Checkmarx

CxQL 规则自定义技术分享

Happy.Yang@checkmarx.com

Agenda

- CxQL自定义规则难点
- CxQL自定义规则最佳实践
- CxQL DOM类型
- Java SSRF自定义规则
  - 误报和漏报产生的原因（Cx原生规则分析）
  - 示例代码
  - 规则自定义分析

CxQL自定义规则难点

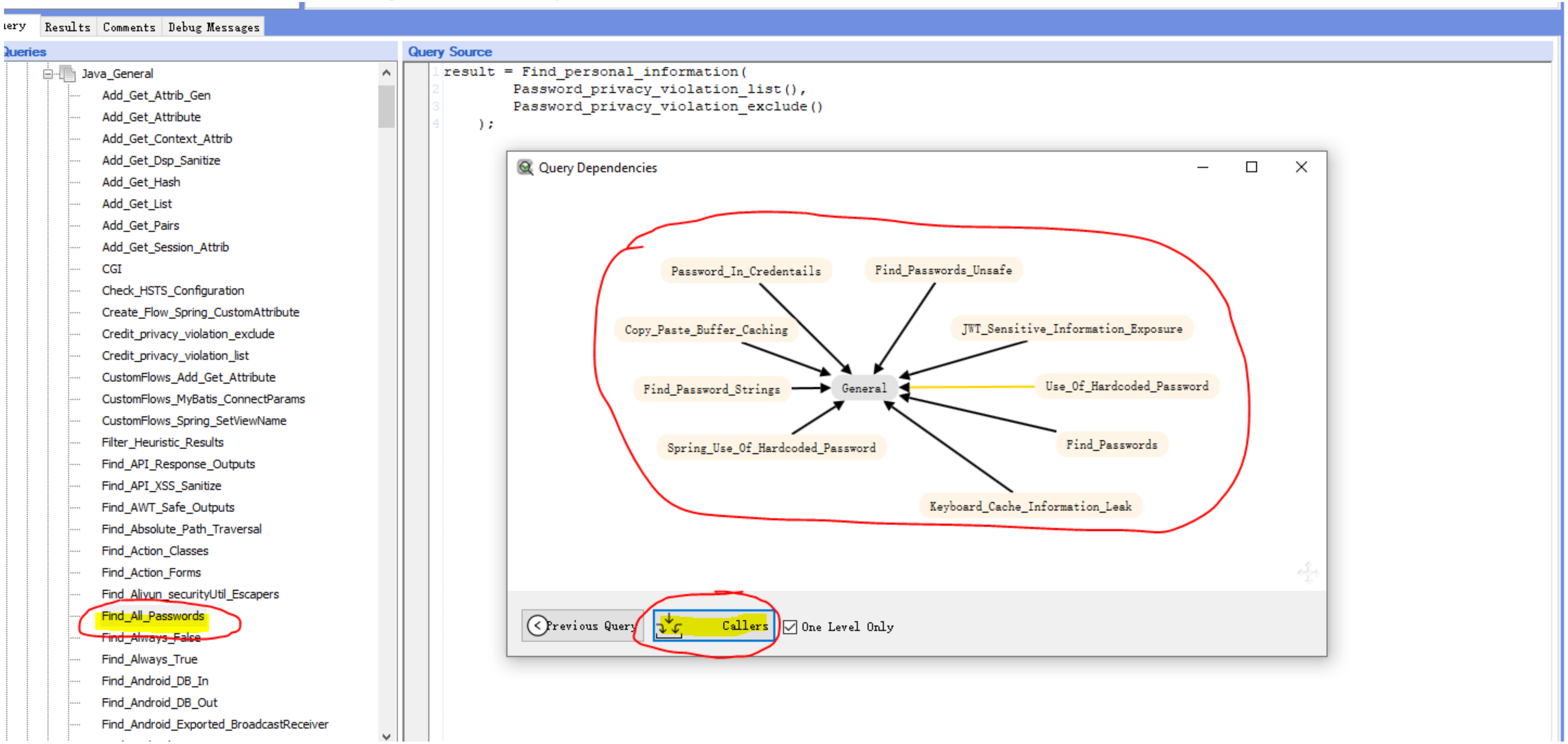
CxQL规则定义难点

- 不熟悉Checkmarx引擎分析原理
  - https://github.com/HappyY19/CxKnowlegeRepo/blob/main/Slides/CxSAST%20-%20CxQL%20Query%20Customization-%20How%20to%20fix%20FP%2C%20FN.pdf
- 不理解Cx DOM类型含义
  - https://github.com/checkmarx-ts/CxDOM-Types/wiki
- 不知如何实现想查找的代码元素
  - 参考Cx原生规则
  - 获取Cx原生规则：https://github.com/HappyY19/CxKnowlegeRepo/blob/main/PythonScripts/GetQueries.py

CxQL自定义规则最佳实践

规则自定义最佳实践

- https://github.com/HappyY19/CxKnowlegeRepo/blob/main/Slides/CxQL%20-%20Best%20Coding%20Practices.pdf
- 写规则类似写函数，注意dependency。确保修改一个规则，不会引发别的规则误报。



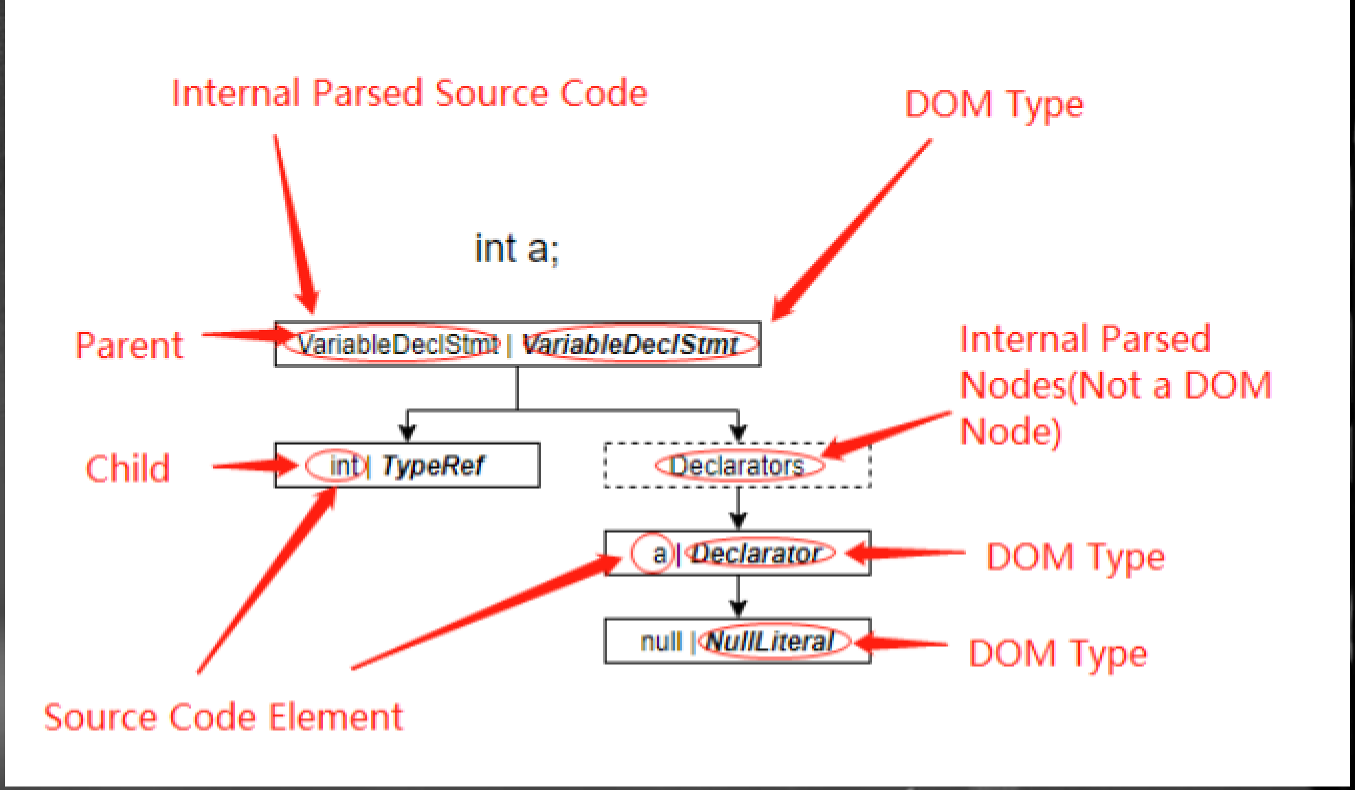
- Java_General
  - Add_Get_Attrib_Gen
  - Add_Get_Attribute
  - Add_Get_Context_Attrib
  - Add_Get_Dsp_Sanitize
  - Add_Get_Hash
  - Add_Get_List
  - Add_Get_Pairs
  - Add_Get_Session_Attrib
  - CGI
  - Check_HSTS_Configuration
  - Create_Flow_Spring_CustomAttribute
  - Credit_privacy_violation_exclude
  - Credit_privacy_violation_list
  - CustomFlows_Add_Get_Attribute
  - CustomFlows_MyBatis_ConnectParams
  - CustomFlows_Spring_SetViewName
  - Filter_Heuristic_Results
  - Find_API_Response_Outputs
  - Find_API_XSS_Sanitize
  - Find_AWT_Safe_Outputs
  - Find_Absolute_Path_Traversal
  - Find_Action_Classes
  - Find_Action_Forms
  - Find_Aliyun_securityUtil_Escapers
  - Find_All_Passwords
  - Find_Always_False
  - Find_Always_True
  - Find_Android_DB_In
  - Find_Android_DB_Out
  - Find_Android_Exported_BroadcastReceiver

```
result = Find_personal_information(
        Password_privacy_violation_list(),
        Password_privacy_violation_exclude()
    );
```

