Security Evaluation: Adversarial Robustness and Privacy Protection