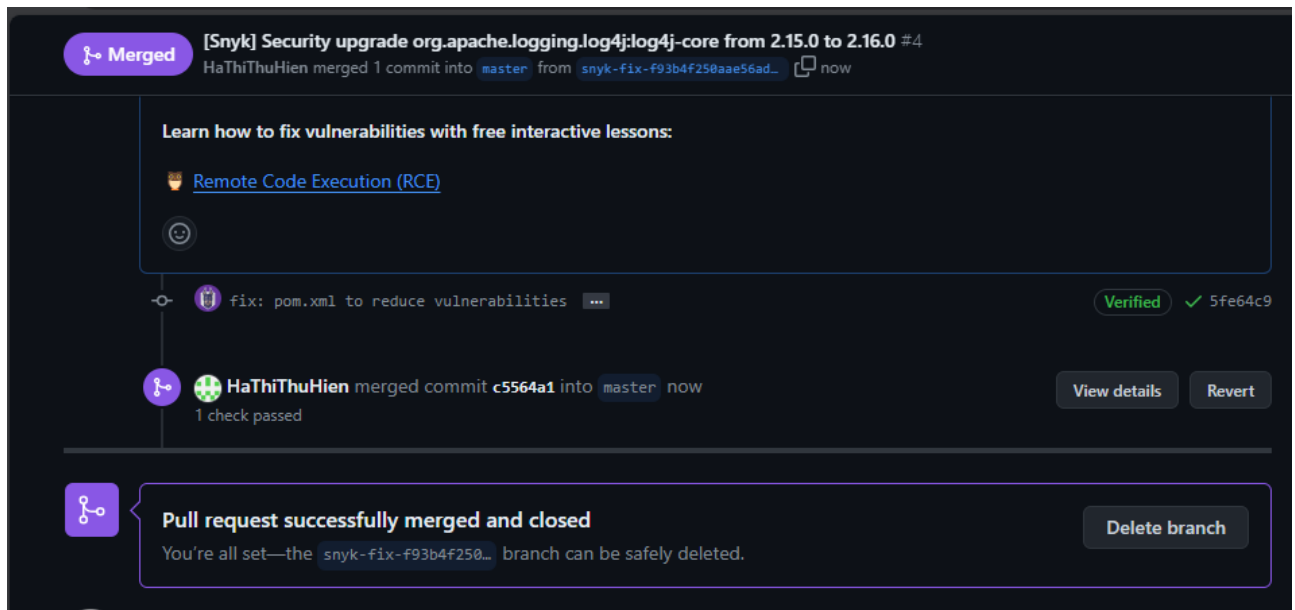
Add more commits by pushing to the `snyk-fix-f93b4f250aae56ad2ae93e7305015065` branch on `HaThiThuHien/snyk-boot-web`.

**Require approval from specific reviewers before merging**  
Rulesets ensure specific people approve pull requests before they're merged. [Add rule](#)

**All checks have passed**  
1 successful check [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](#).



- Quay lại Snyk, kiểm tra và thấy rằng số lượng cảnh báo trên tập tin pom.xml đã giảm từ 3 Critical thành 2 Critical.



