**🐞 BUG Report: API Security Issues in Resolution Pro**

**🔐 BUG ID 01**

* **🪪 API Endpoint**: [/v1/role](https://a5izddda32.us-east-1.awsapprunner.com/v1/role)
* **📄 Test Case 09**: *Verify token without Bearer prefix returns 401*

**✅ Expected Result**

🔁 Request with malformed token should return **401 Unauthorized**

**❌ Actual Result**

🔁 Request returned **200 OK** even without Bearer prefix

**📉 Impact**

⚠️ *Weak token format validation* — this is a **potential security vulnerability**.  
Unauthorized users may gain unintended access due to improper auth format checks.

**🛠️ Suggested Fix**

🔐 Enforce strict validation of the token format:  
**Authorization: Bearer <token>** only should be accepted.

**🔐 BUG ID 02**

* **🪪 API Endpoint**: [/v1/users](https://a5izddda32.us-east-1.awsapprunner.com/v1/users)
* **📄 Test Case 15**: *Verify token without Bearer prefix returns 401*

**✅ Expected Result**

🔁 Request with malformed token should return **401 Unauthorized**

**❌ Actual Result**

🔁 Request returned **200 OK** without proper token prefix

**📉 Impact**

⚠️ *Weak token format validation* — exposes system to **security risks**

**🛠️ Suggested Fix**

🔐 Enforce strict adherence to the **Authorization: Bearer <token>** format

**🧾 Conclusion**

🚨 These two bugs reflect a **critical lapse in token validation** across key endpoints. While they are marked with **medium severity**, the **high priority** arises from the **security risk** involved.

🔒 **Why Fixing is Crucial:**

* Protects the API from unauthorized access attempts
* Ensures consistent and secure handling of authentication tokens
* Upholds industry-standard security practices

🛡️ *Proper token validation is a first line of defense in any secure system — enforcing strict checks will significantly strengthen Resolution Pro's security posture.* 💪