LAB04B: Working around the str\_ireplace(script, null, ) function to create alerts and run scripts.

[Simon X. Camilo. Cybersecurity Student]

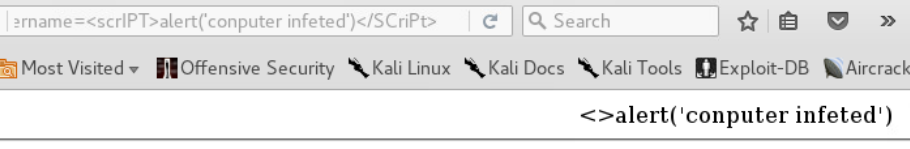
[Redacted]

# Introduction

str\_ireplace(script, null, ) is a function that is disallowing html from displaying an alert box, by removing any kind of script that is inserted into the url. This document tries to find ways to bypass this so we can have an alert on the webpage, or run any kind of script.

**What is str\_ireplace?**

str\_ireplace does the same thing as str\_replace, but case insensitive. This allows people to protect themselves against an easy way to bypass the str\_replace function, which is to use different cases



A demonstration of how this function works can be seen on the screenshot above. In this case, the function is str\_ireplace(script, null, $\_REQUEST[‘myusername’]). This make it so when the url above is entered even if the cases had been changed. Instead of showing an alert box, the only thing that’s shown is the name of the variable.

The page source also shows that it’s not there anymore, it has been replaced with null (which means nothing), it has been erased. This is how str\_ireplace works.

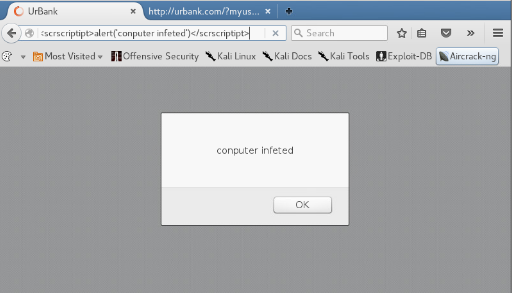


# Analysis

### Bypass: Writting **script** before and after **script**

The wording is confusing. A better way to explain this, is that we should type scrscriptipt instead of script. The word script that’s in the middle will be erased, making the other letters besides it combine and show the word script. This method has a lot of variations, which makes it hard to bypass by using str\_replace.

A demonstration of it is shown below. Typing urbank.com/?myusername=<scrscriptipt>alert(‘conputer infeted’)</scrscriptipt> in the url will show our alert box



# Conclusion

str\_replace is one of the most basic and most ineffective methods of mitigation, and it can be easily worked around by most hackers with a basic understanding of sql injection. It’s important to use more efficient methods to protect against these types of attacks, instead of relying on this function.

# Citations

Str\_ireplace. (n.d.). Retrieved February 22, 2021, from https://www.php.net/manual/en/function.str-ireplace.php

Bypassing str\_replace. (n.d.). Retrieved February 22, 2021, from https://www.sevenlayers.com/index.php/328-bypassing-str-replace