Teaching Security

Cédric Lauradoux
Most of my students have never followed a programming course...

- File - You mean a .mp3 file?
- Filesystem - Windows 7
- Code/Executable/Data - You mean a .html file?

... I was super depressed! (Awesome colors!)
WHAT I TRY TO PUT IN THEIR BRAINS:

- Lab 1 - File: data/metadata, puzzling, logic bombs, chameleons, werewolves
- Lab 2 - Filesystem: forensics, hashing, carving, covert channels
- Lab 3 - Symmetric crypto: openssl
- Lab 4 - Rest of crypto: openssl
- Lab 5 - Password: john, wget, wget2, cewl
- Lab 6 - Mock exam
#!/usr/bin/env bash
TARGET=$1
length="100 8 8 8 12 12 8 1 100 8 2 32 32 8 8 155"

for offset in 0 100 188 116 124 136 148 156 157 257 263 265 297 329 337 345; do
cp $TARGET tmp.tar
dd if=/dev/urandom of=tmp.tar bs=1 count=${length[$offset]} seek=${offset} conv=notrunc status=none
printf '
' | dd of=tmp.tar bs=1 count=8 seek=148 conv=notrunc status=none
chksum -f$HEAD < $500 tmp.tar | sun -c
printf "%80s" $chksum | dd of=tmp.tar seek=148 bs=1 count=8 conv=notrunc status=none
tar tfv tmp.tar >> log 2>> log
rm tmp.tar

done
THANK YOU!