1.综合查询 uint c=a\*b 参数 overflow

//expressionStatement[expression[text()="="] and expression/expression[1]/variableDeclaration/typeName/elementaryTypeName[matches(text()[1],"uint|int")] and expression/expression[2]/muldivOperator/mulOperator

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

[not(ancestor::libraryDefinition/identifier[matches(text()[1],"Math")])]

[not(ancestor::contractDefinition/identifier[matches(text()[1],"Math")])]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//primaryExpression/identifier)]

and 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/muldivOperator/mulOperator]/expression[2]/expression/primaryExpression/identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression/primaryExpression/identifier)]

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//primaryExpression/identifier)]

])

)]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

(parent::\*/parent::\*/preceding-sibling::expression/expression/primaryExpression/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

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

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

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

(parent::\*/parent::\*/preceding-sibling::expression/expression/expression/primaryExpression/identifier) and text()[1]=

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

])

)]

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

2.综合查询 uint256 c;c=a\*b;参数 overflow3，c可以是返回值定义变量

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

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

and expression/expression[2]/muldivOperator/mulOperator

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

[not(ancestor::functionDefinition/identifier[text()[1]=(ancestor::contractDefinition/identifier)])]

[not(ancestor::functionDefinition[text()[1]= "constructor"])]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//primaryExpression/identifier)]

and 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/muldivOperator/mulOperator]/expression[2]/expression/primaryExpression/identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression/primaryExpression/identifier)]

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//primaryExpression/identifier)]

])

)]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

and expression/expression[1]/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/muldivOperator/mulOperator]/expression[2]/expression/primaryExpression/identifier)]

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

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

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

(ancestor::functionDefinition//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

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

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

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

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

])

)]

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

3. 乘法溢出(overbuy 非参数，定义的变量)，可通过msg.value改变 uint newTokens = msg.value \* PRESALE\_PRICE muloverflow5

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

and expression/expression[2]/muldivOperator/mulOperator

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

]

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

and expression/muldivOperator/divOperator

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

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

and expression//identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

])

)]

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

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

and expression//identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

and expression/expression[2]//identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

])

)]

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

and functionCall/callArguments/tupleExpression/expression/environmentalVariable[text()[1]= "msg.value"]]

)]

4. 乘法溢出(非参数，定义的变量)，可通过msg.value改变 uint newTokens ; newTokens = msg.value \* PRESALE\_PRICE muloverflow6

//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 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[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

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

and expression//identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

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

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

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

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

])

)]

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

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

and expression//identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

(ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

and expression/expression[2]//identifier[text()[1]= (ancestor::contractPartDefinition/(functionDefinition|functionFallBackDefinition)//expressionStatement/expression[expression/muldivOperator/mulOperator]/expression[2]/expression//identifier)]

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

])

)]

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

and functionCall/callArguments/tupleExpression/expression/environmentalVariable[text()[1]= "msg.value"]]

)]

5. 综合查询require(this.balance >= amount \* sellPrice);undersell

//functionCall

[functionName/identifier[text()[1] = "require"]]

[callArguments/tupleExpression[expression[text()[1] = ">="]

and expression/expression[2]/muldivOperator/mulOperator

and expression/expression[1][matches(text()[1],"^.balance$")]

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

or text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[text()[1]="address"]]/identifier)]]

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

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

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

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

]]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

])

)]

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

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

(ancestor::functionDefinition//functionCall//expression[muldivOperator/mulOperator]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

6综合查询require( amount \* sellPrice<= this.balance);undersell

//functionCall

[functionName/identifier[text()[1] = "require"]]

[callArguments/tupleExpression[expression[text()[1] = "<="]

and expression/expression[1]/muldivOperator/mulOperator

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

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

or text()[1]= (ancestor::functionDefinition//variableDeclaration[typeName/elementaryTypeName[text()[1]="address"]]/identifier)]]

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

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

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

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

]]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

])

)]

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

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

(ancestor::functionDefinition//functionCall//expression[muldivOperator/mulOperator]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

7. 综合查询require(tokenLimit >= amount \* sellPrice),参数 muloveflow78

//functionCall

[functionName/identifier[text()[1] = "require"]]

[callArguments/tupleExpression[expression[text()[1] = ">="]

and expression/expression[2]/muldivOperator/mulOperator

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

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

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

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

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

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

]]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

])

)]

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

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

(ancestor::functionDefinition//functionCall//expression[muldivOperator/mulOperator]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

8.综合查询require( amount \* sellPrice<= tokenLimit); muloverflow78

//functionCall

[functionName/identifier[text()[1] = "require"]]

[callArguments/tupleExpression[expression[text()[1] = "<="]

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

]]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

])

)]

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

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

(ancestor::functionDefinition//functionCall//expression[muldivOperator/mulOperator]/expression/primaryExpression/identifier)]

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

9. 查询类似amount \*= mintedAmount;参数 muloverflow9

//expressionStatement

[expression[lvalueOperator/mulLvalueOperator

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//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

])

)]

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

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

10.查询balanceOf[target] \*= mintedAmount; 参数 muloverflow9

//expressionStatement

[expression[lvalueOperator/mulLvalueOperator

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[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/expression[1]/primaryExpression/identifier)]

and expression/expression[2]/primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/expression[2]/primaryExpression/identifier)]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression[1]/expression/expression[1]/primaryExpression/identifier)]

and expression/expression[2]/expression[2]/primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/parent::\*/preceding-sibling::expression[1]/expression/expression[2]/primaryExpression/identifier)]

and expression[2]/primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/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/mulLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

11.查询balanceOf[msg.sender] \*= mintedAmount; 参数 muloverflow9

//expressionStatement

[expression[lvalueOperator/mulLvalueOperator

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[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/expression[1]/primaryExpression/identifier)]

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

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

(parent::\*/parent::\*/parent::\*/preceding-sibling::expression[1]/expression/expression[1]/primaryExpression/identifier)]

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

and expression[2]/primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/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/mulLvalueOperator]/expression[1]/expression[1]/primaryExpression/identifier)]

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]

12. 查询allowance[msg.sender][target] \*= mintedAmount; 参数 muloverflow9

//expressionStatement

[expression[lvalueOperator/mulLvalueOperator

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],"address")]]/identifier)]]

]]

[not(ancestor::functionDefinition//(expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

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

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

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/expression[1]/expression[1]/primaryExpression/identifier)]

and expression/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression/expression[2][primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

]

| expression[comparison[text()[1] = "=="]

and expression/muldivOperator/divOperator

and expression/expression[1]/muldivOperator/mulOperator

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

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

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

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

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

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

(parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression[1]/expression/expression[1]/expression[1]/primaryExpression/identifier)]

and expression/expression[2]/expression[1]/expression[2][primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/parent::\*/parent::\*/preceding-sibling::expression[1]/expression/expression[1]/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

and expression/expression[2]/expression[2][primaryExpression/identifier[text()[1]= (parent::\*/parent::\*/parent::\*/preceding-sibling::expression[1]/expression/expression[2]/primaryExpression/identifier)] or environmentalVariable[text()="msg.sender"]]

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

(parent::\*/parent::\*/preceding-sibling::expression/expression[1]/expression/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/mulLvalueOperator]/expression[1]/expression[1]/expression[1]/primaryExpression/identifier)]

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

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

and functionCall/functionName/identifier[matches(text()[1],"mul|Mul")]

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

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

)]