Lab 3

Cross Site Request Forgery (CSRF)

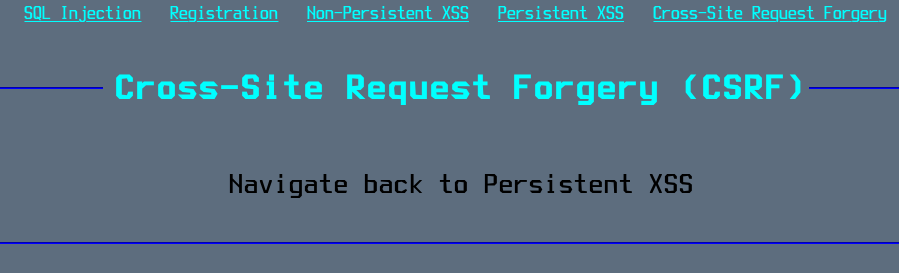
Attackers use CSRF to interact with a web service on the victim’s behalf. This type of attack is difficult for a website to identify since they seem like legitimate requests. The attacker will take advantage of the victim’s active session by tricking them into unintentionally running the attack. This can be done by redirecting the victim to a malicious website.

Part 1.

Navigate to the registration page and create a new user. (Note the password requires 8 characters, one uppercase letter, one lowercase letter, and one or more numbers)

Part 2.

Next navigate to the Cross-Site Request Forgery page.



Part 3.

Finally Navigate to Persistent XSS. You should see a comment inserted using your username. (Take a screenshot)

Questions

1. Include the screenshot from Part 3.

2. Name 2 ways that an attacker could redirect a victim to the CSRF page.