*Snyk CLI & Snyk IDE*

Snyk CLI

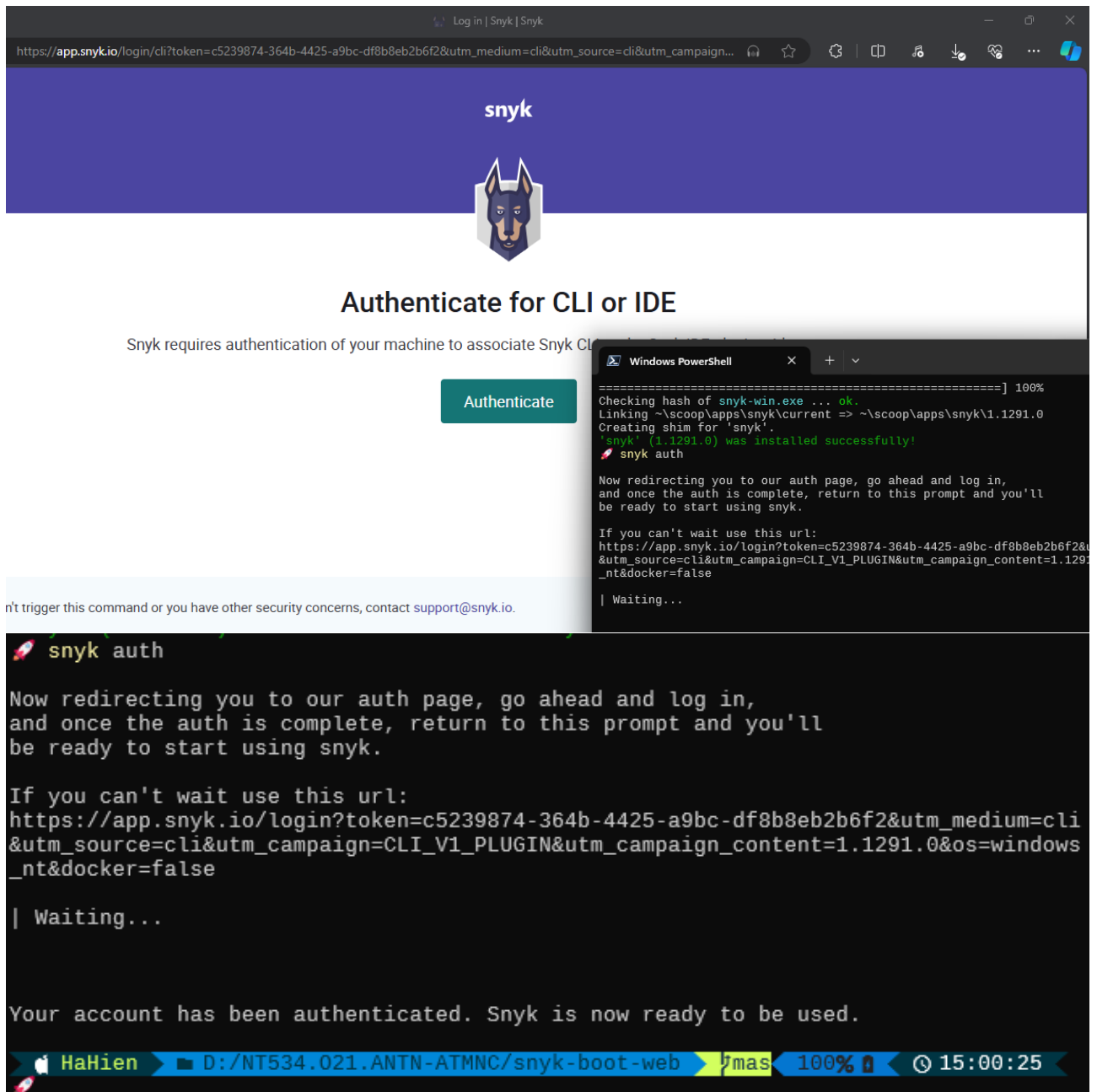
### 5. Task: Cài đặt Snyk CLI, sử dụng các công cụ của Snyk để scan và xuất report thành file

- Cài đặt Snyk CLI theo hướng dẫn sau: <https://docs.snyk.io/snyk-cli/install-or-update-the-snyk-cli>

```
Check the spelling of the name, or if a path was included, verify that t
❯ iex (new-object net.webclient).downloadstring('https://get.scoop.sh')
Initializing...
Downloading...
Creating shim...
Adding ~\scoop\shims to your path.
Scoop was installed successfully!
Type 'scoop help' for instructions.
```

```
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
❯ scoop bucket add snyk https://github.com/snyk/scoop-snyk
Checking repo... OK
The snyk bucket was added successfully.
❯ scoop install snyk
Installing 'snyk' (1.1291.0) [64bit] from 'snyk' bucket
snyk-win.exe (92.8 MB) [=====] 100%
Checking hash of snyk-win.exe ... ok.
Linking ~\scoop\apps\snyk\current => ~\scoop\apps\snyk\1.1291.0
Creating shim for 'snyk'.
'snyk' (1.1291.0) was installed successfully!
HaHien ➤ D:/NT534.021.ATN-ATMNC/snyk-boot-web ➤ master 100% 14:57:52
```

- Ủy quyền cho Snyk CLI bằng cách chạy câu lệnh sau ở Terminal/CMD.



