



# Smart Contract Quick Check

## Project details:

Project name:	DiamondAxs
Contract address:	<a href="#">0x8165883a81d82CB4f11B1a35e343f3F34E8537F0</a>
Contract details:	contract
Client contacts:	Not provided
Owner address:	<a href="#">0x82F0b975610f3a5981A7579b5AfaD150e54Be9b5</a>

## Audit details:

1. Compiler errors.	Passed	11. Economy model.	Passed
2. Race conditions and Reentrancy.	Passed	12. Impact of the exchange rate.	Passed
3. Delays in data delivery.	Passed	13. Private user data leaks.	Passed
4. Oracle calls.	Passed	14. Malicious Event log.	Passed
5. Front running.	Passed	15. Uninitialized storage pointers.	Not checked
6. Design Logic.	Passed	16. Arithmetic accuracy.	Not checked
7. DoS with Revert.	Passed	17. Cross-function race conditions.	Passed
8. Timestamp dependence.	Not checked	18. Scoping and Declarations.	Not checked
9. DoS with block gas limit.	Passed	19. Safe Zeppelin module.	Passed
10. Methods execution permissions.	Passed	20. Fallback function security.	Not checked

Techrate was commissioned by DiamondAxs to perform the Smart Contract quick security check and passed the **15 security issue** checks out of 20 potential. However smart contract could contain **SECURITY ISSUES** in the part that is not checked and in other smart contracts related to the project.