

Secure coding summative assignment

**Hussein Technical University**

Abdullah Istanbuli | (21110366)

Secure coding

Safaa hriez

**Table of Contents**

**Two security principles……………….………………………………………………………………3**

**Two principles in the app…….……………………………………………………. ………………. .3**

**Use case diagram …………………………………………………………………………. ……...…..4**

**Data flow diagram ….…………………………………………………………………………….…...5**

**Analysis for data flow ………………………………………………………………………………..5**

**Threat modeling …………………………………………………………..…………………….…… 5**

**Testing methods ….……………………………………………………………………………….…6**

**Quality based testing………………………………………………………..……………………….6**

**The applied security-based testing …………………………………………………....…………...7**

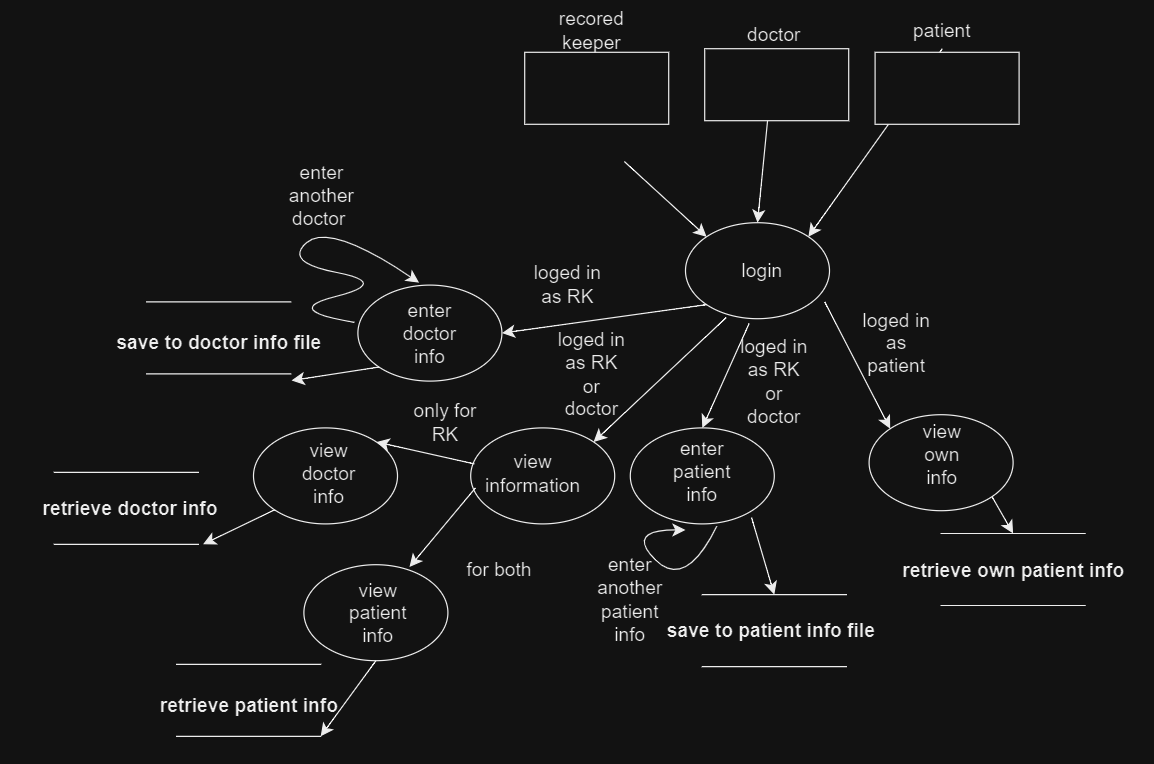
**Code review analysis …….………………… ……………………………………………………...7**

1. **Two security principles that were developed in my application**
   1. **confidentiality: ensuring that information is only accessible to authorized individuals, which keeps the system safe from any one to access what they want from not authorized person.**
   2. **Integrity: ensuring the accuracy and reliability of data and preventing unauthorized modification, since only authorized people can access the data, you can be sure that those people are going to enter reliable data.**
2. **List two quality principles that were illustrated in my application** 
   1. **understandability: code should be clear, concise, and easy to understand. The benefit of understandability is when other developers need to review or modify your code it would take less time to understand, and it wouldn’t be hard for them to understand.**
   2. **Least privilege: code should operate with the least privilege necessary to preform functions, the benefit of least privilege is to improve the security of the application by making users have less access to information that they don’t need**
3. **Use case diagram:**

A diagram of a patient

Description automatically generated

**4.data flow diagram:**



**5.analyze the created data flow diagram:**

**Potential threat 1: there might be identity theft in the login process, if a malicious person gets the credential of the record keeper, he (the malicious person) can access the entire system.**

**Potential threat 2: man in the middle attack, if someone interrupts the login single, they might get the login credential in the system and for that reason we made a hashing process to preserve the password of logged on people.**

**Potential threat 3: denial of service, overloading the system by flooding it with requests.**

**6.the full threat model are attached with the submission**

**7.what type of testing methods have been used to test the satisfaction of the application to the requirements:**

**7.1 system testing:**

**Method: evaluate the entire system against the specified requirements**

**Benefits: ensure that the system meets all functional and non-functional requirements, identifies overall system issues.**

