

# CodeQL

Visão geral, conjugando teoria e prática.

**Marcelo Reis**

[Student]

creis@gmail.com

Department of Computer Systems  
Computer Science Division – IEC  
Aeronautics Institute of Technology – ITA



Today

# Agenda

Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

Conclusion

Questions &  
Answers

- 1 Motivation
- 2 CodeQL
- 3 Exemplos Iniciais
- 4 SQL-Injection
- 5 XSS
- 6 Conclusion
- 7 Questions & Answers

## Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

Conclusion

Questions &  
Answers

1 Motivation

2 CodeQL

3 Exemplos Iniciais

4 SQL-Injection

5 XSS

6 Conclusion

7 Questions &amp; Answers

Surname,  
Name

Motivation

CodeQL

Exemplos

Iniciais

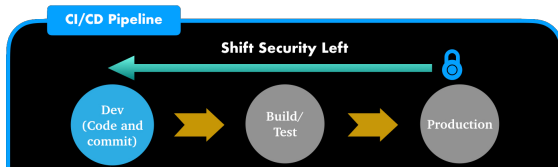
SQL-Injection

XSS

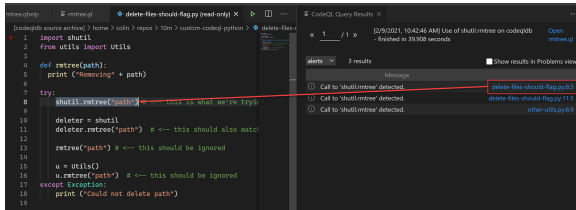
Conclusion

Questions &  
Answers

## Motivation



Como listar e navegar nos pontos do programa, cujo padrão sugere uma vulnerabilidade, antes da produção??



# Agenda

Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

Conclusion

Questions &  
Answers

1 Motivation

2 CodeQL

3 Exemplos Iniciais

4 SQL-Injection

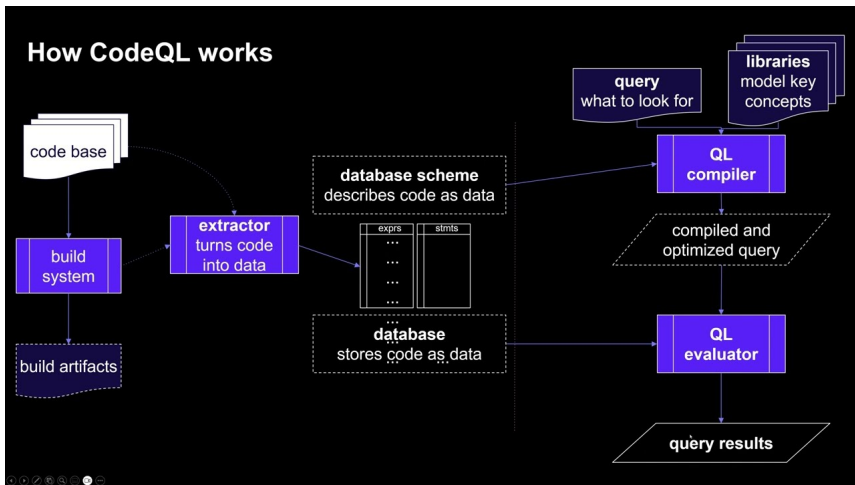
5 XSS

6 Conclusion

7 Questions &amp; Answers

# Definição e Princípios

- 1 Ferramenta de análise estática.
- 2 Trata o código com dado



Motivation

CodeQL

**Exemplos  
Iniciais**

SQL-Injection

XSS

Conclusion

Questions &  
Answers

1 Motivation

2 CodeQL

**3 Exemplos Iniciais**

4 SQL-Injection

5 XSS

6 Conclusion

7 Questions &amp; Answers

# Consultas Básicas

- Analisar a “Blocos Vazios”.
- Retornos compostos por somas.
  - `return x+y;`
- Comentários /\*TODO.....
- Métodos com apenas um argumento



Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

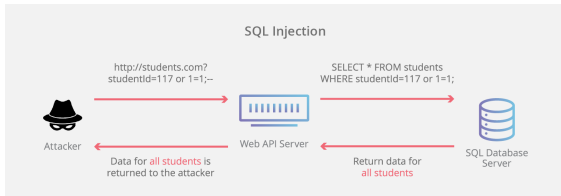
XSS

Conclusion

Questions &  
Answers

- 1 Motivation
- 2 CodeQL
- 3 Exemplos Iniciais
- 4 SQL-Injection**
- 5 XSS
- 6 Conclusion
- 7 Questions & Answers

# SQL-Injection



```
1 public boolean login(String username, String password). {}
2 String sql =
3 "select * from users where username = " + "'" + username + "'" + " and " +
4 "password " + " = " + "'" + password + "'";
5
6 ResultSet result = stmt.executeQuery(query);
7
8 if(result.next()) {
9     /* Login Success */
10    return true;
11 }
12 else. {
13     /* Login Failed */
14    return false;
15 }
16
17 }
```

Como listar todos os pontos do programa em que consultas são passadas por meio de strings??!

