Final Project: Spades

# Introduction

Project: Implement a two-player version of Spades

Project members: Derek Luong and Jamie Bowers

Class: SWE 681- 001

Date: 2019-04-27

# Design/Architecture

# Installation Instructions

## External Dependencies

The following dependencies are required in order to install and play the spades game. This paper assumes the user knows how to install, configure, and run these dependencies.

* PostgreSQL 11
* Any Java IDE that supports Maven 3.5.2 (We used IntelliJ) with the 10.0.2 JDK
* JDK 10.0.2
* Java 1.8
* Two Separate Internet Browsers (We tested against Firefox and Google Chrome) or two separate computers.

## Initial Setup

In order to run the Spades game, the user must set up the initial database. This involves creating the necessary tables for both Spring Security as well as tables used to run and store information about Spades games.

Inside the Java project there is a folder called “sql\_scripts” and a file called “create\_database.sql”. To create the necessary tables, run the file “create\_database.sql” inside the Postgres’s pgAdmin tool using the Query tool.

Next in order for Spring to connect to the database and run you will need to modify your appilication.prooerties file, which is located in the spades/src/resources directory, to tell it what your database URL, username, and password are. You will need to modify lines 15-17 to reflect what your configurations should be.

# Operating Instructions

## Startup In order to start the game you must choose to run the application in your chosen Java IDE, your log upon start up will show the Spring Boot text with the version of Spring Boot being 2.1.3 and you will see “Started SpadesAppilication” in the log, Once Spring has started you are ready to start the Spades application. We have implemented port forwarding in Spring so that if you simply type localhost in your browser it will send you to the correct https://localhost local website ensuring that you are using the TLS self signed certificate that we created through the Java keystore.

## Create Users

The first step in order to play this game requires that two user accounts are created. A user can be created using the “Create User” link from the front page. Creating a user has four fields that are required; Username, Last Name, Email, and Password. We implemented a password whitelist that requires a password be at least eight characters, and must have the following characteristics; It must be use at least one lower case characters, one uppercase character, one numeric character and one of the following special characters “@#%$^” it also must not use whitespaces (tab or space).

## Create and Join a Game Once two or more players have been created, a game can be created. To do this simply click the “Create Game” button. Once a game has been created the users can join a game, the user that created the game is given a link to join the game and it will wait until the 2nd player has joined a game. For the 2nd player there is a “find games” link that they can click to find existing games that have been created. If Player 2 does not join the game in the five minutes that we set up for out game timeout the game is no longer active, and a new game must be created.

## Gameplay

Once both users have joined a game each player will get dealt a random hand and each player must bid the number of tricks they think the can win (see Game Rules). Once each player has bid the game begins and each player plays a card from the hand they are dealt with the objective being to win or not win the round based on their bid. Players may only play the cards they are dealt and only when it is their turn to play. The game keeps track of whose turn it is and tells each player whose turn it is and what card have been played by which player. Statistics on the page what each players Bids were and what their actual tricks won are, these statistics are shown and updated upon each winning trick. When a round is complete statistics showing each round, the bid for each player that round the number of tricks each player won for that round the number of bags they have in total and their current score. The game continues if a player has not won and shows your new hand and asks for a bid, this process continues until one of the two players has won the game.

# Game Rules

## Objective

Be the first player to reach 500 points. If both players reach 500 points in the same round the player with the higher number of points between the two wins.

## Setup

Each “Round” a 52 Card Deck is shuffled. Two players are each dealt thirteen cards from the deck randomly. This leaves 26 cards that are remaining in the deck, which will not be used in the current round. (13 cards per player \* 2 players + 26 cards left over = 52 Total Cards in Deck)

## Card Rank

Card Values are Ace (A), King (K), Queen (Q), Jack (J), 10, 9, 8, 7, 6, 5, 4, 3, and 2. Suits are Spades (S), Hearts (H), Clubs (C), and Diamonds (D). Spades beats every other suited card. E.g. 2S (2 of Spades) beats AH (Ace of Hearts). In the case of same card suits, the higher valued card will win, so 9H (9 of Hearts) beats 7H (7 of Hearts). If a Spades suit is not played but the played cards have different suits, then the leading player (the player that went first in the current trick) will win regardless of card value.

## Bidding

Each player will decide how many “Tricks” they think they can win in a round. They can also choose “nil” if they want to try to lose every trick that hand to try to get 100 points for that round (See Scoring) A “Trick” is simply a winning hand. Bidding occurs each round.

