Team Activity

Discussion: What is a programming language?

You should read Chapter 2,6,7,8 of the course text (Pillai, 2017) and Cifuentes & Bierman (2019) and then answer the questions below, adding them as evidence to your e-portfolio.

1. **What factors determine whether a programming language is secure or not?**

   According to Poll (2019), a programming language is secure if it offers features such as

   - memory safety and typing, as offered by "safe programming" languages. Safe programming languages are languages that have safe program fragments (fragments that do not cause untrapped errors to occur (Cardelli, 1996).

   - language mechanisms to enforce various forms of access control (such as sandboxing), similar to access control traditionally offered by operating systems.

   - mechanisms that go beyond what typical operating systems do, such as information flow control. It takes into account source of data and where it may flow to.

   Cifuentes and Bierman (2019) notes that any language that offers good support for the three main categories of security vulnerabilities, according to the National Vulnerability Database can be considered secure. Those vulnerabilities are:

   Buffer Errors

   Injection Errors : crosssite scripting (XSS), SQL injection, code injection, and OS command injection

   Information leak errors

2. **Could Python be classed as a secure language? Justify your answer.**

   No

   Based on

   Cifuentes and Bierman's (2019), requirements of a secure programming language, none of the top 10 mainstream languages can be considered as secure.

   Buffer Errors in Python

Pillai (2017) mentions buffer overflow errors as one of the security vulnerabilities of Python. xrange() and len() are example of Python
functions prone to integer overflow errors

Injection Errors in Python

"Code injection is a risk with languages that execute or interpret script because of the ease of running a string as an executable statement or statements at runtime (commonly called "eval"). For example, popular languages that have this ability include: JavaScript, Perl, Python, and Ruby." (Kohnfelder et al., 2019)

These Python functions are prone to injection attacks:

- exec(string) # dynamic execution of Python code
- eval(string) # returns the value of an expression or code object
- execfile(string) # reads & executes Python script from a file
- input(string) # equiv to eval(raw_input()) before Python 3000 only
- compile(string) # compile the source string into an executable object

Information Leak Errors in Python

Certain libraries are vulnerable to information leakage (Veracode, n.d)

3. Python would be a better language to create operating systems than C. Discuss.

References

Cardelli, L. (1996) Type systems. ACM Computing Surveys (CSUR), 28(1)"263-264.

Cifuentes, C. and Bierman, G. (2019) What is a Secure Programming Language? In 3rd Summit on Advances in Programming Languages (SNAPL 2019). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Veracode (n.d) Vulnerability Database Available from: https://sca.analysiscenter.veracode.com/vulnerability-database/search#query=language:python [Accessed 25 August 2021]

Kohnfelder L., Heymann E., Miller B.P., (2019) Code Injections. *Introduction to Software Security* Available from: https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/Chapters/3_8_3-Code-Injections.pdf [Accessed 25 August 2021]

Pillai, A.B. (2017). Software architecture with python. Packt Publishing Ltd.

Poll, E. (2019) Language-based Security. Available from: https://www.cs.ru.nl/~erikpoll/papers/language_based_security.pdf [Accessed 23 August 2021]