PENTEST Web: Lab 2

I Introduction

This lab will introduce Cross Site Scripting (XSS) attacks.

XSS: Injects malicious scripts into a trusted application's output, causing a victim's browser to execute attacker-controlled code. This allows the adversary to access or manipulate data within the affected page, impersonate the user in the application's context, or alter the page's behaviour without the user's intention.

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_xss.zip or the arm version here.

As the previous lab exercises, we need to deploy containers and configure 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:

```
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
```

I.1.1 For MacOS users

- Install VMWare Fusion here, you will need to create a Broadcom free account and select personal use after installation.
- Once downloaded, follow this tutorial to install a Ubuntu VM server (the GUI will be downloaded too after).

- Once logged in, install docker for Ubuntu and setup the lab as above.

I.1.2 For those with Docker issues but not on MacOS

- You can use the prebuilt Ubuntu VM from seedlab: download link.
- Once downloaded and unzip, you can create a new linux machine on VirtualBox without any ISO, setup the CPU and RAM, and select the VDI from the archive.
- Log in, and download the lab archive on the website.

```
login: seed
password: dees
```

II XSS attacks

Start the dockers and visite the URL http://www.seed-server.com.

II.1 XSS on GET service

1. Go to http://www.seed-server.com and login as a user Samy.

```
login: samy
password: seedsamy
```

2. Identify the content of the "Add friend" request, and how to access relevant elements.
3. Construct the url corresponding to the action of adding Samy to your friend.
4. Find a way to upload on a page of the webserver the following template, modified by yourself, so that any user vsiting the page automaticaly adds Samy as a friend.

```
<script type="text/javascript">
    window.onload = function () {
        var Ajax=null;
        var ts="&__elgg_ts=" + ...; //FILL IN
        var token="&__elgg_token=" + ...; //FILL IN
        //Construct the HTTP request to add Samy (id = 59) as a friend.
        var sendurl="...";  //FILL IN

        //Create and send Ajax request to add friend
        Ajax=new XMLHttpRequest();
        Ajax.open("GET", sendurl, true);
        Ajax.send();
}
</script>
```

5. Connect with another user and visit Samy's profile to trigger your script.

Question 1: What are the elgg_ts and elgg_token? What is their purpose?

II.2 XSS on POST service

Now, you will perform an XSS using a POST request to send more complexe arguments (from forms) to the server.

1. Go to http://www.seed-server.com and login as a Samy.
2. Identify the content of the "Edit Profile" request, and how to access relevant elements.
3. Construct the url corresponding to the action of editing the profile of the logged user to change the description to anything you want.
4. Find a way to upload on a page of the webserver the following template, modified by yourself, so that any user vsiting the page automaticaly edit their profile.

```
<script type="text/javascript">
  window.onload = function () {
    var guid = ; // FILL THIS
    var name = ; // FILL THIS
    var ts = "&__elgg_ts=" + ...; // FILL THIS
    var token = "&__elgg_token=" + ...; // FILL THIS
    var description = ; // FILL THIS
    //Construct the HTTP request to add Samy as a friend.
    var sendurl = "http://www.seed-server.com/action/profile/edit"
    var content = ; // FILL THIS
    // We don't want our attack to affect Samy
    if (elgg.session.user.guid != 59) {
      var Ajax = null;
      Ajax = new XMLHttpRequest();
      Ajax.open("POST", sendurl, true);
      Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
      Ajax.send(content);
    }
}
</script>
```

5. Connect with another user and visit Samy's profile to trigger your script.

II.3 Bonus

Try to flag the challenges XSS - Stored 1.

Acknowledgements

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