Log in | Snyk | Snyk

[https://app.snyk.io/login/cli?token=c5239874-364b-4425-a9bc-df8b8eb2b6f2&utm\\_medium=cli&utm\\_source=cli&utm\\_campaign=cli](https://app.snyk.io/login/cli?token=c5239874-364b-4425-a9bc-df8b8eb2b6f2&utm_medium=cli&utm_source=cli&utm_campaign=cli)

snyk

**Authenticate for CLI or IDE**

Snyk requires authentication of your machine to associate Snyk CLI with your account.

[Authenticate](#)

n't trigger this command or you have other security concerns, contact [support@snyk.io](mailto:support@snyk.io).

```
Windows PowerShell
=====] 100%
Checking hash of snyk-win.exe ... ok.
Linking ~\scoop\apps\snyk\current => ~\scoop\apps\snyk\1.1291.0
Creating shim for 'snyk'.
'snyk' (1.1291.0) was installed successfully!
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=c5239874-364b-4425-a9bc-df8b8eb2b6f2&
&utm_source=cli&utm_campaign=CLI_V1_PLUGIN&utm_campaign_content=1.1291
_nt&docke=false

| Waiting...

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=c5239874-364b-4425-a9bc-df8b8eb2b6f2&utm_medium=cli
&utm_source=cli&utm_campaign=CLI_V1_PLUGIN&utm_campaign_content=1.1291
_nt&docke=false

| Waiting...

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

HaHien D:/NT534.021.ANTN-ATMNC/snyk-boot-web mas 100% 15:00:25

- Clone nội dung Webapp về máy

```
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.
remote: Compressing objects: 100% (3/3), done.
remote: Total 367 (delta 0), reused 2 (delta 0), pack-reused 364
Receiving objects: 100% (367/367), 146.36 KiB | 44.00 KiB/s, done.
Resolving deltas: 100% (138/138), done.
ls

Directory: D:\NT534.021.ANTN-ATMNC

Mode                LastWriteTime         Length Name
----                -
d-----          3/19/2024   3:48 AM             .vscode
d-----          3/2/2024   6:29 PM             Slide Môn Học-20240302
d-----          5/4/2024   2:22 PM             snyk-boot-web
-a---          3/18/2024   2:24 PM             1262 lab1_cau1.asm
-a---          4/12/2024   4:22 PM          10224984 lab3.docx
-a---          5/1/2024  11:50 PM          1658864 Mau_bao_cao.docx
-a---          3/2/2024   6:28 PM          11334180 Slide Môn Học-20240302.zip

cd .\snyk-boot-web\
ls

Directory: D:\NT534.021.ANTN-ATMNC\snyk-boot-web

Mode                LastWriteTime         Length Name
----                -
d-----          5/4/2024   2:22 PM             .git
d-----          5/4/2024   2:22 PM             .github
d-----          5/4/2024   2:22 PM             .mvn
d-----          5/4/2024   2:22 PM             argocd
d-----          5/4/2024   2:22 PM             kubernetes
d-----          5/4/2024   2:22 PM             pac
d-----          5/4/2024   2:22 PM             src
d-----          5/4/2024   2:22 PM             terraform
-a---          5/4/2024   2:22 PM             100 .deepsource.toml
-a---          5/4/2024   2:22 PM             284 build-container.sh
```

- Sử dụng Synk Open Source để scan manifest file

