

Noel-Lardin Thomas
Lang Ludovic
Moissonnier Shane
Martinez Anthony

Compte-rendu séance 5 :

Voici un programme que nous avons écrit dont l'erreur est détectée par AFL :

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[]) {
    FILE *f;
    char ligne[100];
    f=fopen(argv[1],"r");
    fscanf(f,"%s",ligne);
    char mot[5];
    strcpy(mot,ligne);
}
```

Si le mot contenu dans le fichier ouvert par le programme est trop grand alors une erreur est provoquée, par exemple AFL nous renvoi :

```
#####
#####
#####
```

Ensuite nous avons exécuté AFL sur le programme vulnerable.c, voici l'une des entrées qui provoque une erreur sur le programme :

```
head 2222222222220
```

Qui est lié à un problème avec un des free() exécuté dans le code.

Pour utiliser ce nouvel outils sur notre projet, nous avons changé le Makefile pour qu'il puisse compiler avec le compilateur afl-gcc lorsqu'on lui donne le paramètre AFL=1.

Nous avons trouvé 2 erreurs lors de l'exécution de AFL sur notre projet. Pour remédier à ces erreurs nous avons ajouté des séparateurs au macro SEP, et nous avons corrigé la fonction next_word pour que le programme s'arrête si le caractère n'est pas en minuscule.