

How I Met Your Girlfriend

Samy Kamkar

ISCTE-IUL (Auditório B1.04)

15 de Outubro 2010, 18h30



OWASP

The Open Web Application Security Project



Samy Kamkar é mais conhecido pelo primeiro *worm* XSS (Samy *worm*) que desenvolveu para o MySpace, e que infectou mais de um milhão de utilizadores em menos de 24 horas. É co-fundador da Fonality, Inc., uma empresa de produtos de IP PBX, e liderou anteriormente o desenvolvimento de todo o software de gestão do servidor de nomes dos domínios de topo para a Global Domains International.

Nos últimos 10 anos, o Samy tem-se focado no desenvolvimento de software de algoritmos genéticos e evolucionários, voz sobre IP, pesquisa automática de vulnerabilidades de segurança, *reverse engineering*, e jogos através da rede.

How I Met Your Girlfriend: nesta palestra, Samy Kamkar vem apresentar a descoberta e execução de uma classe de ataques completamente novos que podem ser executados através da Web por forma a travar conhecimento com a sua namorada. Ao longo da sua apresentação, Samy vai falar de um conjunto de novos ataques descobertos, incluindo HTML5 XSS do lado do cliente (sem que o ataque de XSS chegue ao servidor), roubo de sessões e fraca aleatoriedade de números no PHP (adivinhandando com precisão os cookies de sessão em PHP), confusão de protocolos no browser Web (tornando um browser num servidor SMTP), penetração de firewalls e NAT através de Javascript (colocando o router a funcionar contra o utilizador), rapto remoto do Google Maps no iPhone (penetração no iPhone combinado com um ataque man-in-the-middle HTTP), extracção de informação de geo-localização precisa do browser Web (não recorrendo a geo-localização por IP), e muito mais.

Esta sessão, organizada pela OWASP em conjunto com o ISCTE-IUL e ADETTI-IUL, foi igualmente apresentada numa das maiores conferências de Segurança do Mundo, a BlackHat 2010, que se realizou em Las Vegas nos EUA, e faz parte de um Tour Europeu que o Samy está a realizar (mais de 10 cidades da Europa).