CS3511 - P1 - WEBGOAT

Overview

In this practical we are setting up WebGoat and examine basic HTTP communication and cryptography. In this practical a number of tools will be used: *WebGoat*, *WebWolf*, *ZAP* and the web debugging/developer features of *Chrome/Firefox/Safari*. The tools can be used for hacking and you are only to use the tools for the exercises described here; do not test the tools abilities with other servers! What are the tools?

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.

WebWolf

From the WebWolf's description page: Some (WebGoat) challenges requires to have a local web server running. WebWolf is for you the attacker it helps you while solving some of the assignments and challenges within WebGoat. An assignment might for example require you to serve a file or connect back to your own environment or to receive an e-mail. In order to not let you run WebGoat open and connected to the internet we provided these tools in this application, called WebWolf.

For this practical WebWolf is installed on the server X.X.X.X on port 9090 (Both, WebGoat and WebWolf are local installations which can be reached from the machines in the lab but not from the wider Internet).

ZAP

ZAP is very similar to Burp and it is used as proxy for this lab.

From the ZAP's description page: The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers. It can help you automatically find security vulnerabilities in your web applications while you are developing and testing your applications. Its also a great tool for experienced pentesters to use for manual security testing.

If you want to use ZAP you have to install it on your machine. You can obtain it here: https://www.zaproxy.org/download/ (The cross platform core). You can run zap.sh to install the program in user space (for example, into /tmp).

PART1: Introduction

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 and WebWolf.

Use your web browser and open a second tab/window and connect to WebWolf using the link *http://X.X.X.X:9090/WebWolf/*

Complete the 4 WebWolf lesson steps.

PART2: HTTP Basics

Navigate to the *General* section and in there to the subsection *HTTP basics*.

Complete the 3 HTTP Basics lesson steps. To do so you would need to enable the web developer tools in your browser.

PART3: HTTP Proxies

Navigate to the *General* section and in there to the subsection *HTTP proxies*.

Complete the 10 HTTP Proxies lesson steps. The lesson here assumes that you use ZAP and explains in detail setup and use of the tool.

PART4: Developer Tools

Navigate to the *General* section and in there to the subsection *Developer Tools*.

Complete the 6 lesson steps. The lesson is specifically written for Chrome. However, you can also use Firefox, the same development features can also be found in this browser.

PART5: CIA Triad

Navigate to the *General* section and in there to the subsection *CIA Triad*.

Complete the 5 lesson steps.

PART6: Crypto Basics

Navigate to the *General* section and in there to the subsection *Crypto Basics*.

Complete the first 6 lesson steps.

CS3511 Continuous Assessment - PART 1

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 P1 [2 MARKS]: Password Guessing

An application requires a password to log in. The password policy is: 1) the password must be 6 to 8 characters in length 2) passwords must use alphabetic and numeric characters 3) passwords must have at least one alphabetic and one numeric character 4) letters are case sensitive. How many different passwords exist? Describe how you got to your result.