Web Security and the OWASP Top 10: The Big Picture

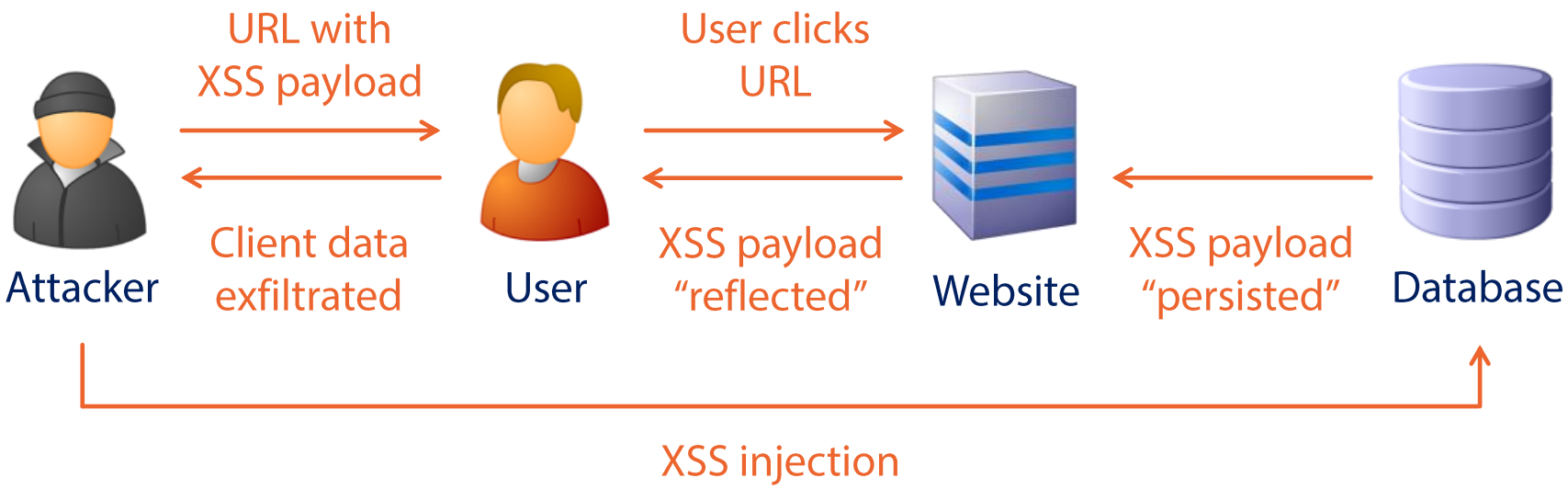
Cross-Site Scripting (XSS)

