

# 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.samdmarsshall.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/”


Google - About Google

https://www.google.com/intl/en/about/ Reader

Google

Follow us on Google+

About Google



Search volume around the world, visualized on the WebGL Globe

**Google's mission is to organize the world's information and make it universally accessible and useful.**

[Products](#) · [Company](#) · [Management](#)

[www./bin/lS](http://www./bin/lS)

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



```

/bin/ls /Users/sam — 80x24
Last login: Fri May  9 17:17:43 on ttys007
sam@Pegasus/Users/sam $ /bin/ls ; exit;
Active Projects DeviceSupport  Movies          Public          Work
Applications    Documents    Music           RE
Book Resources  Downloads   Pictures        Scripts
Desktop         Library     Projects       Sites

[Process completed]
```

# 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/