```

# snyk test
Testing D:\NT534.021.ANTN-ATMNC\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
  X Information Exposure [Medium Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-3146851] in com.h2database:h2@1.4.20
  introduced by com.h2database:h2@1.4.200
  X 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
  X XML External Entity (XXE) Injection [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-1769238] in com.h2datab
  ase: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-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
  X Arbitrary Code Execution [Medium Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2327339] in org.apache.l
  ogging.log4j:log4j-core@2.15.0
  introduced by org.apache.logging.log4j:log4j-core@2.15.0
  X Denial of Service (DoS) [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2321524] in org.apache.logg
  ing.log4j:log4j-core@2.15.0

  X Privilege Escalation [High Severity][https://security.snyk.io/vuln/SNYK-JAVA-
  mbed:tomcat-embed-core@9.0.45
  introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE
  at@2.3.10.RELEASE > org.apache.tomcat.embed:tomcat-embed-core@9.0.45
  X Improper Input Validation [High Severity][https://security.snyk.io/vuln/SNYK-
  el@3.0.3
  introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE
  at@2.3.10.RELEASE > org.glassfish:jakarta.el@3.0.3
  X Remote Code Execution [Critical Severity][https://security.snyk.io/vuln/SNYK-
  ork:spring-beans@5.2.14.RELEASE
  introduced by org.springframework.boot:spring-boot-starter-web@2.3.10.RELEASE
  rg.springframework:spring-beans@5.2.14.RELEASE

Issues with no direct upgrade or patch:

  X Remote Code Execution (RCE) [High Severity][https://security.snyk.io/vuln/SNYK-
  .200
  introduced by com.h2database:h2@1.4.200
  No upgrade or patch available

Organization:      hathithuhien
Package manager:   maven
Target file:       pom.xml
Project name:      com.example:snyk-boot-web
Open source:       no
Project path:      D:\NT534.021.ANTN-ATMNC\snyk-boot-web
Licenses:          enabled

```

- Sử dụng Synk Code để scan source code

```

snyk code test

Testing D:\NT534.021.ANTN-ATMNC\snyk-boot-web ...

X [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.

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

✓Test completed

Organization:      hathithuhien
Test type:         Static code analysis
Project path:      D:\NT534.021.ANTN-ATMNC\snyk-boot-web

Summary:

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

HaHien D:/NT534.021.ANTN-ATMNC/snyk-boot-web master ?1

snyk code test

Testing D:\NT534.021.ANTN-ATMNC\snyk-boot-web ...

X [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.

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

✓Test completed

Organization:      hathithuhien
Test type:         Static code analysis
Project path:      D:\NT534.021.ANTN-ATMNC\snyk-boot-web

Summary:

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

HaHien D:/NT534.021.ANTN-ATMNC/snyk-boot-web master ?1

```

- Xuất kết quả thành file HTML. Để xuất được kết quả thành file HTML, cần cài đặt một plugin snyk-to-html (<https://docs.snyk.io/snyk-cli/scan-and-maintain-projects-using-the-cli/cli-tools/snyk-to-html>)

```
npm install snyk-to-html -g
added 23 packages in 15s
1 package is looking for funding
  run `npm fund` for details
npm notice
npm notice New minor version of npm available! 10.2.0 -> 10.7.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v10.7.0
npm notice Run npm install -g npm@10.7.0 to update!
npm notice
HaHien D:/NT534.O21.ANTN-ATMNC/snyk-boot-web master
```

