Insecure Code

Sam Marshall

What makes code "insecure"

- Code is hard
- Mistakes will happen

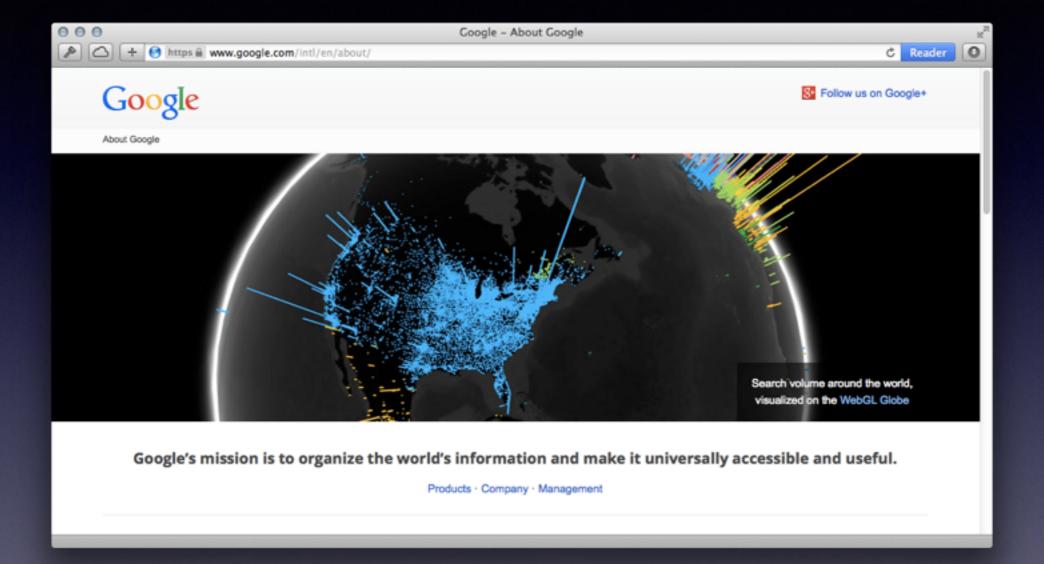
Input Handling

That game studio that cannot count to "3"

What is a valid URL string?

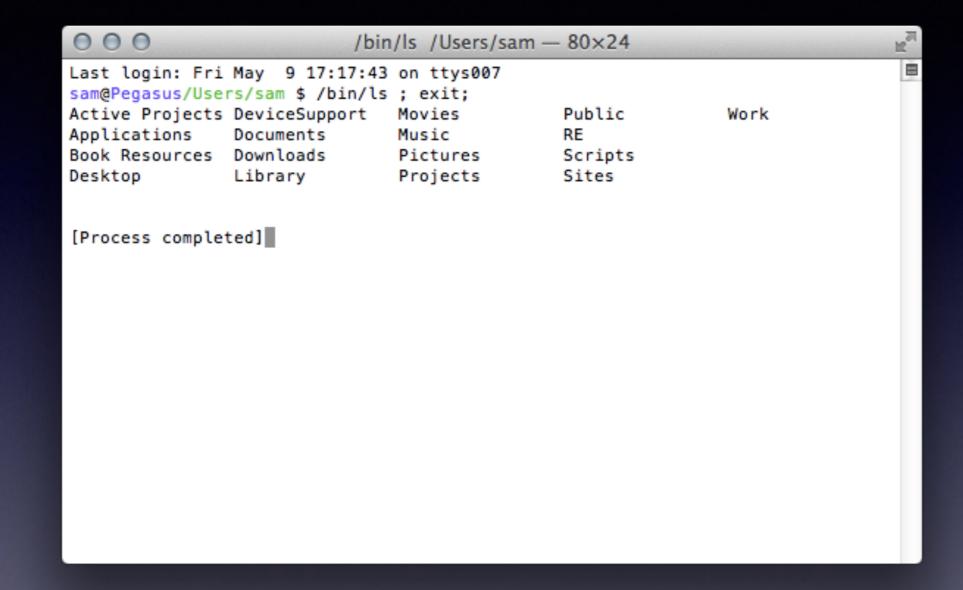
- "http://" e.g. "http://altconf.com"
- "https://" e.g. "https://developer.apple.com"
- "www." e.g. "www.samdmarshall.com"

- Input: "https://www.google.com/intl/en/about/"
- Strip out "https://" and "www."
 - "google.com/intl/en/about/"
- Split by "/"
 - ["google.com", "intl", "en", "about", ""]
- If first item length is greater than zero, put back prefixes
- Join array
 - "https://www.google.com/intl/en/about/"



www./bin/ls

- Input: "www./bin/ls"
- Strip out "www."
 - "/bin/ls"
- Split by "/"
 - ["", "bin", <u>"</u>Is"]
- First element is an empty string! Do not restore prefix
- Join array by "/"
 - "/bin/ls"



The Fix

- Verify URL types
 - - [NSURL isFileReferenceURL]
 - - [NSURL isFileURL]

Concurrency The Fruit Company

Use for Development

- Copy developer tools over to the mobile device
- Verify the authenticity of developer disk image
- Copy disk image into staging environment
- Mount disk image to allow developer access

- Copy developer tools over to the mobile device
- Verify the authenticity of developer disk image
- Rename developer tools disk image (preserving FS ref)
- Copy custom disk image to the mobile device
- Copy (custom) disk image into staging environment
- Mount (custom) disk image to allow developer access

The Fix

- Latest public release changes how disk images are verified and mounted
- Disk Image is moved directly to a private staging environment to be verified then mounted.

Credits

@yaakov_h (URL parsing bug)

@winocm (disk image bug)

@Dirk_Gently me@samdmarshall.com samdmarshall.com

samdmarshall.com/altconf/