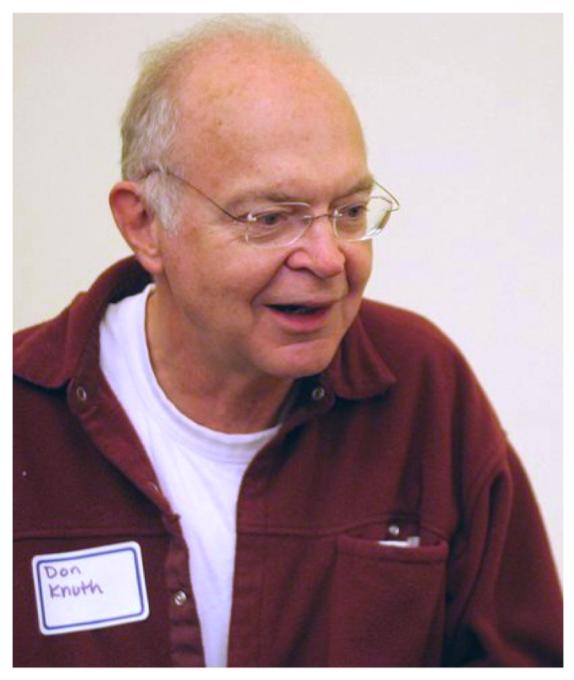




# INJECTIONS LATEX

Les plus beaux shells de votre vie



# LaTeX ?

- Système de macro pour TeX
- Donald Knuth
- Véritable langage de programmation
- Production de documents scientifiques...

# Exemple

Balisage	Rendu
<pre>Les solutions de \$ax^2+bx+c=0\$ sont \$- b\pm\sqrt{b^2-4ac}\over2a\$. \bye</pre>	Les solutions de $ax^2 + bx + c = 0$ sont $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ .

# La compilation

- Le moteur : `pdfTeX`
- `latex` versus `pdflatex`
- C'est à ce moment qu'on fait du sale

# Lecture

- `\input{/mon/fichier}`
- Si le fichier termine par `.tex` : `\include{/mon/fichier(.tex)}`
- Ou encore :

```
\newread\file
\openin\file/usr/share/texmf/web2c/texmf.cnf
\loop\unless\ifeof\file
    \read\file to\fileline
    \text{\fileline}
\repeat
\closein\file
```

# Ecriture

- Ecraser un fichier sensible (logs ?)
- Gagner un autre point d'entrée (SSH ?)
- Préparer une exécution de commande

```
\newwrite\outfile  
\openout\outfile=ZBEUB  
\write\outfile{3P1T3CH}  
\closeout\outfile
```

# Exécution

- Trois niveaux de difficulté
- -no-shell-escape
- -shell-restricted
- -shell-escape
- <https://0day.work/hacking-with-latex/>
- <http://scumjr.github.io/2016/11/28/pwning-coworkers-thanks-to-latex/>

# Du coup...

- La sainte trinité : RWX
- Sécurité par filtre ?
- **Conteneuriser**
- LuaTeX

# Des questions ?

@+