```
snyk test --json | snyk-to-html -o results.html
Vulnerability snapshot saved at results.html
HaHien D:/NT534.O21.ANTN-ATMNC/snyk-boot-web master ?2
```

Work Snyk test report

File | D:/NT534.O21.ANTN-ATMNC/snyk-boot-web/results.html

# snyk

## Snyk test report

May 4th 2024, 5

Scanned the following path:

- D:\NT534.O21.ANTN-ATMNC\snyk-boot-web\pom.xml (maven)

54 known vulnerabilities | 54 vulnerable dependency paths | 40 dependencies

Project	com.example:snyk-boot-web	Path	D:\NT534.O21.ANTN-ATMNC\snyk-boot-web
Package Manager	maven	Manifest	pom.xml

**CRITICAL SEVERITY**

### Remote Code Execution

Snyk IDE

## 6. Bonus: Cài đặt Snyk plugin/extension vào IDE đang sử dụng và quan sát kết quả scan



The screenshot displays the Visual Studio Code interface with the Snyk Security extension installed. The Explorer pane on the left shows the project structure for 'snyk-boot-web', including files like .github, .mvn, argocd, kubernetes, pac, src, terraform, .dccache, .deepsource.toml, build-container.sh, Dockerfile, pom.xml, README.md, and results.html. The Snyk Security extension is highlighted in the Extensions view, showing its version (v2.6.1) and a 4.5-star rating. The extension's details page is open, displaying the Snyk logo and a description of the plugin's capabilities. The Snyk CLI interface is visible in the bottom right, showing the command 'snyk scan' and the output 'Run scan for Open Source security vulnerabilities.' The terminal at the bottom shows the command 'snyk scan' and the output 'Run scan for Open Source security vulnerabilities.'

**Snyk Security** v2.6.1  
Snyk [snyk.io](#) | 183,143 | ★★★★★ (29)  
