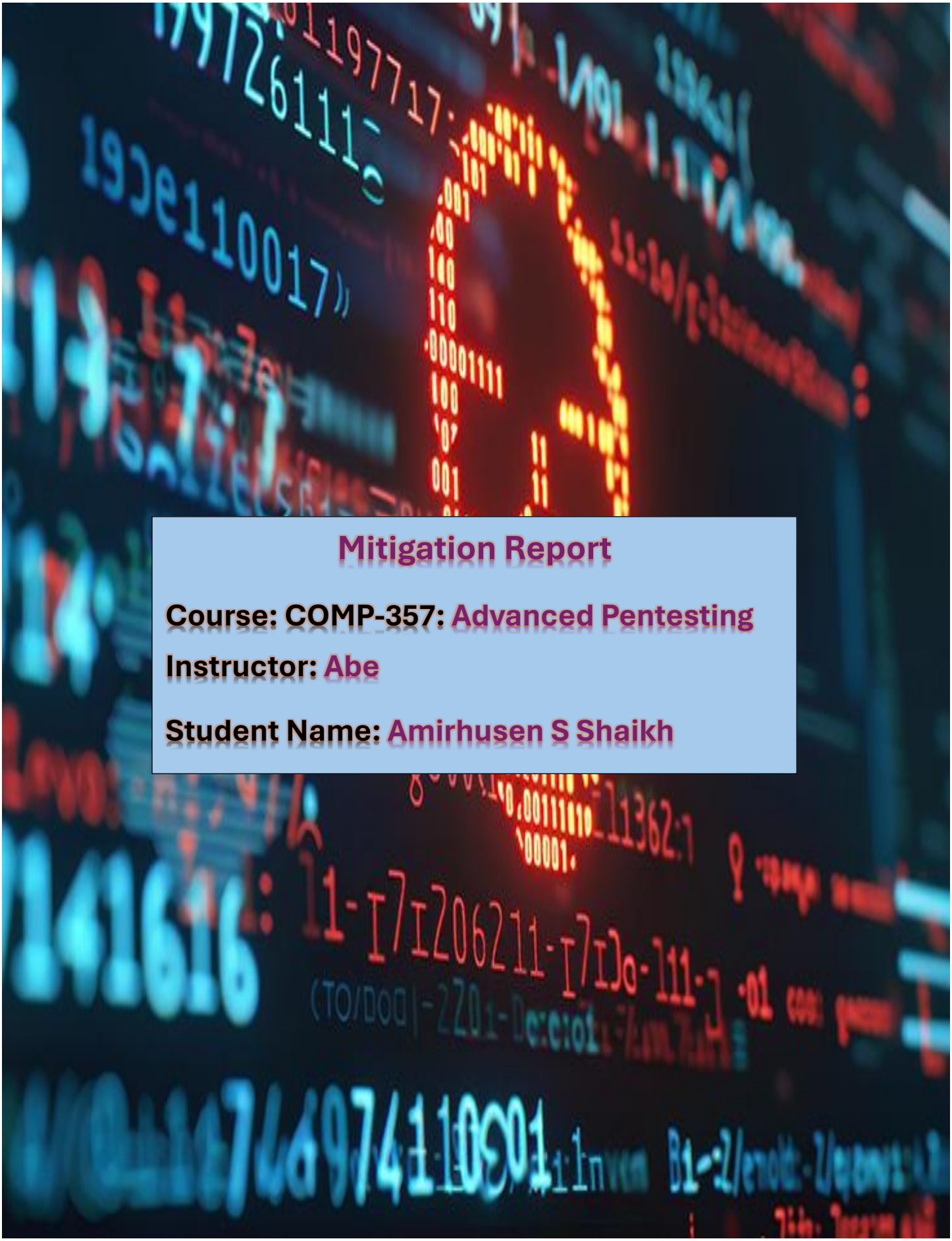

Mitigation Report

Course: COMP-357: Advanced Pentesting

Instructor: Abe

Student Name: Amirhusen S Shaikh

Introduction:

In this lab, we found that Juice Shop's Authentication system accepts the forged i.e. edited JSON web tokens(JWTs) signed with a weak secret. This allowed a normal customer account to be escalated to an admin role. Such a weakness shows how insecure token handling can lead to privilege escalation and loss of control over the application. The following mitigations steps are discussed below.

Mitigation Steps:

1. **Enforce a Single Secure Algorithm**

- Configure the application or its proxy to only accept one strong algorithm (such as **RS256**).
- Do not rely on the "**alg**" value inside the token header, since attackers can change it.

---

2. **Strengthen Key Management**

- Replace weak keys like "**secret**" with long, random values that are hard to guess.
- Store keys securely using Docker secrets or a cloud key vault.
- Rotate keys regularly to reduce the risk of compromise.

---

3. **Validate Roles on the Backend**

- Do not trust the "**role**" claim inside the token.
- Always check user roles against a backend database or identity provider before granting admin access.
- This ensures that even if a token is tampered with, the backend will not give unauthorized privileges.

4. **Use a Reverse Proxy for Token Validation**

- Place Juice Shop behind a **reverse proxy or gateway** that validates JWTs before requests reach the application.
- The proxy should reject tokens that use **insecure algorithms** or **invalid signatures**.
- This adds a protective layer without changing the application code.

---

5. **Harden the Container Setup**

- Run Juice Shop and proxy containers as non-root users.
- Use a dedicated Docker network so Juice Shop is not exposed directly to the host.
- Limit resources and disable privileged mode to reduce the attack surface.

---

6. **Enable Monitoring and Logging**

- Log failed token validations and set alerts for repeated invalid attempts.
- Regularly review logs to detect suspicious activity.
- Monitoring helps detect exploitation attempts early and supports incident response.

Conclusion

By enforcing strict algorithm rules, using strong secrets, validating roles properly, and placing Juice Shop behind a secure proxy, the JWT exploit is neutralized. These documented steps provide a clear path to mitigation, even without immediate testing, and ensure that authentication remains secure against similar attacks.