Bryce Loftin

Computer Science - Morriss

2/3/2020

Code Injection

A code injection is a type of injection cyber attack that involves an attacker intputing or injecting unauthorized application and usually malicious code into a program. That program is then altered and subsequently does not execute or executes its purpose incorrectly. Code injection attacks are one of the most dangerous attacks because the attacker can make the program do a number of harmful things such as access sensitive data, delete important data, deny access and even fully shut down their own system. Not only that, but these types of attacks are also very common. This is because the possible targets are endless with the millions of networks and websites now a part of the internet. This attack happens to all kinds of websites, programs and networks. Anything that uses code is vulnerable to it. There are many variations of code injection but the most common and most dangerous are Cross-site scripting (XSS) and SQL injection (SQLi).It isn’t known where this type of attacks came from or who created it because of how incredibly illegal most the uses of it are.Unfortunately, because of the stealthy nature of injection attacks they are hard to catch before their purpose is carried out. Once the malicious code has served its purpose it is usually fairly easy to find depending on its nature. Attacks that cause obvious and usually worse damage like system shut-downs and bank account infiltrations are easily found while more benign code is only found after a thorough review of the site’s code or by running a malware detector.Code injection attacks both the server and the client. It first alters the server for whatever malicious purpose it exists, then it attacks the client in a variety of ways depending on what variation of code injection it is. XXS specifically alters a website by injecting harmful javascript into a legitimate website’s code which is then activated when another user visits the site. For example, if a site has a comment function to receive feedback from users, a hacker could find a flaw in the website’s security protocols and enter a command that would redirect other users to a forgery of the same website and possibly get sensitive information from them. In SGLi attacks, however, an attacker would modify a site that receives user input and compares it to a database in order to gain access to more restricted parts of the site. For example, if a site such as PayPal takes an account number and password the attacker could modify the execution of the database comparison to either not bother comparing the password or to accept some arbitrary credentials, both of which would allow the hacker access.Depending on what the injection specifically focuses on, the damage done can range from juvenile and insignificant to career ending. Effects include exposing private information, draining bank accounts, taking out loans as a different person, proving a company or more specifically a bank untrustworthy, etc. For example in a XSS attack user could be redirected to an identical side and be lured into entering private information in the input line when in reality they are handing that information over to the attacker. In theory, although it would be nearly impossible, this form of attack could give someone access to government databases with highly classified information such as politicians’ financial records or even nuclear launch codes.There are, however, many ways to prevent or at least try to prevent these attacks. One precaution that many systems use is to encode any input before allowing it to be received. This makes it harder for a hacker to implement a program that would copy or steal that inputted data such as usernames, passwords, or bank accounts. Another fix that is used is input validation which prevents many code injections by recognizing malicious input data and immediately rejecting it. On top of that, some programs even have what is called Canaries which are randomly placed values in a stack of code. When the program is run, these values are checked and if they have been altered, the program stops execution. NX bits can also be used to store databases such as members’ usernames and passwords as non-executable and therefore much harder to alter. Another defense against, specifically SQL injections, is to have stored procedures and code with a failsafe that stops execution of a program if it is compiled and the code has been altered.

It’s hard to do anything as users to prevent against this form of cyberattacks because of the seemingly legitimate nature of it. The most one could do is simply be aware of unusual domain names or strange looking websites.