AUBURN

Case Study
Samy Cross Site Scripting Worm

Samy Cross Site Scripting Worm

AUBURN

- October 4th, 2005 “Samy” worm was released on MySpace website through user input
  - Created by Sam Kamkar – now ethical hacker

- Injected javascript through the user interface into a users profile
  - Added “but most of all, Samy is my hero” on users profile
  - Replicate itself to a users profile, infecting others users when they look at a profile, replicating itself again.
  - Samy worm spread quickly since MySpace (at the time) largest social media website.
  - To this day it is the fastest spreading virus. < 1 day –> 20 million users.
  - Shutdown MySpace website

Samy Cross Site Scripting Worm

AUBURN

- What weaknesses caused the vulnerability:
  - MySpace accepted user input without any validation
  - User pages allow a high degree of customization.
  - User content was stored and served up later as javascript

- What happened to Samy Kamkar
  - 3 years probation with only one computer w/ no internet access
  - 90 days community service
  - Only allowed 1 computer
  - ~15,000 in restitution

Cross Site Scripting Prevention

AUBURN

- Application Level
  - User content should ALWAYS be scrubbed for invalid content (database, javascript, etc.).
  - HTML Special characters should always be encoded so as not to be interpreted as HTML

- Browser Controls
  - Browser including more controls against common known web vulnerabilities
  - **Content-Security-Policy** – passed back from server letting browser know only valid domains to execute scripts from.
  - **Header'X-XSS-Protection'** configured to block.
    - Tells browser to to block XSS code when detected
    - Modern Browsers are starting to deprecate this in favor of Content Security Policy (CSP)

AUBURN UNIVERSITY