Troy Hunt
troyhunt.com
@troyhunt

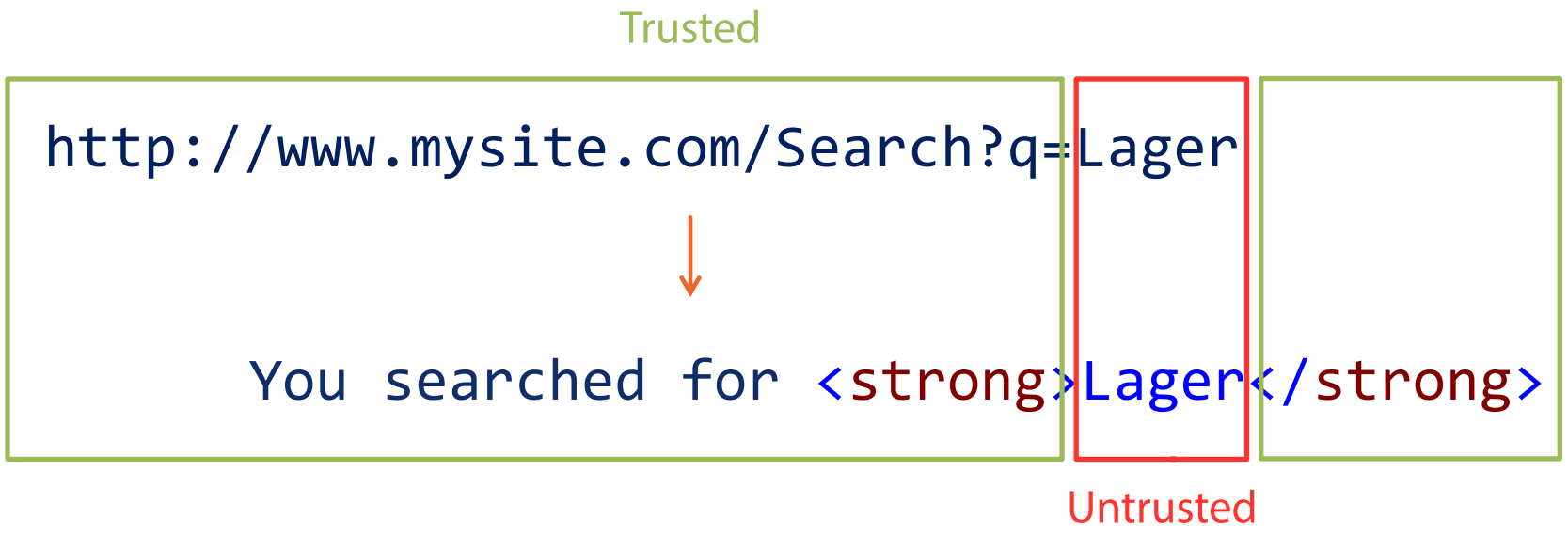
pluralsight
hardcore developer training

XSS Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Average	Prevalence Very Widespread	Detectability Easy	Impact Moderate



Understanding XSS



Common Defences Against XSS Attacks

Whitelist
untrusted data

- What input do we *trust?*
- Does it adhere to expected patterns?

Always
encode output

- Never simply reflect untrusted data
- This applies to data in your own DB too

Encode for
context

- HTML / attributes / JavaScript / CSS
- Wrong encoding in wrong context is useless

XSS in the Wild – Samy's MySpace Hack

Samy Kamkar

From Wikipedia, the free encyclopedia

Samy Kamkar (born December 10, 1985)[1] is a privacy and security researcher, computer hacker, whistleblower and entrepreneur. At the age of 17, he co-founded Fonality, a unified communications company, which raised over $24 million in private funding.[2] He is possibly best known for creating the Evercookie, which appeared in a top-secret NSA document[3] and the front page of the New York Times,[4] and the MySpace worm Samy (XSS), over which he was subsequently raided by the United States Secret Service for creating and releasing.[5] He is also known for his work with The Wall Street Journal and his discovery of the illicit mobile phone tracking where the Apple iPhone, Google Android and Microsoft Windows Phone mobile devices transmit GPS and Wi-Fi information to their parent companies. His mobile research led to a series of class-action lawsuits against the companies and a privacy hearing on Capitol Hill.[6]

Work [edit]

Samy Worm [edit]

Main article: Samy (XSS)

In 2005, Kamkar released the Samy worm, the first self-propagating cross-site scripting worm, onto MySpace.[7] The worm carried a payload that would display the string "but most of all, Samy is my hero" on a victim's profile and cause the victim to unknowingly send a friend request to Kamkar. When a user viewed that profile, they would have the payload planted on their page. Within just 20 hours[8] of its October 4, 2005 release, over one million users had run the payload,[9] making Samy the fastest spreading virus of all time.[10] The MySpace team temporarily shut down MySpace to fix the problem that allowed the worm to operate.

In 2006, Kamkar was raided by the United States Secret Service and Electronic Crimes Task Force, expanded from the USA PATRIOT Act, for releasing the worm.[5] Kamkar pled guilty to a felony charge of computer hacking in Los Angeles Superior Court, and was prohibited from using a computer for three years. Since 2008, Kamkar has been doing independent computer security and privacy research and consulting.[11]

Samy Kamkar

Born	December 10, 1985 (age 28)
Occupation	Privacy and security researcher, computer hacker, whistleblower and entrepreneur
Known for	Releasing the Samy worm, Evercookie, and iPhone, Android and Windows Mobile phone tracking research
Website	samy.pl