LAB08B: Bypassing addslashes

[Simon X. Camilo. Cybersecurity Student]

[BHCC CIT-275-WB Professor Philip Kazanjian]

note: I messed up and deleted my previous intro, the intro here is for 9b, the rest is from 7b

Introduction

The addslashes(string) is a filter that prevents attackers from running malicious code that have quotes in it. This filter makes it impossible for an attacker to perform the most effective methods of damage against the visitors of the site. This document shows that the filter does not protect against all kinds of malicious attacks.

Addslashes can be seen in effect in image 1. After entering the malicious script “<script>Alert(‘Owned’)</script>”, nothing is posted and no alert is seen. The code appears with slashes in the html, as seen in image 2.

  
**Image 1**

*Code is not posted on the website*

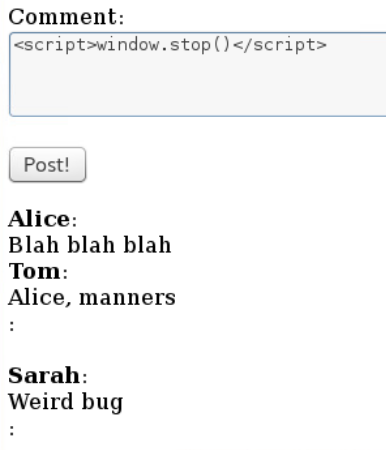
****Image 2**

*Code in html is canceled with start and end slashes.*

# Analysis

It is impossible to run a script such as <script>Alert(‘Owned’)</script>, and any script that contains quotes. But there are still some scripts that can be run to attack the website, such as <script>window.stop()</script>.

Window.stop will stop the website from loading further after the script is executed. This makes the site unusable to users, because users can no longer submit more posts to the site, and it can also be used to maintain the employees busy. After entering the script “window.stop()” in the site, image 3 shows that there are no new posts submitted after running the script, but image4 shows that users had attempted to leave posts on the site, they are just not displayed outside of the html source page.

  
**Image 3**

*script was executed and new posts are not shown.*

  
**Image 3**

*The html source shows that there are new posts that are not visible outside of the html source page.*

# Conclusion

Add\_slashes can be very effective against the common methods of attacks used, and heavily limits what an attacker can do with a website, but it’s not foolproof method. The scripts that are still available allows for an attacker to make the site unavailable among other things that could damage the website. Using a function that’s efficient is not enough, it’s recommended to use a function that is foolproof or that even with knowledge, can make it difficult to exploit the site.

References

Addslashes. (2001, April 13). Retrieved March 03, 2021, from <https://www.php.net/manual/en/function.addslashes.php>

The window object. (2009, October 16). Retrieved March 02, 2021, from <https://www.w3schools.com/jsref/obj_window.asp>