1.减法溢出（uint256 c=a-b,b参数 或uint256 c;c=a-b;)

//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or

primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

[not(expression/expression[2]/expression//primaryExpression/identifier[text()[1]=

(ancestor:: expressionStatement/expression/expression[1]/primaryExpression/identifier)])]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression//primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression//primaryExpression/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1]//primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]//expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

2.uint256 c; c=c-b,b参数 suboverflow

//expressionStatement[expression[text()="="]

and expression/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression/primaryExpression/identifier)]

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

[not(ancestor::functionDefinition/identifier[matches(text()[1],"burn")])]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier))]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

3. 查询balances[\_to] = balances[\_to]-\_value; suboverflow

//expressionStatement[expression[text()="="]

and expression/expression[1][text()[1]="[" and text()[2]="]"]

and expression/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression/expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression/expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/primaryExpression/identifier) and text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

4. 查询balances[msg.sender] = balances[msg.sender]- \_value

//expressionStatement[expression[text()="="]

and expression/expression[1][text()[1]="[" and text()[2]="]"]

and expression/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression/expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/primaryExpression/identifier) and text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

5. 查询allowed[\_to][msg.sender] = allowed[\_to][msg.sender]- \_value;

//expressionStatement[expression[text()="="]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression[2]/plusminusOperator/minusOperator

and expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1] [text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

6. uint256 c; c=c-newTokens,非参数，uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement[expression[text()="="]

and expression/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression/primaryExpression/identifier)]

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/primaryExpression/identifier) and (text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier))]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

7. 查询balances[\_to] = balances[\_to]- newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement[expression[text()="="]

and expression/expression[1][text()[1]="[" and text()[2]="]"]

and expression/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression/expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression/expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/primaryExpression/identifier) and text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

8. 查询balances[msg.sender] = balances[msg.sender]- newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement[expression[text()="="]

and expression/expression[1][text()[1]="[" and text()[2]="]"]

and expression/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression/expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/primaryExpression/identifier) and text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

9 查询allowed[\_to][msg.sender] = allowed[\_to][msg.sender]- newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement[expression[text()="="]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression[2]/plusminusOperator/minusOperator

and expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

]]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1] [text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

10. uint256 c; c=c-newTokens, uint newTokens = \_value \* PRICE;249.sol,26-33同

//expressionStatement[expression[text()="="]

and expression/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression/primaryExpression/identifier)]

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier))]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

11. 查询balances[\_to] = balances[\_to]- newTokens;

//expressionStatement[expression[text()="="]

and expression/expression[1][text()[1]="[" and text()[2]="]"]

and expression/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression/expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression/expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/primaryExpression/identifier) and text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

12. 查询balances[msg.sender] = balances[msg.sender]- newTokens;

//expressionStatement[expression[text()="="]

and expression/expression[1][text()[1]="[" and text()[2]="]"]

and expression/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and expression/expression[2]/plusminusOperator/minusOperator

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression/expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/primaryExpression/identifier) and text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

13 查询allowed[\_to][msg.sender] = allowed[\_to][msg.sender]- newTokens;

//expressionStatement[expression[text()="="]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression[2]/plusminusOperator/minusOperator

and expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/plusminusOperator/minusOperator]/expression[2]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1] [text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression/expression[2][plusminusOperator/minusOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

14. 综合查询\_totalSupply -=\_amount; 参数，ownerUnderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

]]

[not(ancestor::functionDefinition/identifier[matches(text()[1],"burn")])]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

15. 查询 balances[\_spender] -= \_amount; 参数，ownerUnderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

[not(ancestor::functionDefinition//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and

expression[2]/expression[1]/expression[2]/primaryExpression/identifier[text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

16. 查询 balances[msg.sender] -= \_amount; 参数，ownerUnderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

[not(ancestor::functionDefinition//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[2]/environmentalVariable[text()="msg.sender"]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

17. 查询 allowed[msg.sender][\_spender] -= \_amount; 参数，ownerUnderflow 或uint256 allowance = allowed[\_from][msg.sender]; require(balances[allowance >= \_value); allowed[\_from][msg.sender] -= \_value;

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier)]]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1] [text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

)]

[not(ancestor::functionDefinition//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

18. 综合查询\_totalSupply -= newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression[1]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

]]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

19. 查询 balances[\_spender] -= newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

]]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and

expression[2]/expression[1]/expression[2]/primaryExpression/identifier[text()[1]=  
(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

20. 查询 balances[msg.sender] -= newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

]]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[2]/environmentalVariable[text()="msg.sender"]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

21. 查询 allowed[msg.sender][\_spender] -= newTokens;非参数uint newTokens = msg.value \* PRICE;suboverflow18 或uint256 allowance = allowed[\_from][msg.sender]; require(balances[allowance >= newTokens); allowed[\_from][msg.sender] -= newTokens;

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier)]]

]]

[(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement[expression[text()="="]

and expression/expression[1][variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] or primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[2]/expression/environmentalVariable[matches(text()[1],"^msg.value$")]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1] [text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier)]]

)]

[not(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/environmentalVariable[matches(text()[1],"^msg.value$")]]]/expression[1]//identifier) and text()[1]=

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

22. 综合查询\_totalSupply -= newTokens;

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

23. 查询 balances[\_spender] -= newTokens;

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

[not(ancestor::functionDefinition//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and

expression[2]/expression[1]/expression[2]/primaryExpression/identifier[text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

24. 查询 balances[msg.sender] -= newTokens;

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

[not(ancestor::functionDefinition//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[2]/environmentalVariable[text()="msg.sender"]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=  
(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)] and expression[2]/expression[1]/expression[2]/environmentalVariable[text()="msg.sender"] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

25. 查询 allowed[msg.sender][\_spender] -= newTokens;

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier)]]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

)]

[not(ancestor::functionDefinition//expression[text()="."]

