Are You Coding Safely? A Guideline for Web Developers

Chun-Chan Cheng
Department of Computer Science and Engineering
Texas A&M University
Email: aznchat@tamu.edu

Chia-Cheng Tso
Department of Computer Science and Engineering
Texas A&M University
Email:

I. Introduction

With the proliferation of hand-holding devices, the ubiquitous accessibility has been a norm for today's applications. Now basically every service supports an on-demand access through all kinds of devices, and here comes Web applications.

Web applications have many advantages over traditional ones which require installation: 1. It works on every platform as long as there's a web browser. This takes a lot of pains off the engineer, since once a job done, it works everywhere. No more customization for different platforms. No more seperated team members. 2. Patch the application instantely, which people usually ignore. No more asking for user to upgrade 3. fast deploy, fast prototype, light-weighted best to get feedback from market.

Due to its advantages, tons of framework/language emerge.

with the help of new language, new framework building an website/web application becomes very easy. everybody can code

And there are many more pitfall While engineer are busying on bring out all the functionalities, they may not have time to work on secuirty.

Our propose here is to provide some simple, clear but useful guidelines to help engineer code with "good habits"

Note that our goal here is not to cover every vulneribilities, which is intuitively impossible. Our goal here is to cover as many problems as possible with minimal efforts.

You might think it's not good enough. However, the concept of security is that if the value of the data in your website least than the effort that one need to break in, then, in this case, the protection should be sufficient.

20/80 law most of the easy vulneribilities should be able to eliminated. avoid most of vulnerability by void bad coding style.

It's not likely to notice every single problem without the help of scanner or static analyzer, however,

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.