Security Assessment Report

Executive Summary

During security testing, a privilege escalation vulnerability was identified in the application’s password reset workflow. The issue allows an attacker to exploit the “Forgot Password” functionality to obtain an administrator-level JSON Web Token (JWT). This enables unauthorized access to administrative API endpoints such as */api/admin/tickets*.

Steps to Reproduce

1. Trigger the 'Forgot Password' functionality using a controlled email account.
2. In Burp Suite, review HTTP history and identify the first /api call (e.g., /api/auth/forgot).
3. Replay the password reset workflow, modifying the target email to an admin account.
4. Capture the issued JWT token, which now contains the role 'admin'.
5. Use this JWT in Authorization headers to access restricted endpoints such as GET /api/admin/tickets.

Example Captured JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3QwMDIyQHZ6eXc0bnlnZzA1a3l1aHA
2Y3I5aTM1NDh2ZW0yaHE2Lm9hc3RpZnkuY29tIiwiaWQiOiI2OGJjYTllZGI4MzkxOGY4ZmMwNjg0MGIiLCJ
yb2xlIjoiYWRtaW4iLCJpYXQiOjE3NTcxOTU4MjQsImV4cCI6MTc1ODQ5MTgyNH0.YKPbUenaWgHqtpLcLv7
aor3DffRwQAKxdA72TQiwiZU
```

Impact

- Privilege Escalation: Normal users can obtain administrator rights.
- Sensitive Data Exposure: Unauthorized access to administrative APIs.
- Potential System Takeover: With full admin access, attackers may control the system entirely.

Root Cause

The password reset workflow lacks strict verification, allowing an attacker to manipulate the process and receive a JWT token with elevated privileges. This results in insecure role assignment and improper access control.

Recommendations

- Enforce strict validation on password reset workflows.
- Ensure reset links/tokens are single-use and bound to the requesting user.
- Do not allow arbitrary role escalation during token issuance.
- Implement monitoring and alerting for unusual reset requests.
- Regularly review access control mechanisms for sensitive API endpoints.