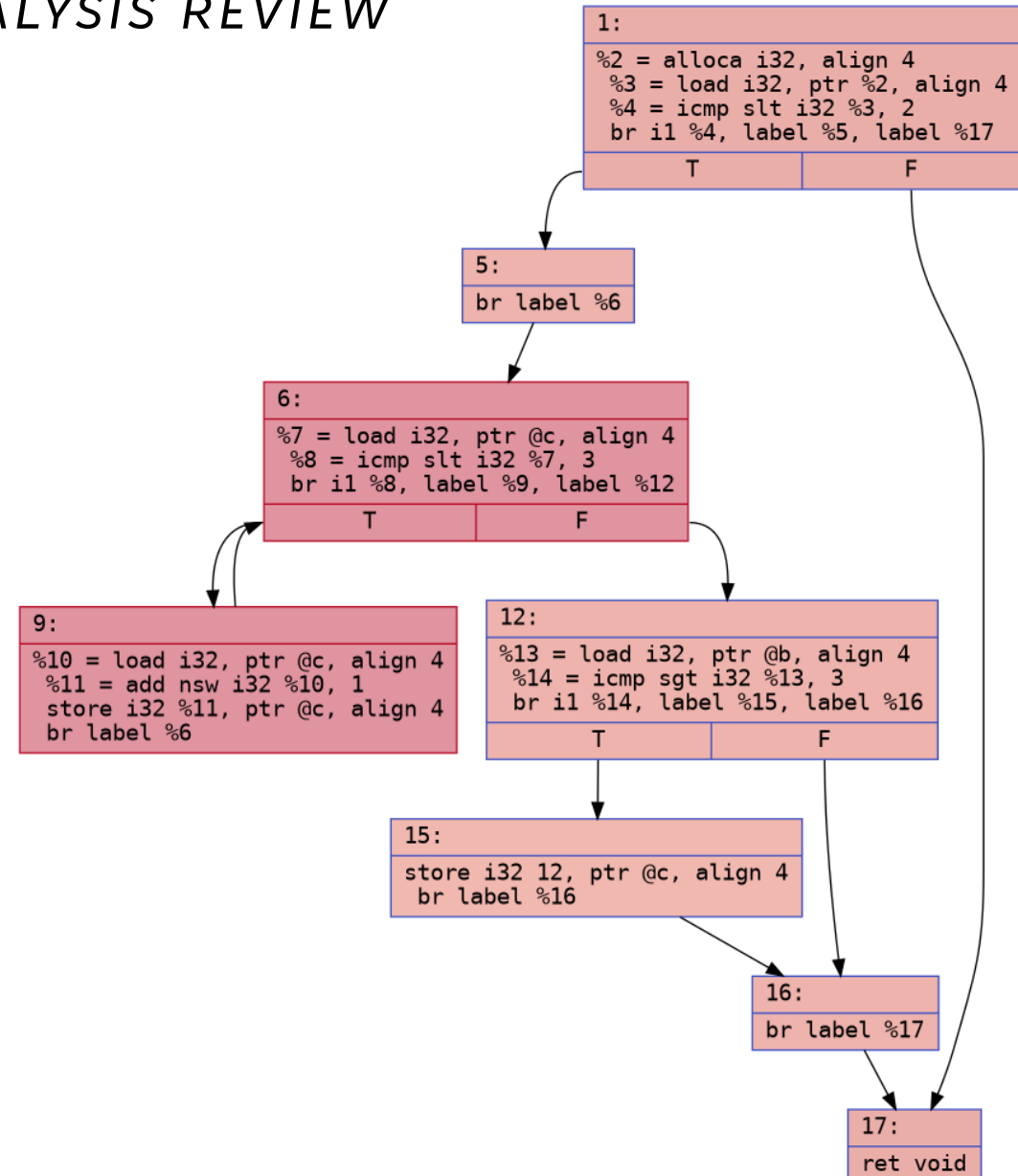


EXERCISE #9

STATIC ANALYSIS REVIEW

- Use path notation to indicate one path (or set of paths) through this CFG:



CODEQL

“a language and toolchain for code analysis”

EECS 677: Software Security Evaluation

Drew Davidson

Guest: Dominic Tassio

ADMINISTRIVIA AND ANNOUNCEMENTS

Drew is not here

A little about me...

