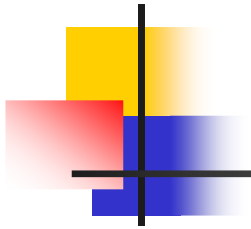


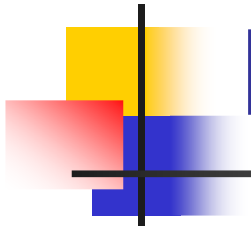
# nuf-fuzzer

**Samostatná práca**

**A4M35OSP - Open-Source programování**

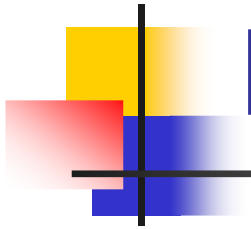
**Michal Strelec (strelmic)**

**2010/2011**



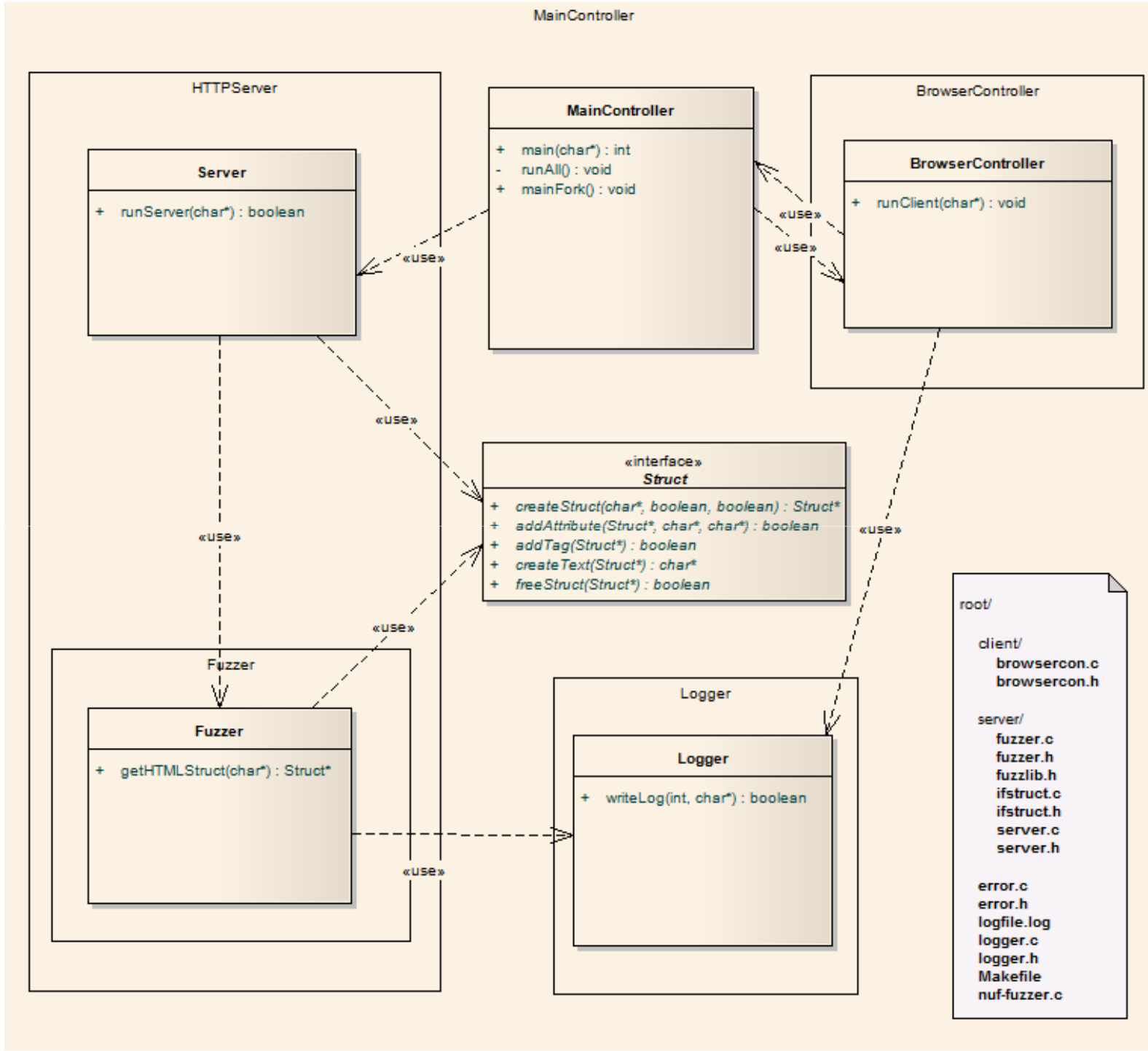
# Popis projektu

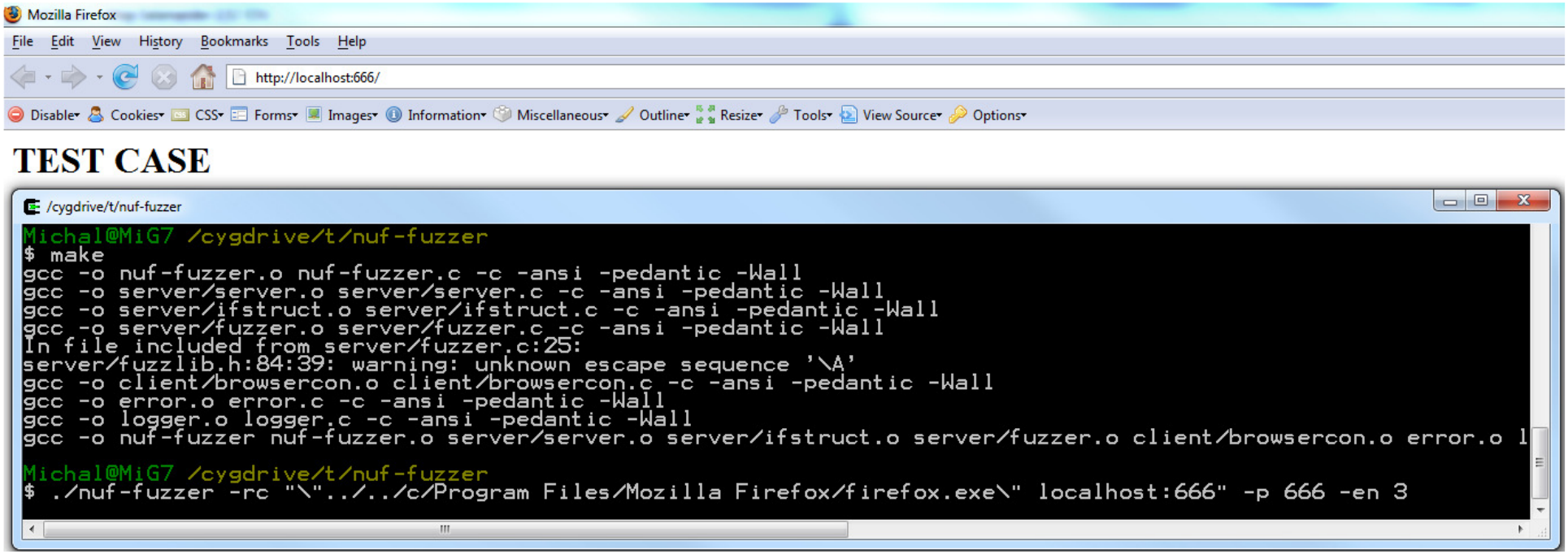
- **Nový projekt**
  - Projekt ešte neexistuje
- **Browser fuzzer**
  - Hľadá bezpečnostné chyby
  - Fuzovanie CSS, DOM, HTML, JavaScript
- **Ako sa bude používať**
  - Program beží nonstop
  - Ak browser padne, program to zaloguje, znovu sa spustí browser a pokračuje bez zásahu operátora
- **Motivácia**
  - The Mozilla Security Bug Bounty Program ($500 - $3000 odmena)



# Moja úloha v projekte

- **Naprogramovať komponentu HTTPServer**
  - Jednoduchý HTTP server pre potreby fuzzeru
  - Podpora HTTPS
  - Po requeste z webového prehliadača, zoberie výstup fuzzeru, vytvorí z neho adekvátnu www stránku a pošle ju prehliadaču. Zároveň pomocou rozhrania medzi HTTPServrom a hlavnou časťou programu zašle informácie čo bolo fuzovane a akým vstupom.

