Unit 4: Programming Language Concepts

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

ReDOS is a denial of service attack in which a poorly implemented regex is exploited in a system to divert resources from legitimate users (Davis, 2019). Evil Regexes contain some characters which when used in a code can make the system susceptible to attack (Weidman, n.d).

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

According to (Larson, 2018), some common problems associated with use of regex include:

- Bad regular expressions could be exploited by an attacker to crash a system
- Failure of compilation of some regexes: for example, unbalanced parentheses would cause a failure but unbalanced braces will not.
- Some symbols have different meanings in different situations: for example, '^' could mean negation or the start of a string. This could cause confusion

Mitigations

Use of tools for checking Regex errors. Examples include:

EGRET Tool: which takes a regex as input and generates a test string that exposes some common programming errors (Larson and Kirk, 2016)

ACRE tool: Use of Automatic Checking of Regular Expression (ACRE) tool which focuses on common mistakes in regular expressions

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

For user input validation: improper input validation can expose a system to all forms of injection attacks including cross site scripting (XXS), sql injection, buffer overflow and XML external entity attacks (Banach, 2020)

References

Banach Z. (2020) Input Validation Errors: The root of all evil in web applications. Available from: https://www.netsparker.com/blog/web-security/input-validation-errors-root-of-all-evil/ [Accessed 03 September 2021]

Davis, J.C. (2019) August. Rethinking Regex engines to address ReDoS. In Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering: 1256-1258

Larson, E. (2018) September. Automatic checking of regular expressions. In 2018 IEEE 18th International Working Conference on Source Code Analysis and Manipulation (SCAM) :225-234. IEEE.

Larson, E. and Kirk, A. (2016), April. Generating evil test strings for regular expressions. In 2016 IEEE International Conference on Software Testing, Verification and Validation (ICST) :309-319. IEEE.

Weidman A. (n.d) Regular Expression – Denial of Service. Available from: https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS [Accessed 02 September 2021]