

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)



Berner
Fachhochschule



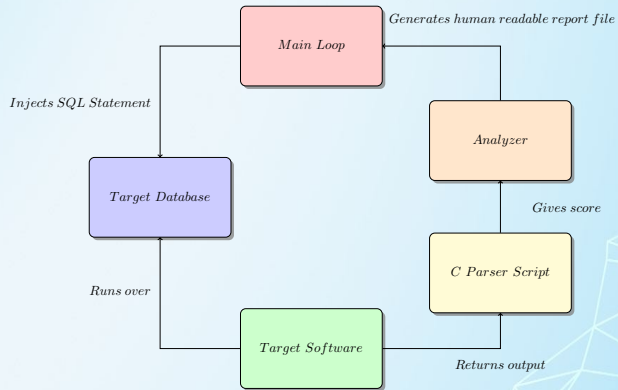
SchemaFuzz

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

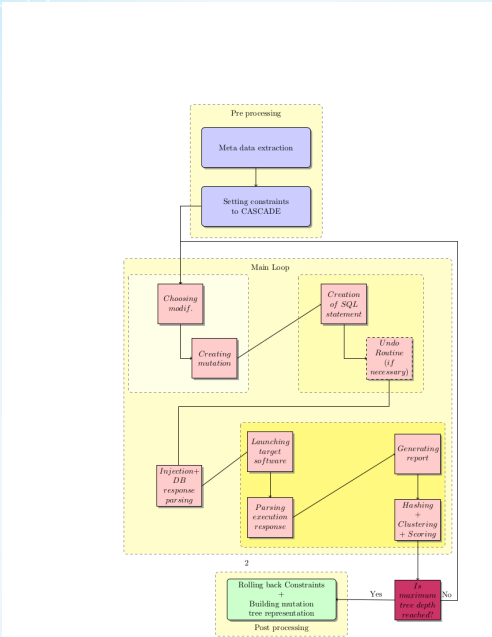
What is SchemaFuzz ?

- ▶ 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

```
Run: SchemaFuzz Runner
-----[ MUT ID 6 Depth = 5 SG
[SG - attachedToMutation : 6 | parentTable : auditor_wire_fee_balance | parentTableColumn : wire_fee_balance_curr | OV : ETR | NV : DTR ]
-----[ MUT ID 7 Depth = 6 SG
[SG - attachedToMutation : 7 | parentTable : auditor_reserve_balance | parentTableColumn : reserve_balance_curr | OV : EUR | NV : EUR ]
-----[ MUT ID 8 Depth = 2 SG
[SG - attachedToMutation : 8 | parentTable : auditor_progress | parentTableColumn : last_wire_out_serial_id | OV : 1 | NV : 798569985635816222 ]
-----[ MUT ID 9 Depth = 3 SG
[SG - attachedToMutation : 9 | parentTable : auditor_progress | parentTableColumn : last_reserve_payback_serial_id | OV : 0 | NV : 1 ]
-----[ MUT ID 10 Depth = 1 SG
[SG - attachedToMutation : 10 | parentTable : auditor_progress | parentTableColumn : last_melt_serial_id | OV : 2 | NV : 0 ]
-----[ MUT ID 11 Depth = 2 SG
[SG - attachedToMutation : 11 | parentTable : auditor_reserves | parentTableColumn : reserve_balance_val | OV : 3987879876380079749 | NV : 922337203685477580 ]
-----[ MUT ID 12 Depth = 3 SG
[SG - attachedToMutation : 12 | parentTable : auditor_denomination_pending | parentTableColumn : denom_risk_curr | OV : EUR | NV : EUS ]
-----[ MUT ID 13 Depth = 4 SG
[SG - attachedToMutation : 13 | parentTable : auditor_reserve_balance | parentTableColumn : withdraw_fee_balance_val | OV : 0 | NV : 1 ]
-----[ MUT ID 14 Depth = 3 SG
[SG - attachedToMutation : 14 | parentTable : auditor_reserves | parentTableColumn : withdraw_fee_balance_curr | OV : EUR | NV : EUR ]
-----[ MUT ID 15 Depth = 4 SG
[SG - attachedToMutation : 15 | parentTable : auditor_balance_summary | parentTableColumn : deposit_fee_balance_val | OV : 0 | NV : 5045635296941541624 ]
-----[ MUT ID 16 Depth = 5 SG
[SG - attachedToMutation : 16 | parentTable : auditor_denomination_pending | parentTableColumn : denom_risk_curr | OV : EUR | NV : EUR ]
-----[ MUT ID 17 Depth = 6 SG
[SG - attachedToMutation : 17 | parentTable : auditor_balance_summary | parentTableColumn : risk_val | OV : 8 | NV : 0 ]
-----[ MUT ID 18 Depth = 5 SG
[SG - attachedToMutation : 18 | parentTable : auditor_reserve_balance | parentTableColumn : withdraw_fee_balance_curr | OV : EUR | NV : EUR ]
-----[ MUT ID 19 Depth = 7 SG
[SG - attachedToMutation : 19 | parentTable : auditor_reserve_balance | parentTableColumn : withdraw_fee_balance_val | OV : 0 | NV : 478148315227818365 ]

Version Control Terminal Run TODO Event Log
1020:1 LP: UTF-8 Git: master
```

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

```
feldeus@user-ThinkPad-X201-Tablet: ~/Work/Gnunet/schemafuzz/errorReports
{13:30}~/Work/Gnunet/schemafuzz/errorReports:master X ↵ cat parsed_StackTrace_1
0
{13:30}~/Work/Gnunet/schemafuzz/errorReports:master X ↵ █
```

Enrichments

- ▶ Technical improvement
- ▶ Languages
- ▶ Work methodology

Conclusion