**7.2 performance testing:**

**Method: re-run previously execute test to ensure that new change do not adversely affect existing functionality.**

**Benefits: identifies performance bottlenecks, ensures the application can handle expected loads, and helps optimize resource utilization.**

**8.what type of security testing methods have been used:**

**8.1 vulnerability assessment:**

**Method: scans the application for known vulnerabilities and weaknesses.**

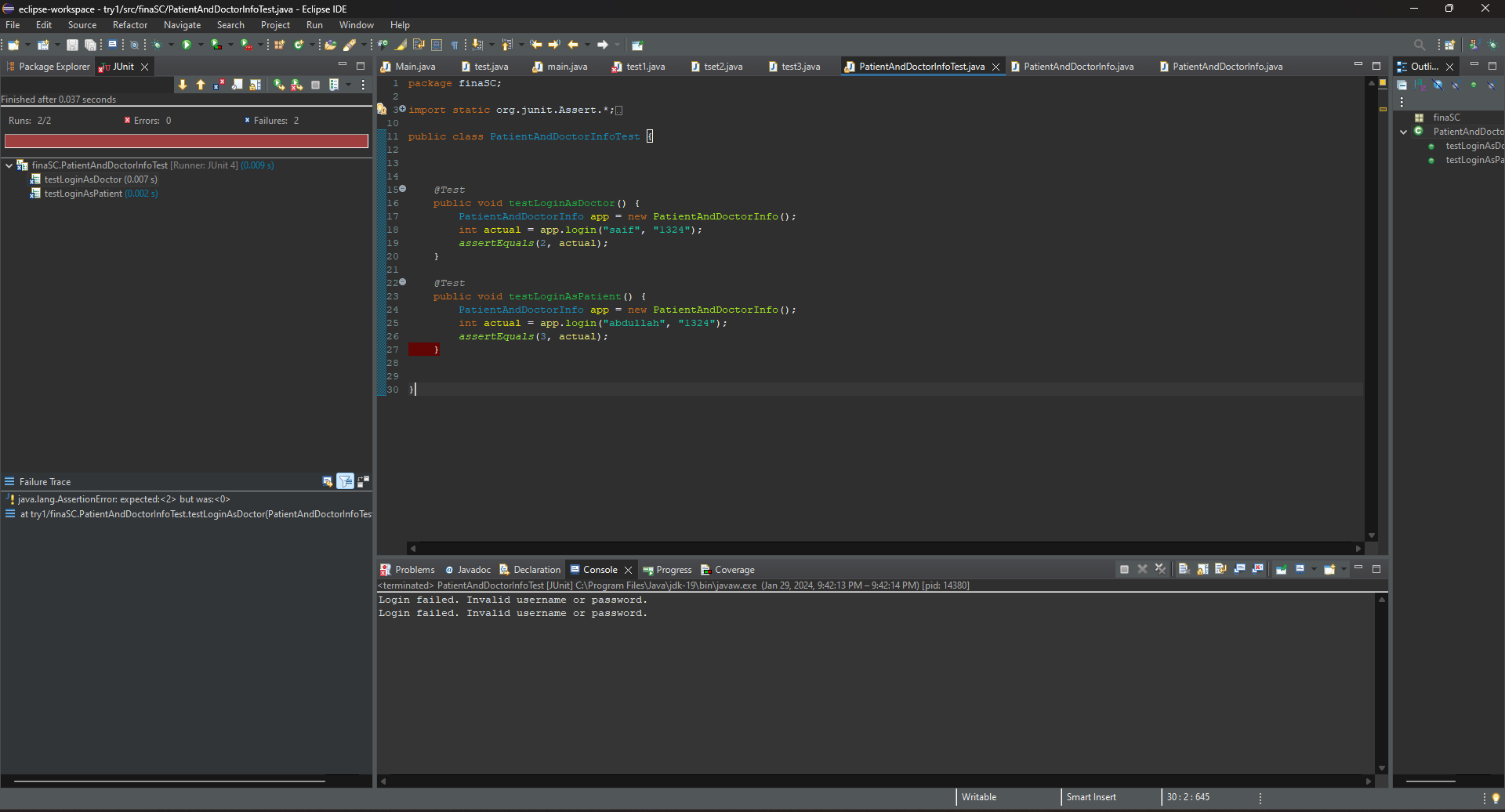
**Benefits: identify common vulnerabilities, such as outdated software, misconfigurations, and known security issues.**

**8.2 security code review:**

**Method: analyzes the source code to identify security vulnerabilities and coding errors**

**Benefits: helps identify vulnerabilities at the code level, promotes secure coding practices, and reduces the risk of introducing security flaws during development.**

**9.**



**10.**

|  |  |  |
| --- | --- | --- |
|  | input | output |
| login | **RK, 1234** | **Login successful as record keeper** |
|  | **Abdullah, 1234** | **Login successful as patient** |
|  | **Saif, 1234** | **Login successful as doctor** |
|  | **Anything, anything** | Login failed. Invalid username or password. |

**11.** A screenshot of a computer

Description automatically generated

1. code versioning

**Reference list**

The slides