## Scoring

Each winning trick is worth 10 times the bid amount and every trick that is won that goes over the bid amount is referred to as a “Sandbag” or “bag” and is worth 1 point. **Example:** Player 1 bids 6 tricks and wins 8. They are awarded 62 points, 60 for their bid and 2 for their bag.

If a player fails to meet the number of tricks they bid the player is deducted the entire bid times 10 points for each bid. **Example:** Player 2 bids 8 tricks but only gets 6 tricks in the round, they are deducted 80 points.

Sandbags are kept track of for each player and once a player hits 10 bags or more they are deducted 100 points, and their bags are subtracted by 10.

A player can bid 0 (known as a NIL bid) if they believe they can lose every trick in order to get 100 points for the round. If they fail to do this and get even 1 trick they are deducted 100 points.

## Gameplay

Player 1 starts the game and plays a card, player 2 then follows. Spades are not allowed to be played unless they have already been “broken”. In order to “Break Spades” a player may play a spade if they do not have any cards of the suit that the opening player plays, or if the opening player only has cards of the Spades suit remaining. Once Spades is broken it can be opened with in any following round.

Example: Player 1 has 5S, 4C, 2D and 3D, player 2 has QH, 10D, 3S, and 4S. Player 1 plays 2D, player 2 must play a Diamond, in the next hand Player 1 Plays 3D because Player 2 no longer has any Diamonds they can play their 3 of Spades to win the trick, Spades are now broken and Player 1 can play their 5S in the next hand.

The winner of the trick starts the next hand. Each hand is played until the players are out of their initial 13 cards. The round is then scored and a new round is started. This process goes on until one of the players wins the game.

# Why This Application is Secure

## Confidentiality

**Requirement:** “You must create an audit trail of every game move, and these game moves must not be available to those not in the game until the game has completed. After the game is completed, the final audit record (including every move) must be publicly available to all authenticated users (but to not to unauthenticated ones). The win/loss/draw record of each user must be made available to authenticated users (but not to unauthenticated ones).”

We have created an audit trail of every game move using a database table called “moves” each time a player has played a card it records the card they played in the moves table, if a game crashes the round is reset and moves that we’re made before the completion of the round are deleted from that table, this is done because of the randomness of dealing a deck each round does not let us persist who had what cards if your game has crashed. The overall game moves are not shown until the game is over and the final audit report of who won that game, the rounds played during that game, the moves of that game, and points for the game. A win/loss statistics page is available when you are not playing a game, which shows wins and losses for every player and is only available to authorized players. We consider an authorized player any player that has an account and is logged in.

## Integrity

**Requirement: “**Only the current player can make a move in a given game, and it must be a legal move (syntactically and given the current situation). Make sure that the audit trail of game moves can’t be changed (except by legal moves during a game!), and that the win/loss/draw record of each user can only be changed by actually winning, losing, or drawing.”

In order to meet the requirement that only the current player can make a move in a given game we implement a check on whose turn it currently is and if the player whose turn it is makes a move it is allowed, if they player whose turn it is not tries to play a card the game does not allow that card to be played and the game continues to wait for the player whose turn it is. The same audit trail of moves we implemented for the “moves” table only records moves if the move was allowed as such it is impossible for players to change that table themselves, only the game records moves if the move was allowed. The “Win, lose, and draw” statistics is calculated each time a game is completed and is calculated from the games table in the database. Users can not make changes to these statistics themselves in any malicious way, if they want to change the statistics, they must complete playing a game.

## Availability

**Requirement:** “The player must not be able to make any game (including one he’s playing) pause forever. A timeout eventually means forfeit, and sending 1 byte should not cause a stall forever. A simple packet or command shouldn’t kill or stall a game. You can’t prevent everything, so in the case of DDoS attacks, try to relatively quickly recover once the attack ceases or is filtered out upstream. If a player gets logged out for some reason (e.g. wireless failure), they must be able to reconnect to the game and continue to play (as long as the timeout hasn’t expired). Your system must support multiple simultaneous games by different users (threads are permitted, but not necessary). It’s fine if a given user can only play one game at a time.”

We met the requirement to have a timeout in two ways. One we have a game time out in which after a user has created a game we set this timer to 5 minutes. We also have a hand time out that will forfeit the game for the user whose turn it is if they do not play a card in the 3 minutes we set for the hand timeout. For the second part of this requirement if a game for some reason crashes we allow the users to rejoin the game once they log back into their account. Our system also allows for multiple simultaneous games to be played however a player can only play one game at a time.