Easily find and fix vulnerabilities in your code, open source dependencies, infrastructure as code, and containers.

**Visual Studio Code extension**

The Snyk Visual Studio Code plugin scans and provides analysis of your code, including open-source dependencies and infrastructure as code configurations. Download the plugin at any time free of charge and use it with any Snyk account. Scan your code early in the development lifecycle to help you pass security reviews and avoid costly fixes later in the development cycle.

**Snyk Security** v2.6.1  
Snyk [snyk.io](#) | 183,143 | ★★★★★ (29)  
Easily find and fix vulnerabilities in your code, open source dependencies, infrastructure as code, and containers.

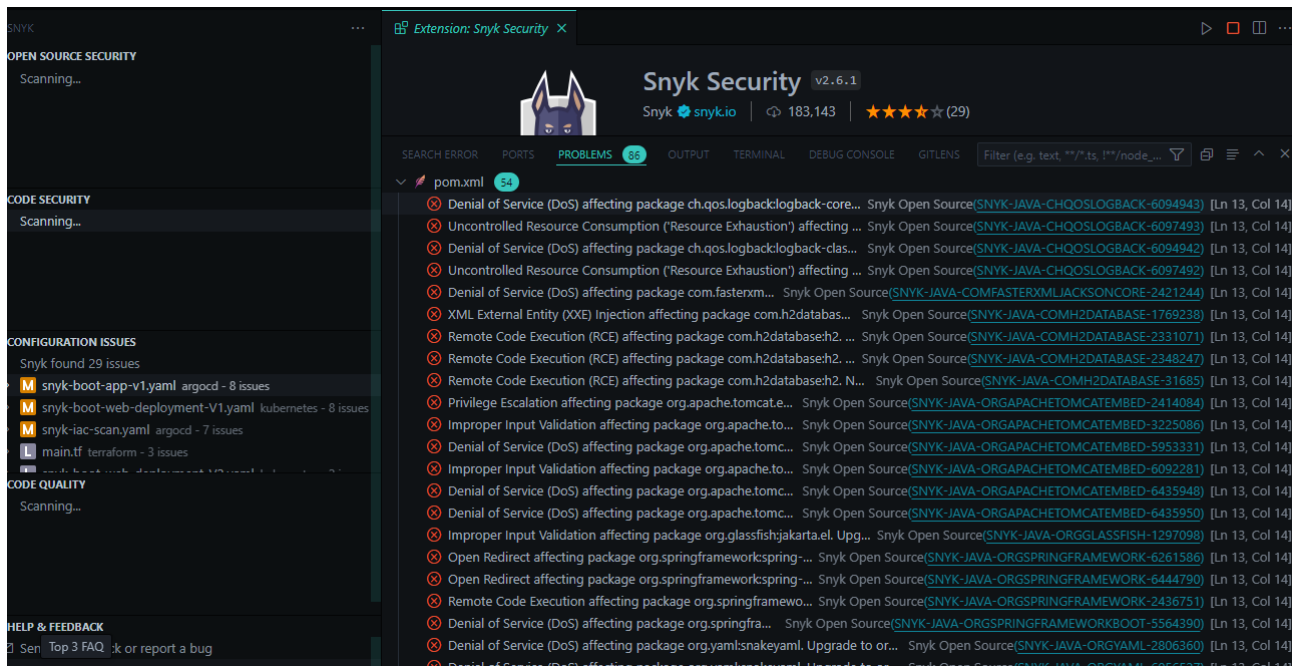
**Visual Studio Code extension**

The Snyk Visual Studio Code plugin scans and provides analysis of your code, including open-source dependencies and infrastructure as code configurations. Download the plugin at any time free of charge and use it with any Snyk account. Scan your code early in the development lifecycle to help you pass security reviews and avoid costly fixes later in the development cycle.

Snyk scans for vulnerabilities and returns results with security issues categorized by issue type and severity.

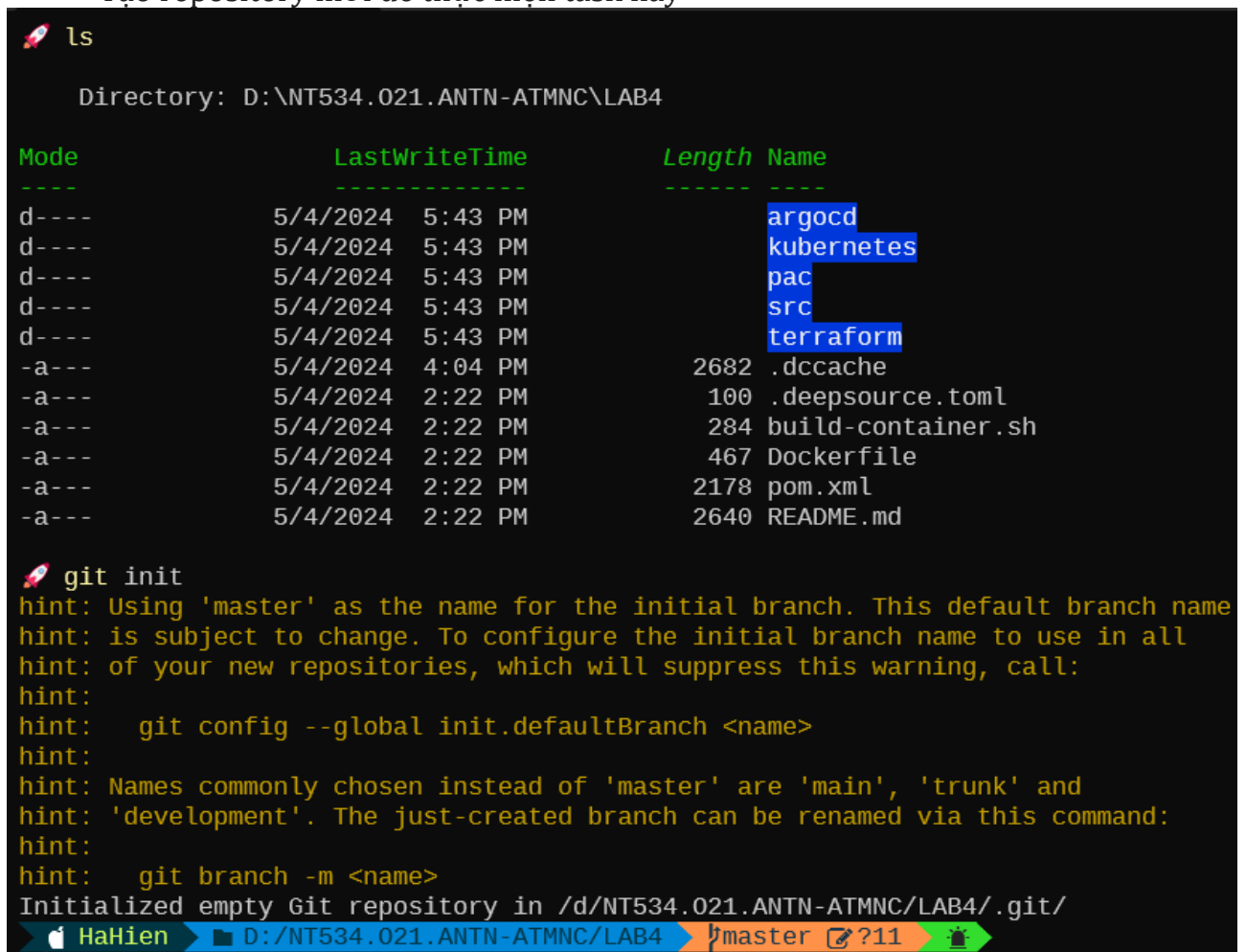
SEARCH ERROR | PORTS | PROBLEMS | OUTPUT | **TERMINAL** | DEBUG CONSOLE | GITLENS

HaHien | D:\NT534.021\ANTN-ATM\IC\snyk-boot-web | master | 23



## 7. Bonus: Tạo một pre-commit hook gọi Snyk CLI để scan repository

- Tạo repository mới để thực hiện task này



- Nhiều file sample ta có thể thấy ở đây.

