???

Gabriel Laskar <gabriel@lse.epita.fr>

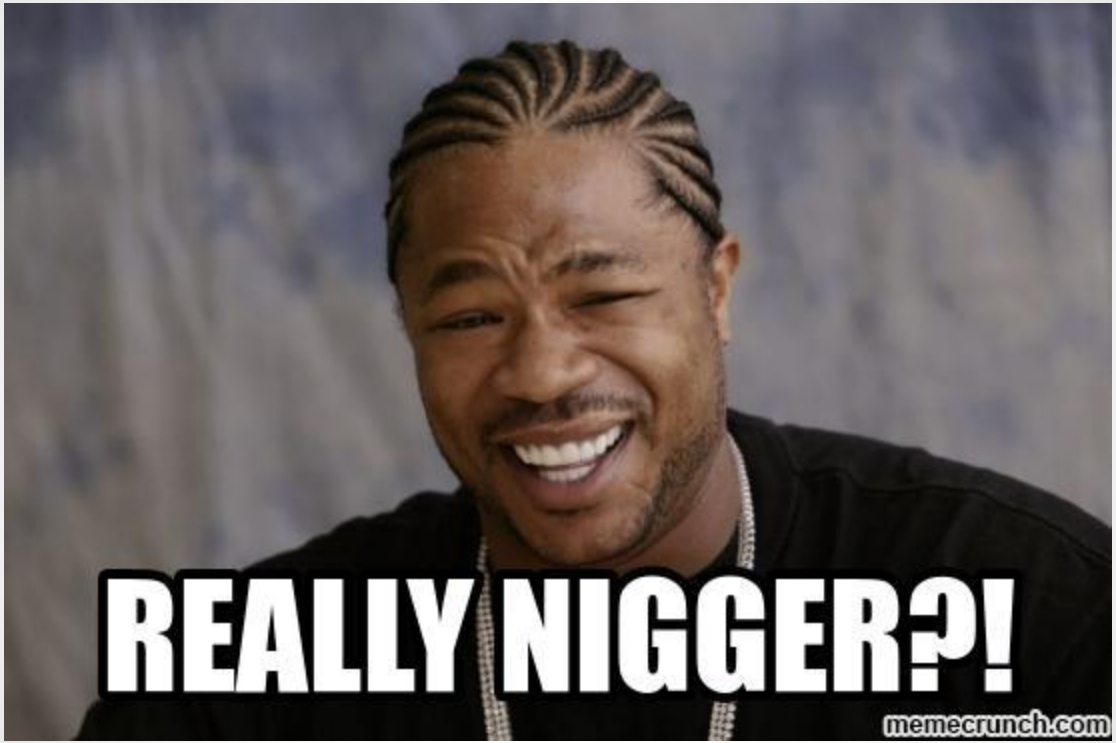
LSE Security System

```
int lets_segv()
{
    char *ptr = (char *)0;
    printf("%c\n", *ptr);
    return 0;
}

int main()
{
    try {
        lets_segv();
    } catch (const std::exception &e) {
        printf("[!] exception : segv!\n");
    }

    return 0;
}
```

LSE Security System



LSE Security System

```
template <int SigNum>
struct SigExcept {
      static void install() {

            struct sigaction sig;
            sig.sa_sigaction = SigExcept<SigNum>::handler;
            sig.sa_flags = SA_SIGINFO | SA_ONSTACK;

            sigaction(SigNum, &sig, NULL);
      }

      static void handler(int, siginfo_t *, void *ptr) {
            ucontext_t *ctx = (ucontext_t *)ptr;

            ctx->uc_mcontext.gregs[REG_RSP] += 8;
            *(greg_t *)ctx->uc_mcontext.gregs[REG_RSP] =
                  ctx->uc_mcontext.gregs[REG_RIP];

            ctx->uc_mcontext.gregs[REG_RIP] =
                  (greg_t)SigExcept<SigNum>::throw_exception;
      }

      static void throw_exception() {
            throw signal_exception<SigNum>();
      }
};
```

LSE Security System