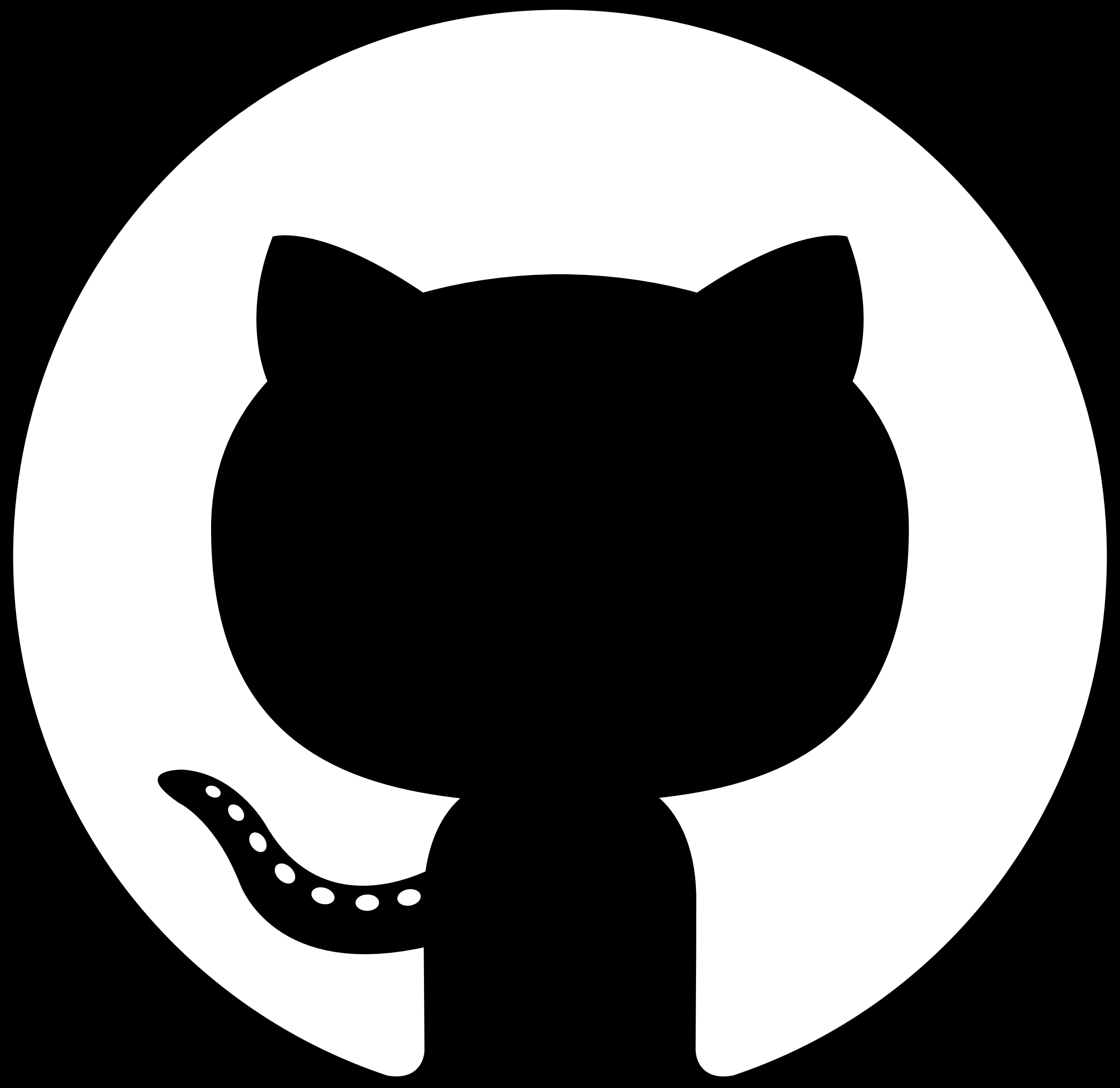

> sessions/workshops/

Satellite
VIRTUAL 2020

Finding security vulnerabilities in Java with CodeQL

7 May 2020

Presented by @lcartey

Moderated by @aibaars @aschackmull @adityasharad

Finding security vulnerabilities in JavaScript with CodeQL

7 May 2020

Presented by @adityasharad

Moderated by @asgerf @erik-krogh @esbena @lcartey

Today we will learn

- What CodeQL is
- How to write queries in CodeQL to identify patterns in code
- How to use CodeQL to find known security vulnerabilities in a well-known open-source project
- https://github.com/githubsatelliteworkshops/codeql

What is CodeQL?

An expressive query language and engine for code analysis

- Treats code as data
- Lets you describe and find patterns in the code
- CLI and IDE tools

What can I do with it?

- Find bugs and security vulnerabilities
- Quickly make your analyses more precise
- Share security knowledge within your teams using codified, readable and executable queries

A new language!

What's different about it?

CodeQL is...

- Logical
- Declarative - no side effects
- Object-oriented
- Read-only
- Equipped with rich standard libraries for analyzing source code

What does a query look like?

Import: lets us reuse logic defined in other libraries

```
import java (import javascript)
```

```
from IfStmt ifStmt, Block block
where
  block = ifStmt.getThen() and
  block.getNumStmt() = 0
select ifStmt, "This if-statement has an empty then-block."
```

Query clause: describes what we are trying to find

Building blocks of a query

Predicates

Like functions, but better!

Create reusable logic and give it a name.

Just a query

```
from IfStmt ifStmt, Block block
where
  block = ifStmt.getThen() and
  block.getNumStmt() = 0
select ifStmt
```

Using a predicate

```
predicate isEmpty(Block block) {
  block.getNumStmt() = 0
}
from IfStmt ifStmt
where isEmpty(ifStmt.getThen())
select ifStmt
```

Classes

Describe a set of values.

Using a predicate

```
predicate isEmpty(Block block) {
  block.getNumStmt() = 0
}
from IfStmt ifStmt
where isEmpty(ifStmt.getThen())
select ifStmt
```

Using a class

```
class EmptyBlock extends Block {
  EmptyBlock() {
    this.getNumStmt() = 0
  }
}
from IfStmt ifStmt
where ifStmt.getThen() instanceof
      EmptyBlock
select ifStmt
```

Using a predicate

```
predicate isEmpty(Block block) {
  block.getNumStmt() = 0
}
from IfStmt ifStmt
where isEmpty(ifStmt.getThen())
select ifStmt
```

Using a class

```
class EmptyBlock extends Block {
  EmptyBlock() {
    this.getNumStmt() = 0
  }
}
from IfStmt ifStmt, EmptyBlock block
where ifStmt.getThen() = block
select ifStmt
```

Let's write some CodeQL!

https://github.com/githubsatelliteworkshops/codeql