Master's degree InternShip Presentation

Erwan 'Feideus' Ulrich

Galileo Institute - University Paris 13

September 10, 2018

Presentation structure

- Internship environment
- SchemaFuzz Presentation
- Results
- Enrichment
- Conclusion

The Berner FachHochschule (BFH)

GNU Taler

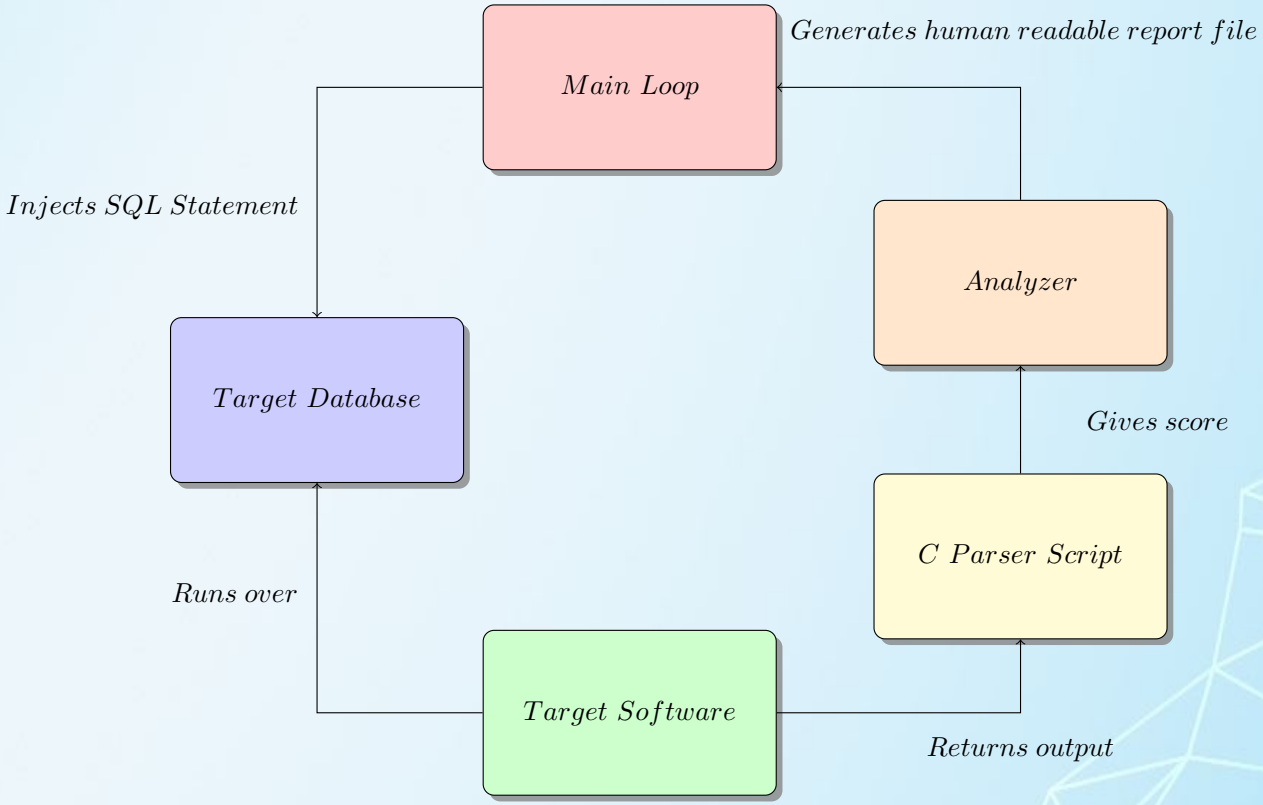
SchemaFuzz

- What is SchemaFuzz ?
- General Structure
- How does it Work ?
- Obstacles and solutions