## Information protection

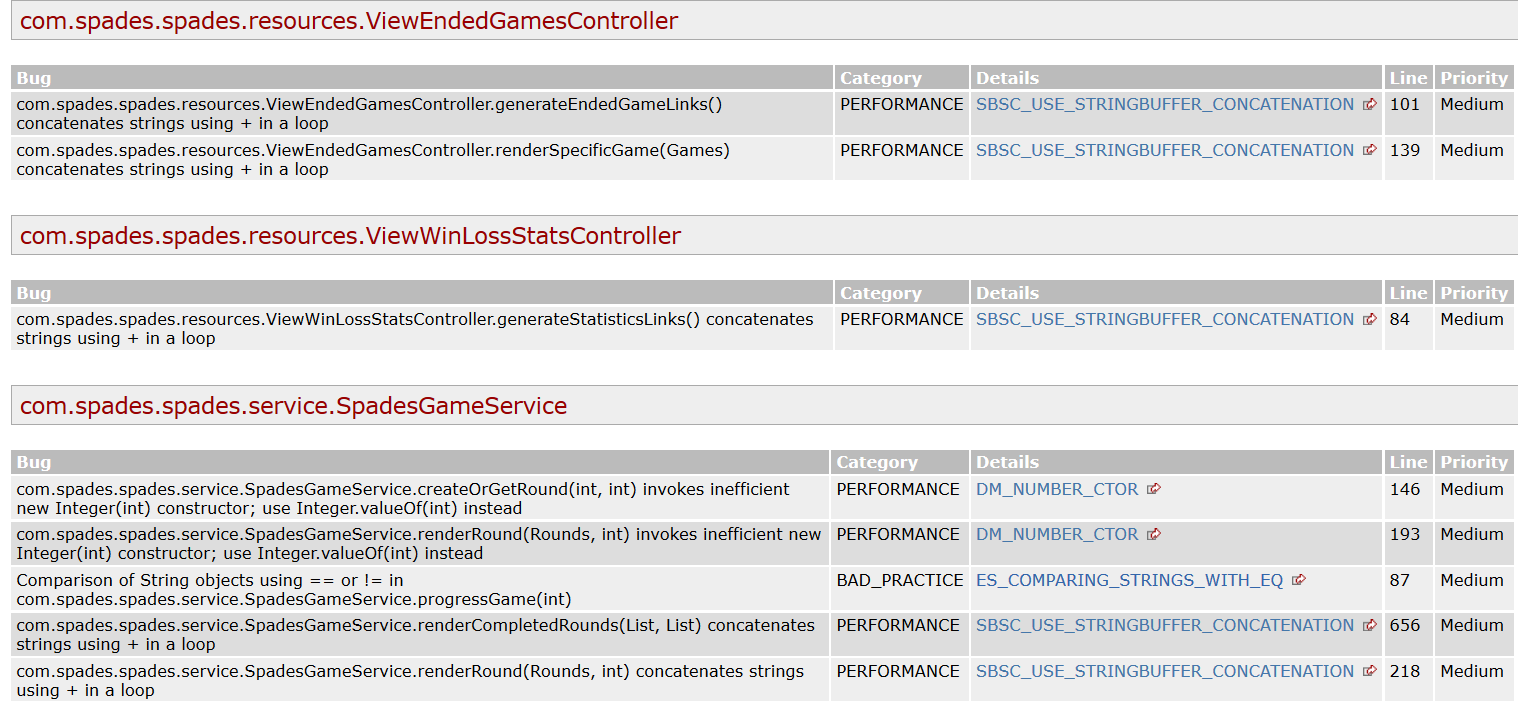
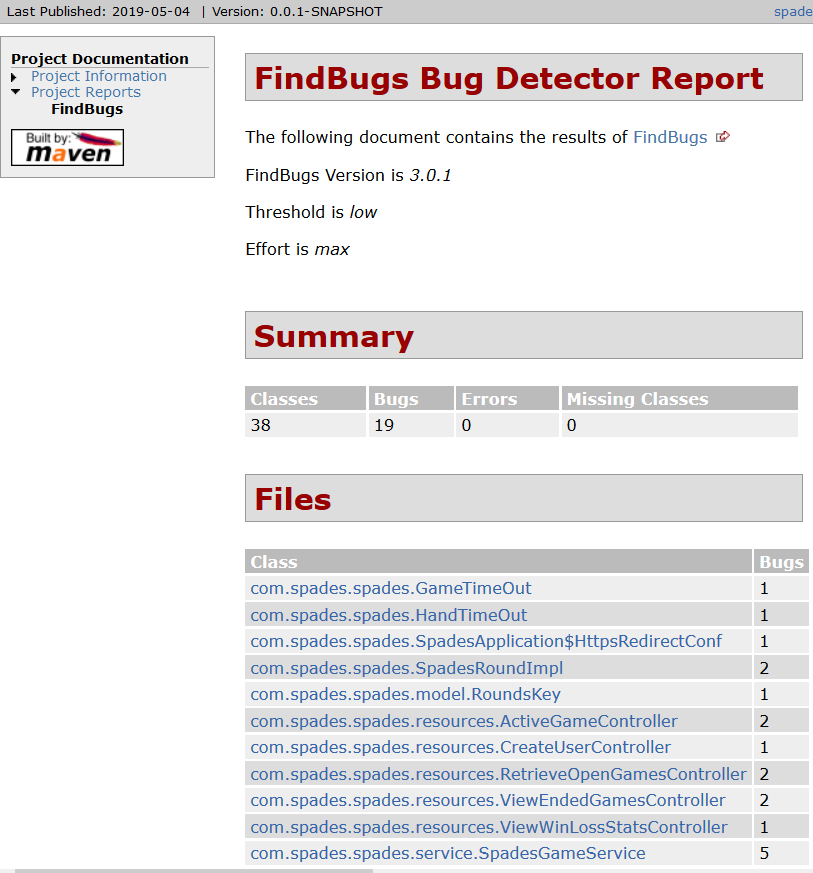
The entire application uses HTTPS to encrypt information that is exchanged. This reduces the risk that a third-party could retrieve sensitive data from web traffic that could be used to inflict damage.