CxQL DOM类型

CxQL DOM 类型

- https://github.com/checkmarx-ts/CxDOM-Types/wiki



Checkmarx

在CxQL规则里您可使用的C#类型

- bool
- Int
- string
- char
- List
- Dictionary
- Tuple
- System.Collections.ArrayList
- System.Text.RegularExpressions.Regex

Java SSRF自定义规则

Checkmarx

Java SSRF 误报和漏报产生的原因（Cx原生规则分析）

```
CxList inputs = Find_Interactive_Inputs();
CxList declarators = Find_Declarators();
CxList paramss = base.Find_ParamDecl();

CxList declParams = declarators;
declParams.Add(paramss);

CxList stringDeclaratorsAndParams = declParams.FindByType("String");
CxList unkRefs = Find_UnknownReference();
CxList unkRefsAndDeclAndParams = unkRefs;
unkRefsAndDeclAndParams.Add(declarators);
unkRefsAndDeclAndParams.Add(paramss);


CxList stringDeclaratorsReferences = unkRefsAndDeclAndParams.FindAllReferences(stringDeclaratorsAndParams);
inputs = inputs.InfluencingOn(stringDeclaratorsReferences);

CxList requests = Find_Remote_Requests();
CxList sanitizers = Find_Remote_Requests_Sanitize();


result = requests.InfluencedByAndNotSanitized(inputs, sanitizers).ReduceFlowByPragma();
```

Java SSRF示例代码

- https://github.com/checkmarx-ts/CxQL/tree/master/Java/JavaSampleCode/Java_Medium_Threat/SSRF

Java SSRF规则自定义分析

- https://github.com/checkmarx-ts/CxQL/blob/master/Java/Java_Medium_Threat/SSRF.txt

/ Thank you

Happy.Yang@checkmarx.com

www.checkmarx.com