Cyber Security and Ethical Hacking Program

Web Application Source Code Vulnerability Analysis

2. Web Application Source Code Vulnerability Analysis

Introduction

How do you perform a source code review to find vulnerabilities in web applications?

Reviewing code is probably the best way to find vulnerabilities in a web application. It's a lot faster than black-box testing, and it helps you learn how to program safely in the future by observing the mistakes of others. Auditing code is also a great way.

Requirement

A student should have a basic understanding of how code works and explore the source code of a website (HTML, CSS, and JAVA).

Goals

The goal is to identify information through sources and find the clues to complete the task.

Lab 1

The CEO of Saturn Inc. has hired you to find the bugs on the website. One of the developers was mischievous and hid confidential information in the nooks and corners of the website. The website has hidden elements that ultimately reveal too much information. The higher authorities of the company have identified the following code to have a "bad smell". You are tasked to identify the hidden path and traverse it to find the information. The developer was removed from the company and a chit was found on the desk which has the following:

"You think you got good security. Check something about Saturn and you'll know who you are. Take the next step and view what the source says. Once you connect with your source the secrets will reveal themselves once you use them in your Universal Resource Locator. Felt happy? not long. Your source might be getting this information from some other source. Huh? Confused already? Think.

Many hidden mysteries revolve around this office. Hey Mr. CEO want some hidden source? and that when he will sweat profusely because there are some Super Hidden acts of Mr. CEO.

Ah, finally some smart brains. But will you be able to get the access code that runs the Production Server? Or will it be gone with my source?"

Topic_2_lab.zip

Let's download the file from this URL: file:///C:/Topic%202%20Lab%202/Topic%202%20Lab%202/index.html

Note

1. The below-shown URL path is a reference and directly clicking them might show errors because the local path of your personal computer might vary.
2. The candidate is requested to extract the file "Topic_2_lab.rar" in the C drive.

Hints

1. folders folders folders
2. The Source code can be viewed to get hints on the secret path.

Lab 2

ctf.zip

- Copy the attached file to the C drive and extract it.
- You should find a folder called “CTF“.
- Inside double-click on main.html.
- There are 5 hyperlinks according to each level.

Hint for level 4

Robots.txt:

A robots.txt file tells search engine crawlers which URLs the crawler can access on your site.

Hint for level 5

- **Base64=**It is a type of encoding.
- Kali has an inbuilt command to encode and decode base64 strings

Example: `echo 'bGludXhoaW50LmNvbQo=' | base64 --decode`