LAST TIME

- Continued Rice's Theorem discussion
 - “All non-trivial semantic properties of programs are undecidable.”
- Program Guarantees
 - “Provide assurances about what a program will NEVER or ALWAYS do”
- Analysis Over CFGs
 - Building/Notating/Visualizing/Overapproximating Reachability

TODAY'S ROADMAP

- What is CodeQL?
- What is CodeQL used for?
- How to use CodeQL
- Live* Demo

WHAT IS CODEQL?

FIRST, SEMMLE

- CodeQL was originally a product from Semmle, Inc.
- Acquired by GitHub/Microsoft in September 2019
- Made free for open source and research
- Now integrated directly with GitHub and as a vscode extension

CODEQL NOW

- “a language and toolchain for code analysis”
- CodeQL allows for code to be queried like a database
- Provides a “standard library” of queries to discover vulnerabilities, measure code quality, or to mix and match

A LANGUAGE

```
UnsafeDeserialization.ql
```

```
import TaintTracking::Global<UnsafeDeserializationConfig>
```

```
from PathNode source, PathNode sink
```

```
where flowPath(source, sink)
```

```
select sink.getNode().(UnsafeDeserializationSink).getMethodAccess(), source, sink,  
       "Unsafe deserialization of $@.", source.getNode(), "user input"
```

**WHAT IS CODEQL USED
FOR?**

SUPPORTED LANGUAGES

Language	Variants	Compilers
C/C++	C89, C99, C11, C17, C23, C++98, C++03, C++11, C++14, C++17, C++20, C++23	Clang, GCC, MSVC, armcc
C#	.NET 5, .NET 6, .NET 7, .NET 8, .NET 9, .NET 10	
GitHub Actions		
Go	up to 1.27	
Java	to 26	javac, ecj
Kotlin	.8.0 to 2.4.20	Kotlin compiler
JavaScript	ECMAScript 2022 or lower	
Python	2.7, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14	
Ruby	up to 3.3	
Rust	editions 2021 and 2024	Rust compiler
Swift	5.4 to 6.3	Swift compiler
TypeScript	2.6 to 7.0	

SUPPORTED FRAMEWORKS

Language	Framework
C#	ASP.NET, ASP.NET Core, ASP.NET Razor, Dapper, EntityFramework, Json.NET, NHibernate, WinForms
Go	beego, Chi, Couchbase, Echo, Gin, glog, go-pg, go-restful, go-sh, go-spew, GoKit, Gokogiri, goproxy, goxpath, htmlquery, jsonpatch jsonquery, protobuf, sqlx, xmlpath, xmlquery, xpath, yaml, zap, ...
Java/Kotlin	Guava, Hibernate, Jackson, JSON-java, JDBC, protobuf, String, ...
JavaScript/TypeScript	angular, axios, ejs, electron, express, fastify, handlebars, hapi, hogan, jquery, lodash, mustache, mysql, nest.js, react, request, sequelize, socket.io, sqlite3, swig, underscore, vue, ...
Python	Django, FastAPI, Flask, Twisted, httpx, requests, urllib, urllib2, urllib3, simplejson, toml, ujson, psycopg2, sqlite3, SQLAlchemy, libxml2, ...
Ruby	Faraday, http_client, httparty, nokogiri, open-uri, posix-spawn, rubyzip, ...
Rust	Actix-web, alloc, biscotti, clap, cookie, digest, futures, hyper, libc, log, md5, mysql, mysql, once_cell, poem, postgres, rand, regex, reqwest, rocket, rustls, sqlx, tokio, url, warp, ...
Swift	Alamofire, CryptoKit, CryptoSwift, Foundation, GRDB, JavaScriptCore, libxml2, Network, SQLite3, UIKit, WebKit, ...

