PENTEST Web: Lab 1

I Introduction

This lab will introduce Cross Site Request Forgery (CSRF) attacks.

CSRF: Tricks an authenticated user's browser into submitting unintended requests to a target application, leveraging the victim's existing credentials (cookies, session tokens, TLS client auth, etc.).

I.1 Prerequisites

For this lab, you must install or download the following tools/files:

- docker
- the lab zip file here: https://avalonswanderer.github.io/assets/zip/pentest/Labsetup_csrf.zip or the arm version here.

The lab exercises for the Web section require deploying containers and configuring DNS resolution in order to correctly resolve the site names and simulate a real-world scenario.

These environments come from seedsecuritylabs.org and have been slightly modified for the course content.

The idea is to expose the different sites on your machine's local network (10.9.0.0/24) and to define the IP/URL mappings in the static resolution file.

Steps to do:

1. Modify your configuration to add the static mapping of the URLs used for the exercises. This configuration should be added to the /etc/hosts file on Linux (or on Windows: C:\Windows\System32\drivers\etc\hosts):

```
10.9.0.5    www.seed-server.com
10.9.0.5    www.example32.com
10.9.0.105  www.attacker32.com
```

2. Unzip the archive and build the docker files using:

```
$ docker compose build
```

3. To start the dockers use the following:

```
$ docker compose up
```

4. Once you've finished the lab, you can turn off the dockers:

```
$ docker compose down
```

II CSRF attacks

Start the dockers and visite the URL http://www.seed-server.com. You can connect with the account of Alice (alice:seedalice).

II.1 CSRF on GET service

By inspecting HTTP request, find out what a "Add Friend" request looks like (you can use the build in inspector or extension like HTTP Header Live).

Question 1: How could you use a CSRF to make Alice add friend unwillingly?

- Do it by modifying the attacker-controlled Lab_CSRF/attacker/addfriend.html page.
- Test your attack by visiting the website http://www.attacker32.com with Alice's browser.

Tips

- You might need to disable cross-site cookie isolation (about:preferences#privacy)

II.2 CSRF on POST service

By inspecting HTTP request, find out what a "Edit Profile" request looks like.

Question 2: How could you use a CSRF using a POST form to make Alice edit her profile?

- Do it by modifying the attacker-controlled Lab_CSRF/attacker/editprofile.html page.
- Test your attack by visiting the website http://www.attacker32.com with Alice's browser.

II.3 Bonus

Try to flag the challenges CSRF - 0 protection.

Acknowledgements

This work is inspired by seedlabs and the book *Internet Security: A Hands-on Approach, 3rd Edition,* by Du Wenliang.