

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

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

① Motivation

② CodeQL

③ Exemplo 1

④ SQL-Injection

⑤ XSS

⑥ Conclusion

⑦ Questions & Answers

Agenda

Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers**1 Motivation**

2 CodeQL

3 Exemplo 1

4 SQL-Injection

5 XSS

6 Conclusion

7 Questions & Answers

Surname,
Name

Motivation

CodeQL

Exemplo 1

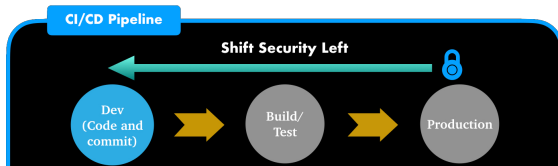
SQL-Injection

XSS

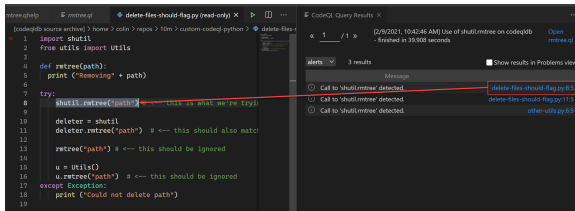
Conclusion

Questions &
Answers

Motivation



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



Agenda

Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

1 Motivation

2 CodeQL

3 Exemplo 1

4 SQL-Injection

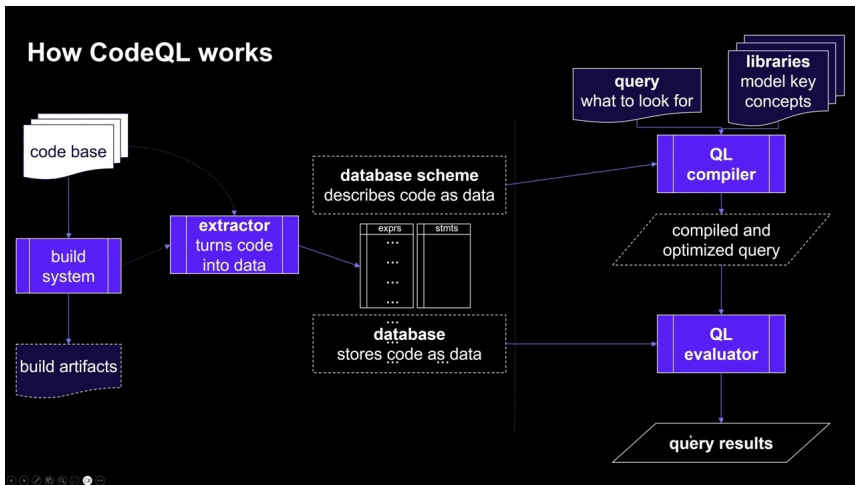
5 XSS

6 Conclusion

7 Questions & Answers

Definição e Princípios

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



Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

1 Motivation

2 CodeQL

3 Exemplo 1

4 SQL-Injection

5 XSS

6 Conclusion

7 Questions & Answers

Esquentando

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

Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

1 Motivation

2 CodeQL

3 Exemplo 1

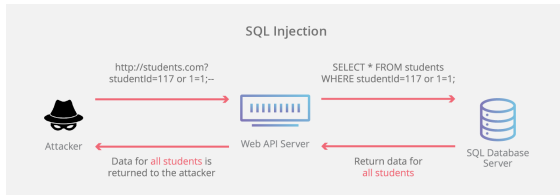
4 SQL-Injection

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 the CodeQL interface. On the left, a Python file named `delete-files-should-flag.py` is open, showing a function `rmtree` that recursively removes files. The function signature is `def rmtree(path):`, and it includes a `try:` block that calls `shutil.rmtree("path")`. A red arrow points from the `shutil.rmtree("path")` call in the code to the first result in the 'CodeQL Query Results' panel on the right. The results panel shows three alerts, all with the message 'Call to 'shutil.rmtree' detected.' The first alert is highlighted with a red box and its file path, `delete-files-should-flag.py:8:5`, is visible. The second alert is at `delete-files-should-flag.py:11:5` and the third is at `other-utils.py:6:9`. The top of the results panel shows the query name 'CodeQL Query Results' and the execution details: '[2/9/2021, 10:42:46 AM] Use of shutil.rmtree on codeql.db - finished in 39.908 seconds'.

```
[codeql.db source archive] > home > colin > repos > 10m > custom-codeql-python > delete-files-should-flag.py (read-only) X ▶ □ ...
```

```
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 do
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 X

« 1 / 1 » [2/9/2021, 10:42:46 AM] Use of shutil.rmtree on codeql.db - finished in 39.908 seconds [Open rmtree.q](#)

alerts 3 results ☐ Show results in Problems view

Message
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

Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

1 Motivation

2 CodeQL

3 Exemplo 1

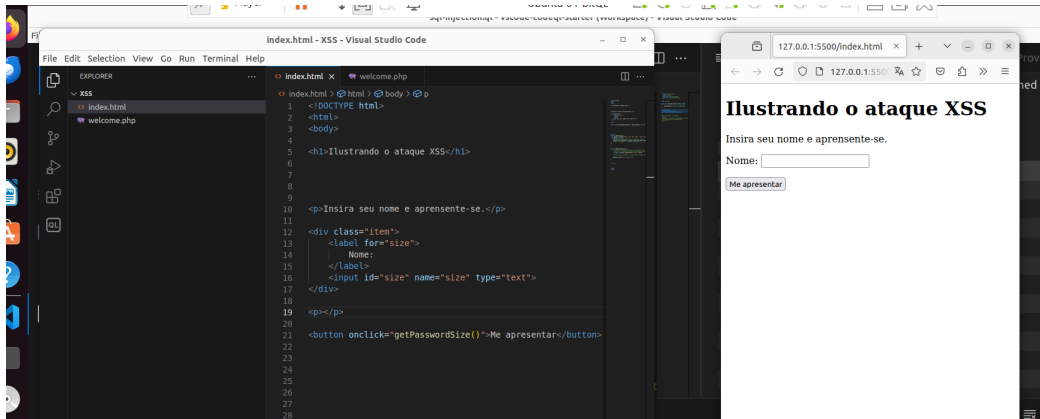
4 SQL-Injection

5 XSS

6 Conclusion

7 Questions & Answers

Execução de um trecho de código indesejado.



Agenda

Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

1 Motivation

2 CodeQL

3 Exemplo 1

4 SQL-Injection

5 XSS

6 Conclusion

7 Questions & Answers

Conclusion

Bem-vindo ao vasto mundo do codeQL.

Agenda

Motivation

CodeQL

Exemplo 1

SQL-Injection

XSS

Conclusion

Questions &
Answers

1 Motivation

2 CodeQL

3 Exemplo 1

4 SQL-Injection

5 XSS

6 Conclusion

7 Questions & Answers

Questions & Answers