[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1] [text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and functionCall/functionName/identifier[matches(text()[1],"sub|Sub")]

and functionCall/callArguments/tupleExpression/expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

)]

[not(ancestor::functionDefinition//(expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]]

| expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression[2]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]] and expression[2]/plusminusOperator/minusOperator]/expression[1]/(variableDeclaration|primaryExpression)/identifier)]

]

[expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[expression[2][muldivOperator/mulOperator and expression/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]]]/expression[1]/(variableDeclaration|primaryExpression)/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier)]

])

)]

26. 若为数值情况；查询在for/while/dowhile循环中含有\_totalSupply -= 2000 \* 10\*\*8; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[2]//primaryExpression/numberLiteral/decimalNumber

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier))]]

[expression//primaryExpression/numberLiteral/decimalNumber[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]//primaryExpression/numberLiteral/decimalNumber)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

27. 若为数值情况；查询在for循环中含有 balances[owner] -= 2000 \* 10\*\*8; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

and expression[2]//primaryExpression/numberLiteral/decimalNumber

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))]

]]

[expression//primaryExpression/numberLiteral/decimalNumber[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression//primaryExpression/numberLiteral/decimalNumber)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

28.若为数值情况；查询在for循环中含有 balances[msg.sender] -= 2000 \* 10\*\*8; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and expression[2]//primaryExpression/numberLiteral/decimalNumber

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression//primaryExpression/numberLiteral/decimalNumber[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression//primaryExpression/numberLiteral/decimalNumber)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

29.若为数值情况；查询在for循环中含有 allowed[owner][msg.sender] -= 2000 \* 10\*\*8; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier)]]

and expression[2]//primaryExpression/numberLiteral/decimalNumber

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression//primaryExpression/numberLiteral/decimalNumber[text()[1]= (ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression//primaryExpression/numberLiteral/decimalNumber)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

30.若为常量情况, 查询在for循环中含有\_totalSupply -= TOTAL; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")]]/identifier))]]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[2]/primaryExpression/identifier) and text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

31.若为常量情况, 查询在for循环中含有balances[owner] -= TOTAL; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))]

]]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression/primaryExpression/identifier) and text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

32.若为常量情况, 查询在for循环中含有balances[msg.sender] -= TOTAL; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier)]

and expression[1]/expression[2]/environmentalVariable[text()="msg.sender"]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[2]/environmentalVariable[text()="msg.sender"]

]]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression/primaryExpression/identifier) and text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]

33.若为常量情况, 查询在for循环中含有allowed[owner][msg.sender] -= TOTAL; ownerunderflow

//expressionStatement

[expression[lvalueOperator/minusLvalueOperator

and expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/expression[1]/primaryExpression/identifier[text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier)]

and expression[1]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression[1]/expression[2][environmentalVariable[text()="msg.sender"] or primaryExpression/identifier[text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier)]]

and expression[2]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]

]]

[not(ancestor::functionDefinition//expression[text()[1] = ">" or text()[1] = "<" or text()[1] = "<=" or text()[1] = ">="]

[expression[text()[1]="[" and text()[2]="]"]]

[expression[expression[1][text()[1]="[" and text()[2]="]"]

and expression[1]/expression[1]/primaryExpression/identifier[text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/mappingSt[typeName[1]/elementaryTypeName[matches(text()[1],"address")] and typeName[2]/elementaryTypeName[matches(text()[1],"uint|int")]]]]/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

and expression[1]/expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

and expression[2][primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression[1]/expression[2]/primaryExpression/identifier) and (text()[1]= (ancestor::functionDefinition/parameterList/parameter[typeName/elementaryTypeName[matches(text()[1],"address")]]/identifier) or text()[1]= (ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|uint256")]]/identifier))] or environmentalVariable[text()="msg.sender"]]

]]

[expression/primaryExpression/identifier[text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[lvalueOperator/minusLvalueOperator]/expression/primaryExpression/identifier) and text()[1]=

(ancestor::sourceUnit//stateVariableDeclaration[typeName/elementaryTypeName[matches(text()[1],"uint|int")] and constantType[text()="constant"]]/identifier)]]

)]

[ancestor::statement/(forStatement|whileStatement|doWhileStatement)/condition/expression/expression[2][text()=".length"]]

[ancestor::functionDefinition/parameterList/parameter/typeName[typeName/elementaryTypeName[matches(text()[1],"address")]][text()="[]"]]