# SQL-Injection

*Melhor ainda....*

The screenshot displays a CodeQL interface with a Python file on the left and query results on the right.

**Python File:** `delete-files-should-flag.py` (read-only). The code defines a function `rmtree(path)` that prints the path and attempts to delete it using `shutil.rmtree`. It includes comments indicating which calls should be detected or ignored.

```
1 import shutil
2 from utils import Utils
3
4 def rmtree(path):
5     print ("Removing" + path)
6
7     try:
8         shutil.rmtree("path") # <-- this is what we're trying to delete
9
10        deleter = shutil
11        deleter.rmtree("path") # <-- this should also match
12
13        rmtree("path") # <-- this should be ignored
14
15        u = Utils()
16        u.rmtree("path") # <-- this should be ignored
17    except Exception:
18        print ("Could not delete path")
19
```

**CodeQL Query Results:** The query is titled "Use of shutil.rmtree on codeql db" and finished in 39.908 seconds. It shows 3 results for the alert "Call to 'shutil.rmtree' detected.".

Message	Location
Call to 'shutil.rmtree' detected.	delete-files-should-flag.py:8:5
Call to 'shutil.rmtree' detected.	delete-files-should-flag.py:11:5
Call to 'shutil.rmtree' detected.	other-utils.py:6:9

A red arrow points from the first result (line 8:5) to the corresponding line in the Python code.

Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

**XSS**

Conclusion

Questions &  
Answers

- 1 Motivation
- 2 CodeQL
- 3 Exemplos Iniciais
- 4 SQL-Injection
- 5 XSS**
- 6 Conclusion
- 7 Questions & Answers

*Execução de um trecho de código indesejado.*

Motivation

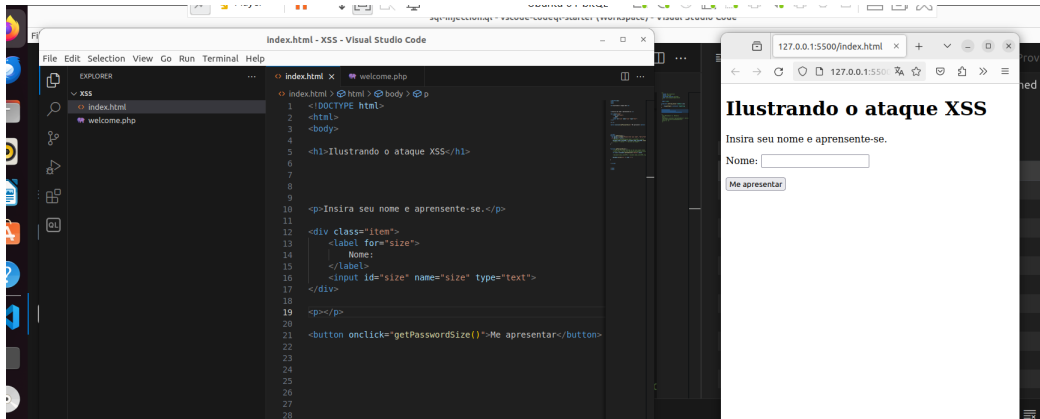
CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

Conclusion

Questions &  
Answers

Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

**Conclusion**Questions &  
Answers

- 1 Motivation
- 2 CodeQL
- 3 Exemplos Iniciais
- 4 SQL-Injection
- 5 XSS
- 6 Conclusion**
- 7 Questions & Answers

# Conclusion

*Bem-vindo ao vasto mundo do codeQL.*

Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

Conclusion

Questions &  
Answers

① Motivation

② CodeQL

③ Exemplos Iniciais

④ SQL-Injection

⑤ XSS

⑥ Conclusion

⑦ Questions &amp; Answers



# Questions & Answers

Surname,  
Name

Motivation

CodeQL

Exemplos  
Iniciais

SQL-Injection

XSS

Conclusion

Questions &  
Answers