به نام خدا

پخش ویدیوی سخن‌رانی

BlackHat

The 48 Dirty Little Secrets Cryptographers Don't Want You To Know

16 February 2016

شاخه ی دانشجویی

انجمن رمزایران

در دانشگاه صنعتی شریف

۲۷ بهمن ۱۳۹۴

انجمن رمزایران
iranian Society of Cryptology

چکیده

- **رویداد چالش‌های رمزنگاری Matasano**
  - بیش از ۱۰,۰۰۰ نفر شرکت‌کننده
  - پیاده‌سازی ۴۸ حمله‌ی مختلف برای ساخت‌های واقعی رمزنگارانه
- **چندین کد Exploit برای آسیب‌پذیری‌های رمزنگارانه جمع‌آوری شدند**
  - به زبان‌های گوناگون
  - از زبان X86 Assembly تا Haskell

شاخه‌ی دانشجویی
انجمن رمز ایران در
دانشگاه شریف

کُدها

چالش‌های گفته‌شده در وب‌گاه زیر قرار دارند:

http://cryptopals.com

سخن‌ران‌ها

- Thomas Ptacek (@tqbf)
- Sean Devlin (@spdevlin)
- Alex Balducci (@iamalexalright)
- Marcin Wielgoszewski (@marcinw)

راه‌های ارتباطی

وب گاه شاخه

http://sbsharif.isc.org.ir/

لیست رایانامه‌ای

http://lists.ce.sharif.edu/cgi-bin/mailman/listinfo/sbisc

کانال تلگرام

http://telegram.me/sbsharif

شاخه‌ی دانشجویی
انجمن رمز ایران در
دانشگاه شریف