# Programming language concepts

# What is ReDOS and what part do 'Evil Regex' play?

ReDOS (Regular Expression Denial of Service) is a vulnerability that can occur when using certain patterns called regular expressions to match and manipulate text (Weidman, n.d.). 'Evil Regex' refers to malicious regular expressions intentionally designed to exploit this vulnerability. They can cause regular expression processing to take an excessively long time, potentially leading to denial-of-service attacks on applications (Larson, 2018).

# What are the common problems associated with the use of regex? How can these be mitigated?

Common problems with regular expressions include:

* Performance issues: Some regular expressions can be slow and inefficient, affecting the speed of processing (Larson, 2018).
* Complexity and readability: Regular expressions can become complex and hard to understand, making them difficult to maintain and prone to bugs.
* Vulnerabilities: If regular expressions are not crafted carefully, they can be vulnerable to attacks like ReDOS (Weidman, n.d.). To mitigate these problems:
* Optimise regular expressions: Simplify and optimize regular expressions to improve performance.
* Test and validate inputs: Before using regular expressions, validate and test inputs to prevent unexpected behaviour and vulnerabilities.
* Use appropriate tools: Employ tools designed for working with regular expressions to analyse and optimize their usage.

# How and why could regex be used as part of a security solution?

Regular expressions can be used in security solutions in the following ways:

* Input validation: Regular expressions help validate and sanitize user inputs, preventing injection attacks or unexpected behaviour.
* Pattern matching: They can identify patterns in data, helping to detect malicious code, sensitive information leaks, or security-related events (Jaiswal, 2020).
* Log analysis: Regular expressions can search and extract specific information from logs, aiding incident response and threat hunting.
* Firewall and IDS rules: Regular expressions are used to define rules for firewalls and intrusion detection systems (IDS) to identify and block malicious traffic patterns (Larson, 2018).

References:

* Jaiswal, S. (2020). Python Regular Expression Tutorial.
* Larson, E. (2018). Automatic Checking of Regular Expressions. 18th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM).
* Weidman, A. (n.d.). Regular expression Denial of Service - ReDoS.