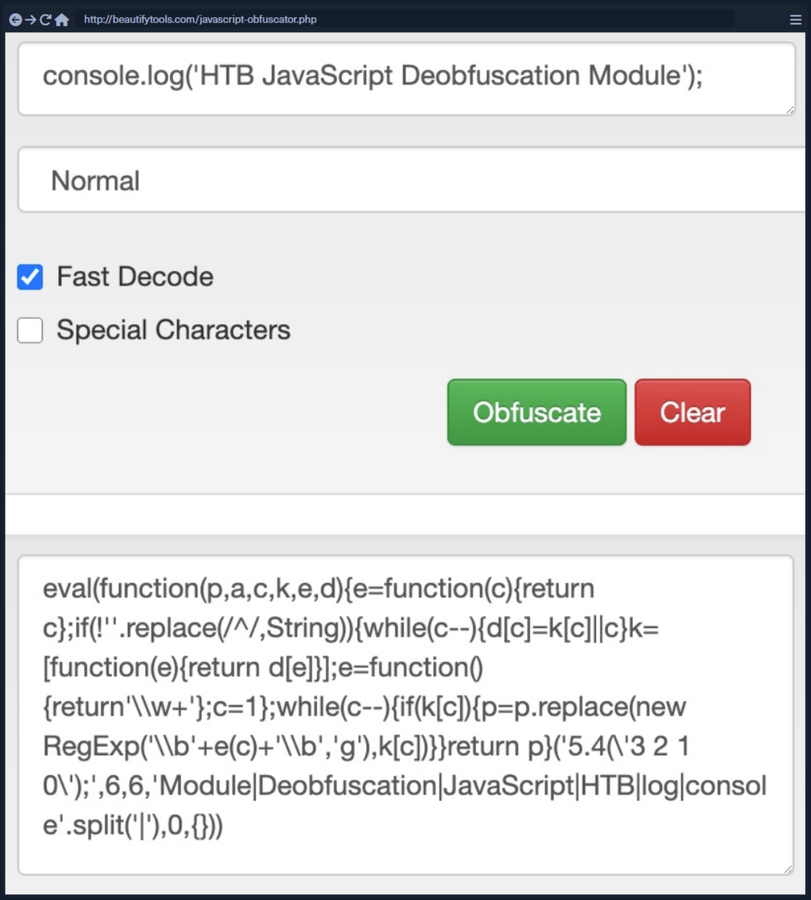
Code Obfuscation

Before we start learning about `deobfuscation`, we must first learn about `code obfuscation`. Without understanding how code is obfuscated, we may not be able to successfully deobfuscate the code, especially if it was obfuscated using a custom obfuscator.

What is obfuscation

Obfuscation is a technique used to make a script more difficult to read by humans but allows it to function the same from a technical point of view, though performance may be slower. This is usually achieved automatically by using an obfuscation tool, which takes code as an input, and attempts to re-write the code in a way that is much more difficult to read, depending on its design.

For example, code obfuscators often turn the code into a dictionary of all of the words and symbols used within the code and then attempt to rebuild the original code during execution by referring to each word and symbol from the dictionary. The following is an example of a simple JavaScript code being obfuscated:



http://beautifytools.com/javascript-obfuscator.php

```
console.log('HTB JavaScript Deobfuscation Module');
```

Normal

☑ Fast Decode

☐ Special Characters

```
eval(function(p,a,c,k,e,d){e=function(c){return
c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=
[function(e){return d[e]}];e=function()
{return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('5.4(\'3 2 1
0\');',6,6,'Module|Deobfuscation|JavaScript|HTB|log|consol
e'.split('|'),0,{}))
```

Codes written in many languages are published and executed without being compiled in `interpreted` languages, such as `Python`, `PHP`, and `JavaScript`. While `Python` and `PHP` usually reside on the server-side and hence are hidden from end-users, `JavaScript` is usually used within browsers at the `client-side`, and the code is sent to the user and executed in cleartext. This is why obfuscation is very often used with `JavaScript`.

Use Cases

There are many reasons why developers may consider obfuscating their code. One common reason is to hide the original code and its functions to prevent it from being reused or copied without the developer's permission, making it more difficult to reverse engineer the code's original functionality. Another reason is to provide a security layer when dealing with authentication or encryption to prevent attacks on vulnerabilities that may be found within the code.

`It must be noted that doing authentication or encryption on the client-side is not recommended, as code is more prone to attacks this way.`

The most common usage of obfuscation, however, is for malicious actions. It is common for attackers and malicious actors to obfuscate their malicious scripts to prevent Intrusion Detection and Prevention systems from detecting their scripts. In the next section, we will learn how to obfuscate a simple JavaScript code and attempt running it before and after obfuscation to note any differences.

← Previous Next →

Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction

Obfuscation

Deobfuscation Examples

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left