November 9, 2021, 1:46 AM System Activated Regex lookahead assertions should not be contradictory Severity set to Critical

Dynamically executing code is security-sensitive Severity set to Critical

Reluctant quantifiers in regular expressions should be followed by an expression that can't match the empty string Severity set to Major

Regular expressions should not be too complicated Severity set to Major

- Parameter maxComplexity set to 20

Repeated patterns in regular expressions should not match the empty string Severity set to Minor

Character classes should be preferred over reluctant quantifiers in regular expressions Severity set to Minor

Regex alternatives should not be redundant Severity set to Major

Alternatives in regular expressions should be grouped when used with anchors Severity set to Major

Character classes in regular expressions should not contain the same character twice Severity set to Major

November 9, 2021, 1:45 AM System Activated Unicode Grapheme Clusters should be avoided inside regex character classes Severity set to Major

Single-character alternations in regular expressions should be replaced with character classes Severity set to Major

Regex boundaries should not be used in a way that can never be matched Severity set to Critical

`str.replace` should be preferred to `re.sub` Severity set to Critical

Using shell interpreter when executing OS commands is security-sensitive Severity set to Major

October 27, 2021, 3:04 AM System Deactivated HTTP response headers should not be vulnerable to injection attacks
October 27, 2021, 3:04 AM System Activated HTTP responses should not be vulnerable to session fixation Severity set to Blocker

April 30, 2021, 7:00 AM System Updated Encryption algorithms should be used with secure mode and padding scheme Severity set to Critical

Cryptographic key generation should be based on strong parameters
Severity set to Critical

Weak SSL/TLS protocols should not be used Severity set to Critical

March 3, 2021, 1:13 AM System Activated Setting loose POSIX file permissions is security-sensitive Severity set to Major

March 3, 2021, 1:13 AM System Updated Insecure temporary file creation methods should not be used Severity set to Critical

March 3, 2021, 1:13 AM System Activated Cipher Block Chaining IVs should be unpredictable Severity set to Critical

March 3, 2021, 1:13 AM System Updated Formatting SQL queries is security-sensitive Severity set to Major

March 3, 2021, 1:13 AM System Activated Using non-standard cryptographic algorithms is security-sensitive Severity set to Critical

JWT should be signed and verified Severity set to Critical

Allowing both safe and unsafe HTTP methods is security-sensitive
Severity set to Minor

September 1, 2020, 6:05 AM System Deactivated Using regular expressions is security-sensitive
September 1, 2020, 6:05 AM System Updated Class names should comply with a naming convention Severity set to Minor

- Parameter format set to ^_?([A-Z_][a-zA-Z0-9]*|[a-z_][a-z0-9_]*)$

Method names should comply with a naming convention
Severity set to Minor

- Parameter format set to ^[a-z_][a-z0-9_]*$

Functions, methods and lambdas should not have too many parameters
Severity set to Major

- Parameter max set to 13

September 1, 2020, 6:05 AM System Activated Type checks shouldn't be confusing Severity set to Major

September 1, 2020, 6:05 AM System Updated Function names should comply with a naming convention Severity set to Major

- Parameter format set to ^[a-z_][a-z0-9_]*$

September 1, 2020, 6:05 AM System Activated Function return types should be consistent with their type hint Severity set to Major

September 1, 2020, 6:04 AM System Activated Values assigned to variables should match their type annotations Severity set to Major

June 30, 2020, 5:24 AM System Activated Operators should be used on compatible types Severity set to Blocker

XML parsers should not be vulnerable to XXE attacks
Severity set to Blocker

Calls should not be made to non-callable values Severity set to Blocker

Item operations should be done on objects supporting them
Severity set to Blocker

June 30, 2020, 5:23 AM System Activated Iterable unpacking, "for-in" loops and "yield from" should use an Iterable object Severity set to Blocker

June 16, 2020, 7:32 AM System Deactivated Reading the Standard Input is security-sensitive
Using command line arguments is security-sensitive
Sending emails is security-sensitive
June 16, 2020, 7:32 AM System Activated String formatting should not lead to runtime errors Severity set to Blocker

June 16, 2020, 7:32 AM System Deactivated Encrypting data is security-sensitive
June 16, 2020, 7:32 AM System Activated The "open" builtin function should be called with a valid mode Severity set to Blocker

Implicit string and byte concatenations should not be confusing Severity set to Major

String formatting should be used correctly Severity set to Major

Only defined names should be listed in "__all__" Severity set to Blocker

Builtins should not be shadowed by local variables Severity set to Major

June 16, 2020, 7:31 AM System Activated Only strings should be listed in "__all__" Severity set to Blocker

May 27, 2020, 5:47 AM System Activated Function arguments should be passed only once Severity set to Blocker

Expressions creating dictionaries should not have duplicate keys Severity set to Major

Expressions creating sets should not have duplicate values Severity set to Major

Loops without "break" should not have "else" clauses Severity set to Major

Wildcard imports should not be used Severity set to Critical

Return values from functions without side effects should not be ignored Severity set to Major

Identity comparisons should not be used with cached typed Severity set to Major

Constants should not be used as conditions Severity set to Critical

New objects should not be created only to check their identity Severity set to Major

Non-empty statements should change control flow or have at least one side-effect Severity set to Major

- Parameter reportOnStrings set to false

- Parameter ignoredOperators set to <<,>>,|

May 27, 2020, 5:46 AM System Activated Exceptions should not be created without being raised Severity set to Major

May 19, 2020, 6:27 AM System Activated Regular expressions should not be vulnerable to Denial of Service attacks Severity set to Critical

May 19, 2020, 6:26 AM System Activated Endpoints should not be vulnerable to reflected cross-site scripting (XSS) attacks Severity set to Blocker

May 11, 2020, 3:19 AM System Deactivated HTML autoescape mechanism should not be globally disabled
May 11, 2020, 3:19 AM System Activated Cipher algorithms should be robust Severity set to Critical

Encryption algorithms should be used with secure mode and padding scheme Severity set to Blocker

Disabling CSRF protections is security-sensitive Severity set to Critical

Server certificates should be verified during SSL/TLS connections Severity set to Critical

LDAP connections should be authenticated Severity set to Critical

Disabling auto-escaping in template engines is security-sensitive Severity set to Major