Additionally, apart from the initial home page and the create user page, all other points in the application requires user authentication in order to access it. This is done by extending Spring Security’s default configuration and requiring that all requests to a certain path (containing the functionality of the application) requires user authentication, and will otherwise prompt the user with a login page.

## Using Analysis Tools

### Findbugs

The static analysis tool FindBugs was used to scan for any potential issues. An initial use of the tool revealed 19 different issues. However, most of these initial issues were related to performance or bad practice, and didn’t reveal any severe problems. After using this tool, the issues were inspected and addressed. Below is the generated summary and a sample excerpt of the issues report.



After these initial issues were resolved, another use of the FindBugs report indicated the following:

<INSERT AFTER REPORT FOR FINDBUGS>

### Visual Code Grepper

The second Static Analysis tool we used is Visual Code Grepper or VSG. VGS found a few issues that FindBugs did not, here is a report that we ran after fixing the issues that Findbugs found. Several of these issues are false positive in that they are issues inside the Maven wrapper which we have no control over. Here is the report.

**STANDARD: Potentially Unsafe Code - java.io.File**

Line: 20 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This functionality acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

import java.io.File;

**STANDARD: Potentially Unsafe Code - FileInputStream**

Line: 21 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

import java.io.FileInputStream;

**STANDARD: Potentially Unsafe Code - java.io.File**

Line: 21 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This functionality acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

import java.io.FileInputStream;

**STANDARD: Potentially Unsafe Code - java.io.File**

Line: 22 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This functionality acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

import java.io.FileOutputStream;

**STANDARD: Potentially Unsafe Code - java.io.FileOutputStream**

Line: 22 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This functionality acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

import java.io.FileOutputStream;

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 29 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class MavenWrapperDownloader {

**STANDARD: Potentially Unsafe Code - FileInputStream**

Line: 65 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

FileInputStream mavenWrapperPropertyFileInputStream = null;

**STANDARD: Potentially Unsafe Code - FileInputStream**

Line: 67 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, carefull checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename.

mavenWrapperPropertyFileInputStream = new FileInputStream(mavenWrapperPropertyFile);

**MEDIUM: Potentially Unsafe Code - Failure To Release Resources In All Cases**

Line: 108 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

There appears to be no 'finally' block to release resources if an exception occurs, potentially resulting in DoS conditions from excessive resource consumption.