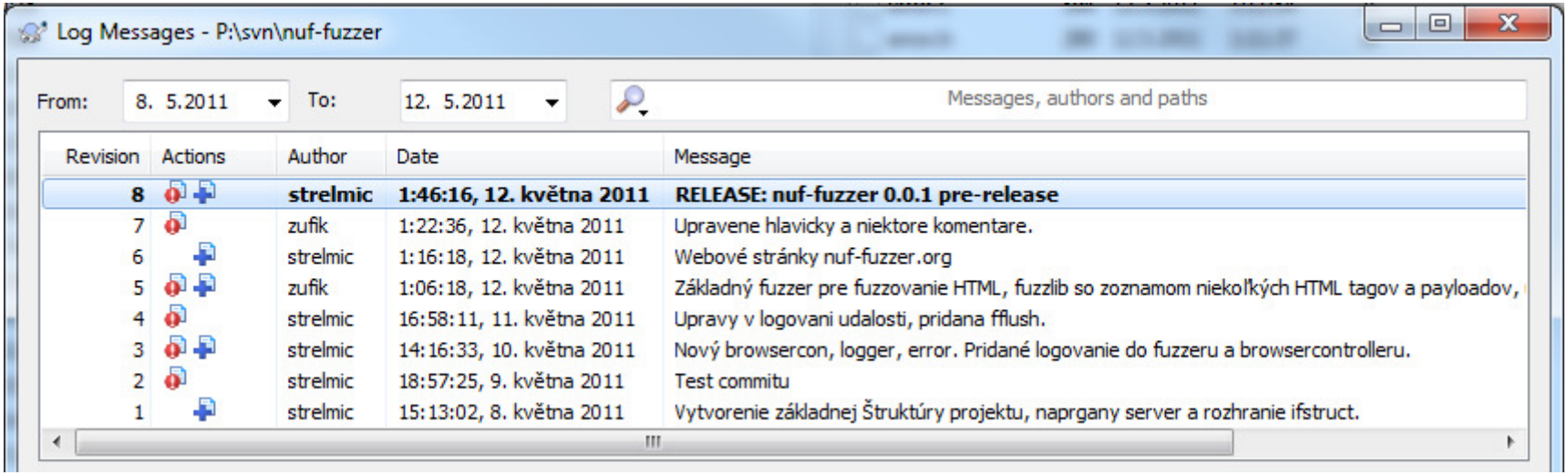

MainController
HTTPServer
Server
+ runServer(char*) : boolean
MainController
+ main(char*) : int
- runAll() : void
+ mainFork() : void
BrowserController
BrowserController
+ runClient(char*) : void
«use»
«use»
«use»
«use»
«use»
«use»
«use»
«use»
«interface»
Struct
+ createStruct(char*, boolean, boolean) : Struct*
+ addAttribute(Struct*, char*, char*) : boolean
+ addTag(Struct*) : boolean
+ createText(Struct*) : char*
+ freeStruct(Struct*) : boolean
Fuzzer
Fuzzer
+ getHTMLStruct(char*) : Struct*
Logger
Logger
+ writeLog(int, char*) : boolean
root/
client/
browsercon.c
browsercon.h
server/
fuzzer.c
fuzzer.h
fuzzlib.h
ifstruct.c
ifstruct.h
server.c
server.h
error.c
error.h
logfile.log
logger.c
logger.h
Makefile
nuf-fuzzer.c

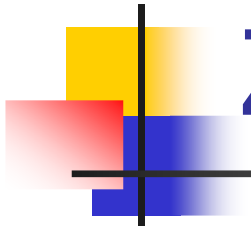



```
28 FUZZER: applet;alt;7;4;13;4;13;3;110;0;4;7;4;9;13;5;55;9;4;5;7;1;410;0;110;5;13;6;4;4;13;4;110;5;2;9;110;8;7;6
29 Thu May 12 00:57:19 2011
30 FUZZER: applet;height;4;4;410;9;7;9;110;8;7;4;55;1;410;6;7;4;2;3;110;6;110;6;7;7;2;9;410;8;55;2;4;9;410;6;55;9;110;7;55;0;13;2;55;6;13;5
31 Thu May 12 00:57:21 2011
32 FUZZER: applet;width;410;5;4;2;7;3;110;7;55;1;110;1;13;7;410;9;55;0;4;1;4;3;13;9;55;5;4;0;410;1
33 Thu May 12 00:57:24 2011
34 BROWSER DOWN
35
36 Thu May 12 00:57:26 2011
37 FUZZER: applet;hspace;2;3;13;0;2;3;55;7;13;8;4;6;2;9;110;4;13;2;55;3;13;4;110;6;13;5;410;0;410;3;55;2
38 Thu May 12 00:57:27 2011
39 FUZZER: applet;vspace;13;3;4;7;110;2;4;0;2;3;410;7;4;8;55;7;410;8;410;4
40 Thu May 12 00:57:30 2011
41 BROWSER DOWN
42
43 Thu May 12 00:57:32 2011
44 FUZZER: applet;download;55;1;110;5;4;0;110;2;4;9;4;2;110;0;13;9;110;9;7;6;4;0;55;9;410;7;4;8;13;1;110;9;410;3;7;4;4;9
45 Thu May 12 00:57:33 2011
46 BROWSER DOWN
47
48 END SEARCH
```

# Spolupráca

- **SVN**
- **ICQ**
- **osobné schôdzky**





# Záver

- **Prvá fáza projektu sa celkovo podarila**
  - Málo času
  - Zmena zadania - podpora HTTPS, na viac administrátorská činnosť a publikovanie (nuf-fuzzer.org)
  - Zatiaľ len veľmi jednoduchý HTML fuzzer

# Ďakujem za pozornosť