DATA FLOW

Computing the possible values that a variable can hold at various points in a program

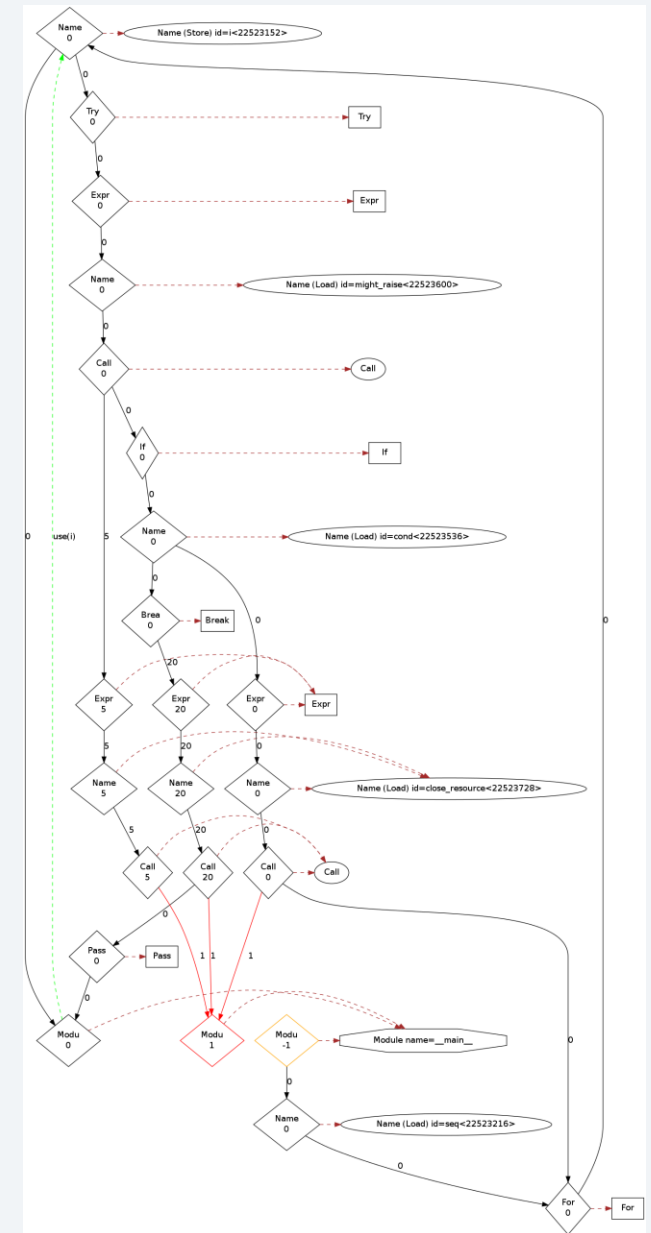
RANGE ANALYSIS

Determine the upper or lower bounds on an expression, or whether an expression could potentially overflow or underflow

ANALYZE CONTROL FLOW

Explore the control flow graph of a program

Discover unreachable code or mutually exclusive blocks of code



NAVIGATE THE CALL GRAPH

Identifying code that calls other code, and code that can be called from elsewhere

Find methods that are never used

DETECTING BUFFER OVERFLOW

Detect potential buffer overflows by checking for allocations

HOW TO USE CODEQL?

1. BUILD THE DATABASE

CodeQL does not operate directly on the program source

A database needs to be generated using the source code before analysis can begin

2. WRITE A QUERY

Using the CodeQL query language, write a query to run the analysis that you're interested

Or use a built-in or preexisting query

3. RUN THE QUERY

Once you have the database created and the query written, run the query

4. INSPECT THE RESULTS

CodeQL supports several outputs for both human and machine consumption

LIVE DEMO