**MEDIUM: Potentially Unsafe Code - FileStream Opened Without Exception Handling**

Line: 108 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

There appears to be no 'try' block to safely open the filestream, potentially resulting in server-side exceptions.

**MEDIUM: Potentially Unsafe Code - Failure To Release Resources In All Cases**

Line: 108 - C:\dev\java\spades\.mvn\wrapper\MavenWrapperDownloader.java

There appears to be no release of resources in the 'finally' block, potentially resulting in DoS conditions from excessive resource consumption.

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 7 - C:\dev\java\spades\src\main\java\com\spades\spades\Deck.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class Deck {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 24 - C:\dev\java\spades\src\main\java\com\spades\spades\Deck.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for (int i = 0; i < RANKS.length; i++) {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 25 - C:\dev\java\spades\src\main\java\com\spades\spades\Deck.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for (int j = 0; j < SUITS.length; j++) {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 26 - C:\dev\java\spades\src\main\java\com\spades\spades\Deck.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

card = RANKS[i] + SUITS[j];

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 9 - C:\dev\java\spades\src\main\java\com\spades\spades\GameTimeOut.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class GameTimeOut {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 7 - C:\dev\java\spades\src\main\java\com\spades\spades\Hand.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class Hand {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 9 - C:\dev\java\spades\src\main\java\com\spades\spades\HandTimeOut.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class HandTimeOut {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 14 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesApplication.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class SpadesApplication {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 21 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesApplication.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class HttpsRedirectConf {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 13 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesRoundImpl.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class SpadesRoundImpl {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 44 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesRoundImpl.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for(int i = 0; i < 13; i++)

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 306 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesRoundImpl.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int leadValue = -1;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 308 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesRoundImpl.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int followValue = -1;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 329 - C:\dev\java\spades\src\main\java\com\spades\spades\SpadesRoundImpl.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int winner = -1;

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 23 - C:\dev\java\spades\src\main\java\com\spades\spades\config\SecurityConfiguration.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class SecurityConfiguration extends WebSecurityConfigurerAdapter {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 36 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ActiveGameController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class ActiveGameController {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 181 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ActiveGameController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int bidAmount = -1;

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 184 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ActiveGameController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

bidAmount = Integer.parseInt(req.getParameter("bidAmount"));

**HIGH: Potentially Unsafe Code - Poor Input Validation**

Line: 184 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ActiveGameController.java

The application appears to use data contained in the HttpServletRequest without validation or sanitisation. No validator plug-ins were located in the application's XML files.

bidAmount = Integer.parseInt(req.getParameter("bidAmount"));

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 221 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ActiveGameController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

String card = req.getParameter("card");

**HIGH: Potentially Unsafe Code - Poor Input Validation**

Line: 221 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ActiveGameController.java

The application appears to use data contained in the HttpServletRequest without validation or sanitisation. No validator plug-ins were located in the application's XML files.

String card = req.getParameter("card");

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 24 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateGameController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class CreateGameController {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 58 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateGameController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

response += "<a href=\"/secured/all/game/" + gameId + "\">Go to new game</a>\n";

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 86 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateGameController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

LOGGER.info("game created with id =" + newId);

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 28 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateUserController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class CreateUserController {

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 43 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateUserController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

String userName = hReq.getParameter("username");

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 44 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateUserController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

String lastName = hReq.getParameter("lastname");

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 45 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateUserController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

String email = hReq.getParameter("email");

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 46 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\CreateUserController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

String password = hReq.getParameter("password");

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 12 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\GeneralErrorController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class GeneralErrorController implements ErrorController {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 19 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\HelloResource.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class HelloResource {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 55 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\HelloResource.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

if (getUserOpenGames(playerID1) != -1) {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 57 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\HelloResource.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

buttonOrLink = "<a href=\"/secured/all/game/" + gameId + "\">Go to Existing Open Game</a>\n";

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 26 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\JoinGameController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class JoinGameController {

**STANDARD: Potentially Unsafe Code - getParameter**

Line: 46 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\JoinGameController.java

This function extracts data directly from the HTTP request. Manually check the code to ensure the data obtained is correctly validated and/or sanitised.

int gameId = Integer.parseInt(req.getParameter("game\_id"));

**HIGH: Potentially Unsafe Code - Poor Input Validation**

Line: 46 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\JoinGameController.java

The application appears to use data contained in the HttpServletRequest without validation or sanitisation. No validator plug-ins were located in the application's XML files.