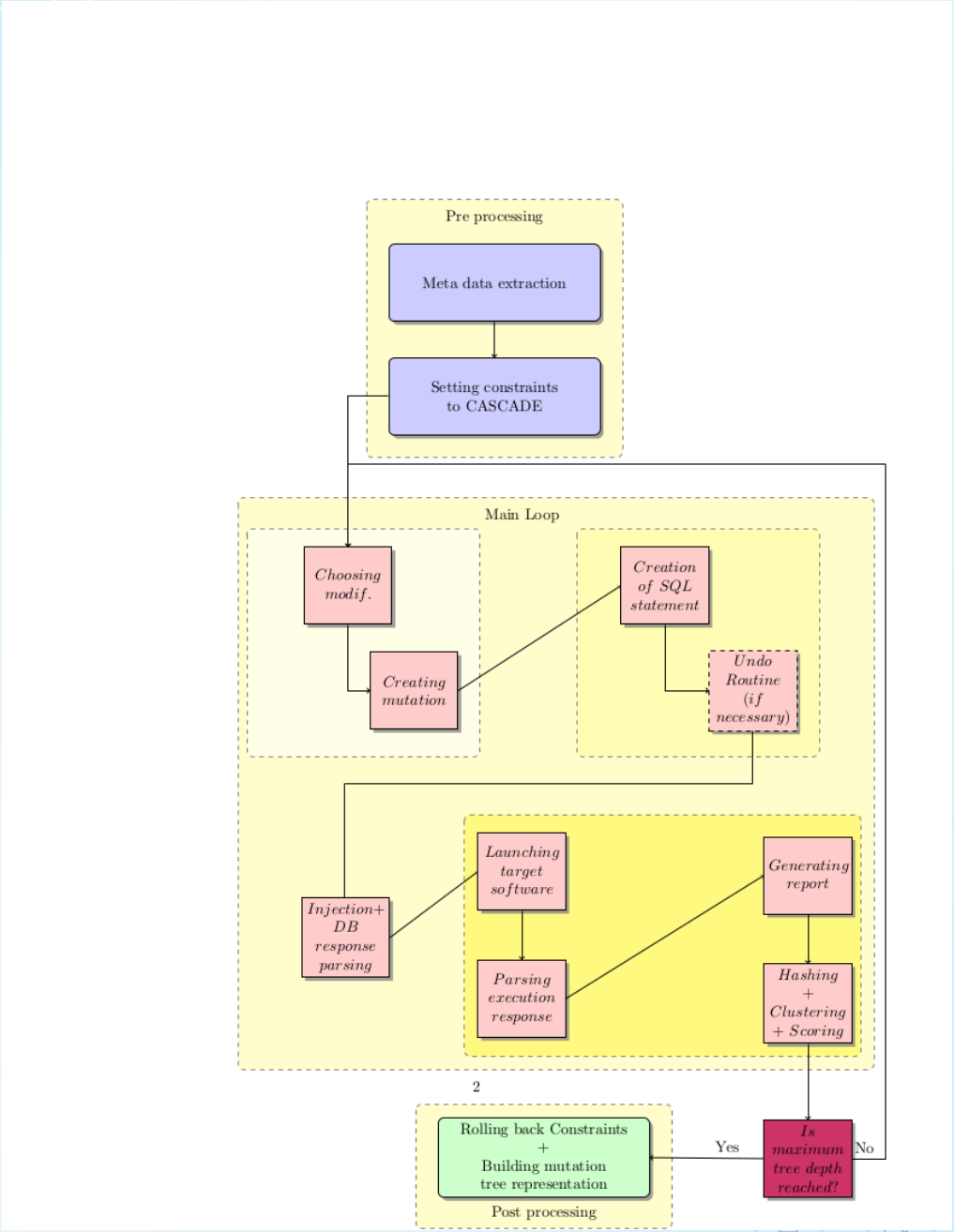
What is SchemaFuzz ?

- Database oriented Fuzzing tool
- Secure database exchange

General Structure



How does it work ?

