CodeQL

Visão geral, conjugando teoria e prática.

Marcelo Reis
[Student]
crereis@gmail.com

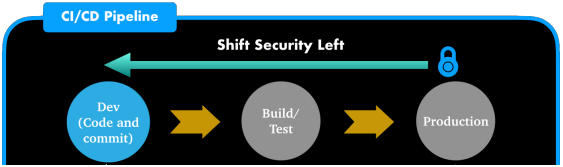
Department of Computer Systems
Computer Science Division – IEC
Aeronautics Institute of Technology – ITA

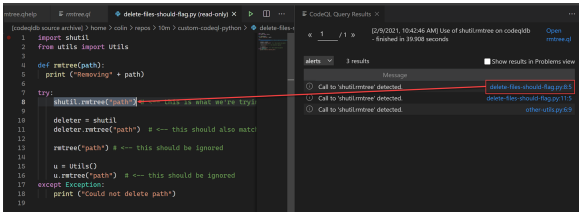
Today

Agenda

Agenda

Motivation



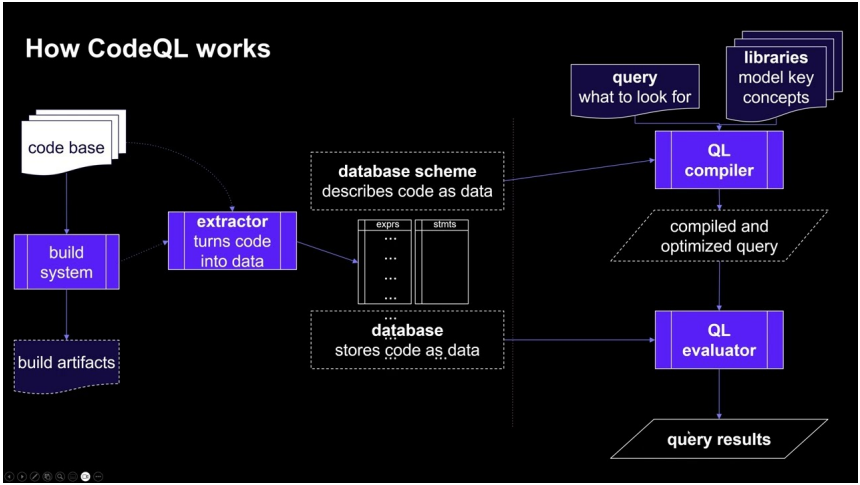


Como listar e navegar nos pontos do programa, cujo padrão sugere uma vulnerabilidade, antes da produção??

Agenda

Definição e Princípios

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



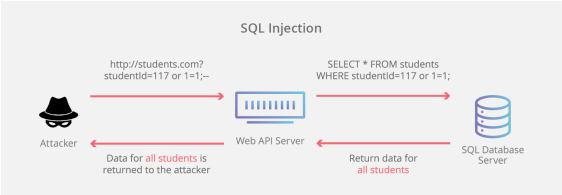
Agenda

Esquentando

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

Agenda

SQL-Injection

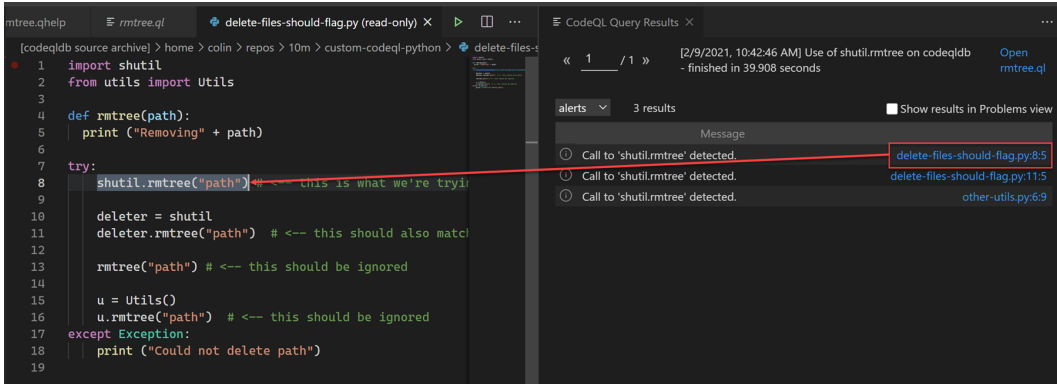



```
1
2  public boolean login(String username, String password). {}
3      String sql =
4      "select * from users where username = " + "'" + username + "'" + " and " +
5              "password " + " = " + "'" + password + "'";
6
7      ResultSet result = stmt.executeQuery(query);
8
9      if(result.next())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

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

SQL-Injection

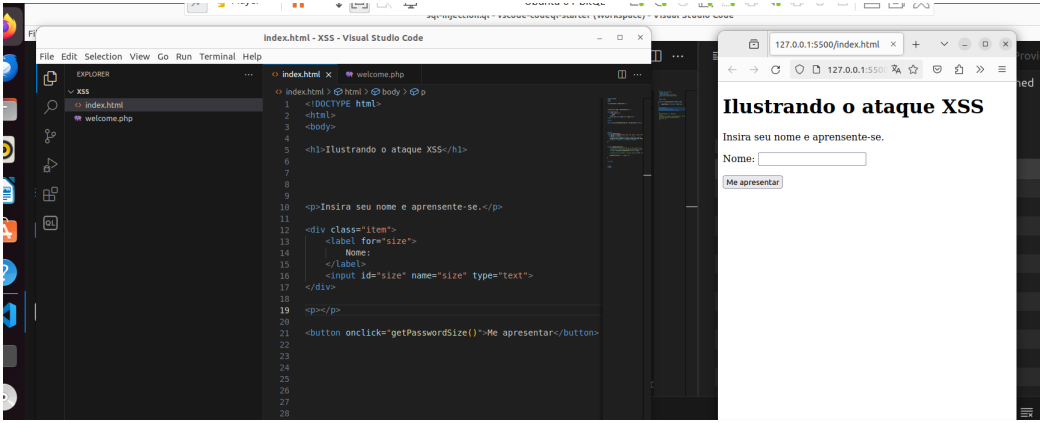
Melhor ainda....



Agenda

XSS

Execução de um trecho de código indesejado.



Agenda

Conclusion

Bem-vindo ao vasto mundo do codeQL.

Agenda

Questions & Answers