int gameId = Integer.parseInt(req.getParameter("game\_id"));

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 58 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\JoinGameController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

String gameURL = "/secured/all/game/" + gameId;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 89 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\JoinGameController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

LOGGER.debug("Joined game id = " + gameId);

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 17 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\RetrieveOpenGamesController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class RetrieveOpenGamesController {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 26 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class ViewEndedGamesController {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 101 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

String specificGameUrl = "/secured/all/viewendedgames/" + idGame;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 103 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

listResponse.append("<a href=\"" + specificGameUrl + "\">View Spades Game ID # " + idGame + "</a><br/>");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 134 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for(int i = 0; i < players.size(); i++)

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 137 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

result.append("<p>Player #" + (i+1) + ": " + u.getName());

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 172 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

result.append("<p> Move " + moveCount + ": ");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 175 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewEndedGamesController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

moveCount++;

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 18 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewWinLossStatsController.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class ViewWinLossStatsController {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 72 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewWinLossStatsController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

wins += 1;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 76 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewWinLossStatsController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

losses += 1;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 83 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewWinLossStatsController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

personalResponse.append("<p> Win/Loss: " + wins + "/" + losses + "</p>");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 87 - C:\dev\java\spades\src\main\java\com\spades\spades\resources\ViewWinLossStatsController.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

othersResponse.append("<p>Statistics for " + u.getName() + " (win/loss): " + wins + "/" + losses + "</p>");

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 15 - C:\dev\java\spades\src\main\java\com\spades\spades\service\CustomUserDetailsService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class CustomUserDetailsService implements UserDetailsService {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 10 - C:\dev\java\spades\src\main\java\com\spades\spades\service\GameTimerService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class GameTimerService {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 13 - C:\dev\java\spades\src\main\java\com\spades\spades\service\GenerateGameIdService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class GenerateGameIdService {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 8 - C:\dev\java\spades\src\main\java\com\spades\spades\service\GetAuthenticationService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class GetAuthenticationService {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 17 - C:\dev\java\spades\src\main\java\com\spades\spades\service\GetCurrentPlayerInfoService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class GetCurrentPlayerInfoService {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 10 - C:\dev\java\spades\src\main\java\com\spades\spades\service\HandTimerService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class HandTimerService {

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 33 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class SpadesGameService {

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 140 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

roundnum = temp.getRoundNumber() + 1;

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 193 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

TODO: reconstruct a working game state?

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 424 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int actual1 = r.getPlayer1Actual() + 1;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 430 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int actual2 = r.getPlayer2Actual() + 1;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 476 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

player1Points += calculatePoints(roundBid1, roundActual1);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 477 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

player1Bags += calculateBags(roundBid1, roundActual1);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 482 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

player2Points += calculatePoints(roundBid2, roundActual2);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 483 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

player2Bags += calculateBags(roundBid2, roundActual2);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 487 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

player1Points -= (player1Bags / 10) \* 100;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 488 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

player2Points -= (player2Bags / 10) \* 100;

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 663 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for(int i = 0; i < players.size(); i++)

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 676 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for(int i = 0; i < players.size(); i++)

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 702 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for(int i = 0; i < players.size(); i++)

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 716 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

totalScore.set(i, accumulatedPoints + points);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 718 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

totalBags.set(i, accumulatedBags + bags);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 721 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

tableResult.append("<td>" + roundBid.get(i) + "</td>");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 722 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

tableResult.append("<td>" + roundActual.get(i) + "</td>");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 723 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

tableResult.append("<td>" + points + "</td>");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 724 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

tableResult.append("<td>" + bags + "</td>");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 733 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

for(int i = 0; i < players.size(); i++)

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 737 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

int finalPoints = rawPoints - ((numBags / 10) \* 100);

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 740 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

aggregateResults.append("<p>" + playerString + " Raw Score: " + rawPoints + ",");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 741 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

aggregateResults.append(" Total Bags: " + numBags + "<br/>\n");

**LOW: Potentially Unsafe Code - Operation on Primitive Data Type**

Line: 742 - C:\dev\java\spades\src\main\java\com\spades\spades\service\SpadesGameService.java

The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.

aggregateResults.append(playerString + " Adjusted Score (subtract bags): " + finalPoints + "\n");

**POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final**

Line: 10 - C:\dev\java\spades\src\test\java\com\spades\spades\SpadesApplicationTests.java

The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.

public class SpadesApplicationTests {