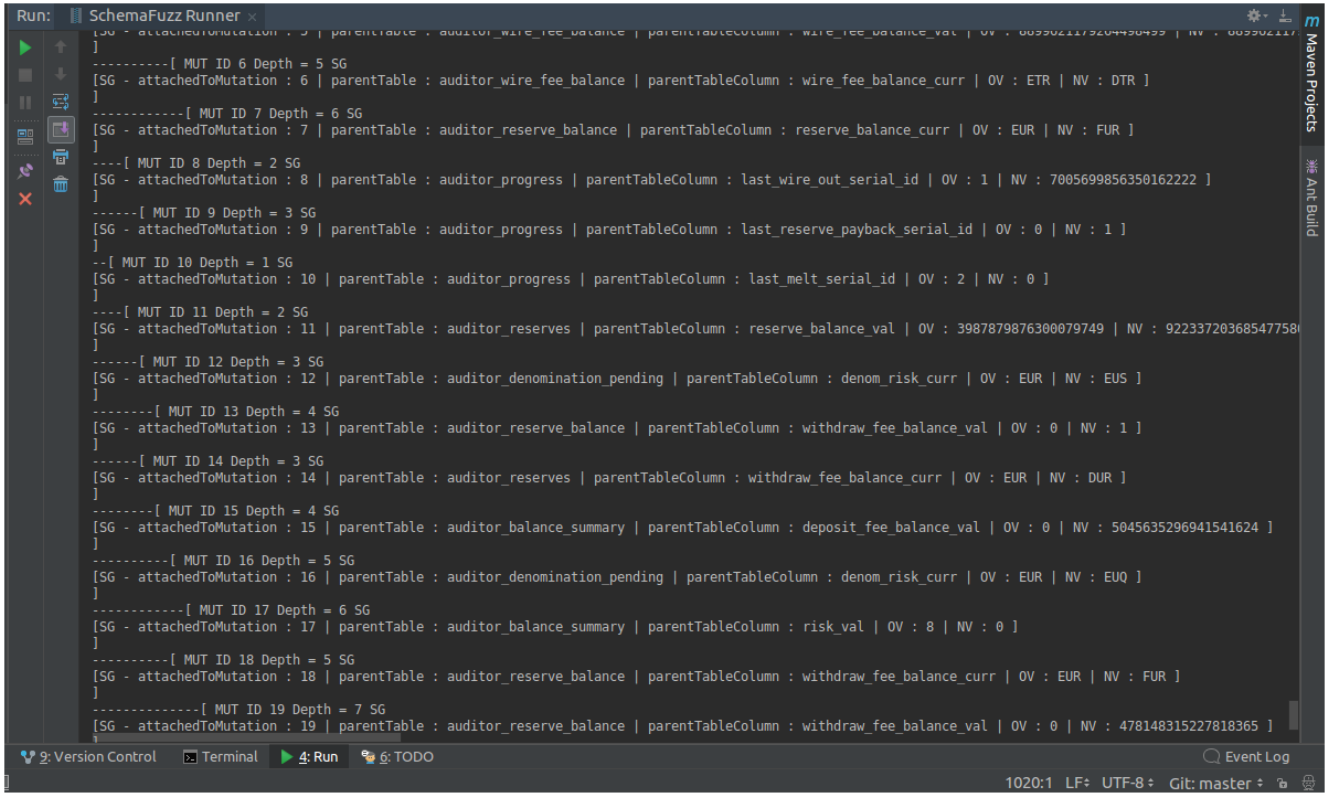


Obstacles and solutions

- SchemaSpy's code complexity
- Scheduling
- Structural thinking

Results

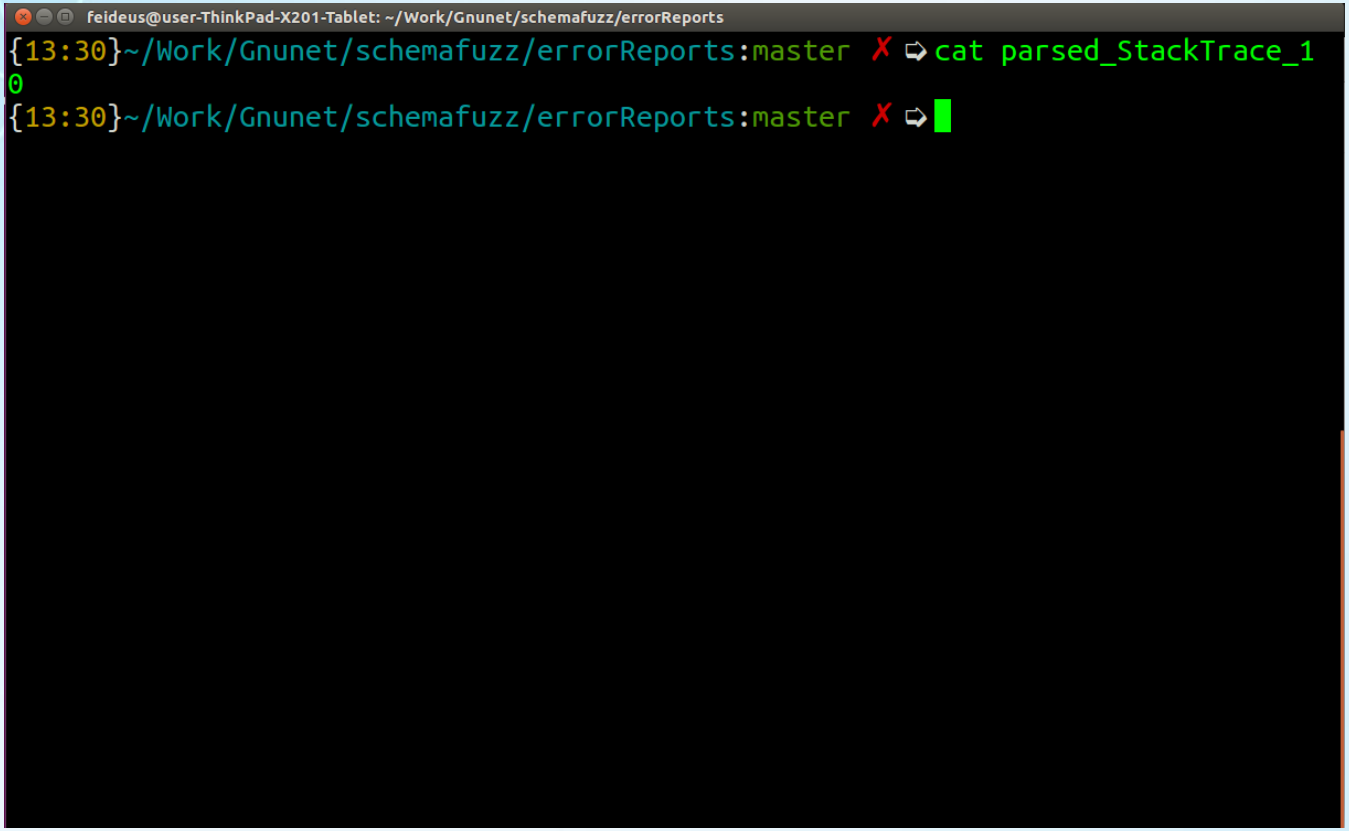
SchemaFuzz's output



Development environment

```
~/Work/GnuNet/schemafuzz/errorReports> cat parsedStackTrace_13          master!?
functionNames:
tmpfun2,
tmpfun,
main,
fileNames:
test_c_crash.c,
test_c_crash.c,
lineNumbers:
25
20
end:
path:
[SG - attachedToMutation : 1| OV :0 | NV :0 ]
[SG - attachedToMutation : 2| OV :138 | NV :32767 ]
[SG - attachedToMutation : 3| OV :163 | NV :4554 ]
[SG - attachedToMutation : 4| OV :31 | NV :15988 ]
[SG - attachedToMutation : 5| OV :72410 | NV :82410 ]
[SG - attachedToMutation : 6| OV :289 Santo Andr Manor | NV :289 Santo Andr Manoq ]
endpath:
~/Work/GnuNet/schemafuzz/errorReports>
```

Production environment



Enrichments

- Technical improvement
- Languages
- Work methodology

Conclusion