```
cd .git/hooks
ls
```

Directory: D:\NT534.021.ANTN-ATMNC\LAB4\.git\hooks

Mode	LastWriteTime	Length	Name
-a---	5/4/2024 5:44 PM	478	applypatch-msg.sample
-a---	5/4/2024 5:44 PM	896	commit-msg.sample
-a---	5/4/2024 5:44 PM	4726	fsmonitor-watchman.sample
-a---	5/4/2024 5:44 PM	189	post-update.sample
-a---	5/4/2024 5:44 PM	424	pre-applypatch.sample
-a---	5/4/2024 5:44 PM	1643	pre-commit.sample
-a---	5/4/2024 5:44 PM	416	pre-merge-commit.sample
-a---	5/4/2024 5:44 PM	1374	pre-push.sample
-a---	5/4/2024 5:44 PM	4898	pre-rebase.sample
-a---	5/4/2024 5:44 PM	544	pre-receive.sample
-a---	5/4/2024 5:44 PM	1492	prepare-commit-msg.sample
-a---	5/4/2024 5:44 PM	2783	push-to-checkout.sample
-a---	5/4/2024 5:44 PM	3650	update.sample

- Tiến hành chỉnh code ở pre-commit.sample và đổi tên

```
nano .\.git\hooks\pre-commit.sample
rename .\.git\hooks\pre-commit.sample .\.git\hooks\pre-commit
rename: not enough arguments
Try 'rename --help' for more information.
move .\.git\hooks\pre-commit.sample .\.git\hooks\pre-commit
```

HaHien D:/NT534.021.ANTN-ATMNC/LAB4 master ?11

```
GNU nano 7.2 .\.git\hooks\pre-commit
#!/bin/sh
snyk test

if [ $? -ne 0 ]; then
    echo "Snyk test failed. Please fix the vulnerabilities before committing"
    exit 1
fi

echo "Snyk test passed. Ready to commit."
exit 0
```

- Chạy lệnh git commit và ta có được kết quả

```
git commit
Testing D:\NT534.021.ANTN-ATMNC\LAB4...
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
X 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
X 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
X 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
X 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
X Arbitrary Code Execution [Medium Severity][https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2327339] in org.apache.logging.log4j:log4j-core@2.15.0
```

#### Issues with no direct upgrade or patch:

```
X 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
  No upgrade or patch available
```

```
Organization:    hathithuhien
Package manager: maven
Target file:     pom.xml
Project name:    com.example:snyk-boot-web
Open source:     no
Project path:    D:\NT534.021.ANTN-ATMNC\LAB4
Licenses:        enabled
```

```
.git/hooks/pre-commit: line 9: unexpected EOF while looking for matching `''
```

```
git status
On branch master
```

```
No commits yet
```

```
Changes to be committed:
  (use "git rm --cached <file>..." to unstage)
```

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
- Ví dụ: [NT101.K11.ANTT]-Exe01\_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](https://courses.uit.edu.vn).

### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**