CS3511 - P4 - CROSS-SITE SCRIPTING (XSS) AND CLIENT SIDE

Overview

In this practical we are looking at Cross-Site Scripting (XSS). The aim is to explore Cross-Site Scripting and to see how it can be applied. As usual, the aim of this practical is not to teach you how to become a hacker, instead it is the aim to understand what hackers do so that you can implement appropriate defence methods. Use the tools and environments provided for this practical; do not attempt XSS attacks on existing web services!

We will also look at bypassing front-end restrictions, client side filtering and HTML tampering.

In this practical we use again *WebGoat* which has been used as well in previous practicals. A web browser is required for this practical.

WebGoat

From the WebGoat's description page: WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components. Now, while we in no way condone causing intentional harm to any animal, goat or otherwise, we think learning everything you can about security vulnerabilities is essential to understanding just what happens when even a small bit of unintended code gets into your applications. What better way to do that than with your very own scapegoat? Feel free to do what you will with him. Hack, poke, prod and if it makes you feel better, scare him until your heart's content. Go ahead, and hack the goat. We promise he likes it. Thanks for your interest! The WebGoat Team.

For this practical WebGoat is installed on the server X.X.X.X on port 8080. Using a web browser you can navigate to *http://X.X.X.X:8080/WebGoat/* to interact with the service. As a first step you have to create an account by providing a username and password. After logging in you will be provided with a bunch of hacking exercises. In this practical we will look at a subset of these exercises as explained later.

PART1: Introduction

This part is only required if you have not used WebGoat in any of the previous practicals.

Use a web browser to navigate to WebGoat: *http://X.X.X.X:8080/WebGoat/*. Create an account on the system by providing a username and password.

Navigate to the *Introduction* section and read about WebGoat.

PART2: Cross Site Scripting

Navigate to the *Cross Site Scripting* section and in there to the subsection *Cross Site Scripting*.

Complete the 12 lesson steps....

PART3: Client Side

Navigate to the *Client Side* section and in there to the subsection *Bypass front-end restrictions*.

Complete the 3 lesson steps....

PART4: Client Side

Navigate to the *Client Side* section and in there to the subsection *Client side filtering*.

Complete the 3 lesson steps....

PART5: Client Side

Navigate to the *Client Side* section and in there to the subsection *HTML tampering*.

Complete the 3 lesson steps....

CS3511 Continuous Assessment - PART 4

Please submit an answer to the following question with your CS3511 Continuous Assessment. Your answer should not be longer than half a page (You can use figures or code pieces to illustrate your answer).

Question P4 [2 MARKS]: XSS

Explain the difference between a *stored* Cross-Site Scripting attack and a *reflective* Cross-Site Scripting attack.