Notes on Improving Website Security

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems

School of Business & Management

Norwich University

The editing marathon continues. Here are a couple of additions I made to a chapter on Website security.

Embedded Identifiers in URLs

Sometimes registration or unsubscribe messages include personalized URLs; for example, “To unsubscribe, click on < http://www.some-company.com/unusbscribe/?=12345 >. The problem is that the identifying code (12345 in the example) can be replaced by any other number – and some of the generated numbers will unsubscribe other subscribers. Another unfortunate use of such a technique occurs in email messages for participation in Webinars; sometimes the coded URL in the email goes directly to a registration page with information filled in – information such as the precise name, email address, and employer information drawn from the database of previous contacts.

In general, it is poor practice to provide such short identifiers that a user or a simple program or batch file could be used to delete valid records in a database or to harvest confidential data from a Website. For example, a simple html file in Adobe Acrobat can be used to force the program to access every URL in the file; if a malefactor has created, say, 20,000 unique identifiers and all or most of them are affiliated with real people, the malefactor could easily affect the accounts or collect the information shown on the customer-specific pages.

To avoid such problems, either create an address space with far more possible identifier values than a 1:1 mapping of real accounts to identifiers; e.g., for a 100,000-person list, use generated values using a string of 20 positions with 94 values per position available in uppercase, lowercase, numbers, and special characters, resulting in 94^20 = 10^39 keyspace, far beyond anything manageable by an amateur.

Browser-Platform Security

An increasingly important platform for considerations of Website security is smart phones. By the end of 2012,

> There were 2.1 billion mobile Web users in the world at the end of 2012.
>
> According to estimates by The ITU (June, 2012), there were 2.1 billion active mobile-broadband subscriptions in the world. That is 29.5 percent of the global population.
>
> Mobile-broadband subscriptions have grown 40 percent annually over the last three years.
>
> Mobile-broadband subscription outnumber fixed broadband subscriptions 3:1.
>
> In developed countries mobile-broadband users often also have access to a fixed-broadband connection, but in developing countries mobile broadband is often the only

> access method available to people.
>
> Ericsson (November 2012) forecasts that global mobile broadband subscriptions will reach 1.5 billion at the end of 2012, and 6.5 billion in 2018. The mobile phone will continue to be the dominant mobile broadband access device. [1]

Tablets also have their own versions of browsers. Web designers are increasingly having to cope with significant differences among platforms accessing their code.

Craig Smith included the following points in a January 2013 article entitled, “Optimizing Ecommerce for Tablets and Smartphones:”

- Improving navigation and usability: users should be able to select options easily and correctly; avoid drop-down menus and buttons that are close together.
- Leveraging responsive design: determine how to present the Website according to what kind of device is accessing it.
- Determining the purpose of the access: distinguish between the types of queries that are most common – and different – across platforms. Optimize design for the most common types for each platform.[2]

Another question is whether ecommerce sites should depend on Web access or develop applications (apps) specifically for smartphone and tablet operating systems. A major advantage of apps is that they can be programmed to avoid the vulnerabilities common to mobile devices in these early years of widespread adoption.

Notes:

[1] C. Smith, “Optimizing Ecommerce for Tablets and Smartphones.” Practical ecommerce (2013-01-15). http://www.practicalecommerce.com/articles/3869-Optimizing-Ecommerce-for-Tablets-and-Smartphones

[2] D. Traxler, “Mobile Commerce: Website or App?” Practical ecommerce (2013-01-01). http://www.practicalecommerce.com/articles/3862-Mobile-Commerce-Website-or-App-

For Further Reading:

Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd edition . Wiley, 2008.

Bhargav, A. and B. V. Kumar. *Secure Java: For Web Application Development.* CRC Press, 2010.

Cobb, Stephen. *Privacy for Business: Web Sites and Email*. Dreva Hill, 2002.

Elliott, E. *Programming JavaScript Applications: Robust Web Architecture With Node, HTML5, and Modern JS Libraries.* O’Reilly Media, 2013.

Gabarro, S. A. *Web Application Design and Implementation: Apache 2, PHP5, MySQL, JavaScript, and Linux/UNIX*, 2nd edition. Wiley, 2013.

Gookin, D. *Android Phones for Dummies.* For Dummies, 2013.

Gunasekera, S. *Android Apps Security*. Apress, 2012.

Harwani, B. M. *Android Programming Unleashed.* Sams, 2012.

Kissoon, T. *Securing Web Applications.* Auerbach, 2013.

Long, F., D. Mohindra, R. C. Seacord, D. F. Sutherland and D. Svoboda. *The CERT Oracle Secure Coding Standard for Java.* Addison-Wesley Professional, 2011.

Mark, D., A. Horovitz, K. Kim and J. LaMarche. *More iOS 6 Development: Further Explorations of the iOS SDK.* Apress, 2012.

McGraw, G., and E. Felten. *Securing Java: Getting Down to Business with Mobile Code* 2nd edition. Wiley, 1999.

Musciano, C., B. Kennedy and E. Weyl. *HTML5: The Definitive Guide,* 7th edition. O'Reilly Media, 2014.

Scambray, J., Shema, M., and C. Sima. *Hacking Exposed Web Applications*, 2nd ed. San Francisco, CA: McGraw-Hill Osborne Media, 2006.

Six, J. *Application Security for the Android Platform: Processes, Permissions, and Other Safeguards.* O'Reilly Media, 2011.

Sullivan, B. *Web Application Security, A Beginner's Guide.* McGraw-Hill Osborne Media, 2011.

Welling, L. and L. Thomson. *PHP and MySQL Web Development*, 5th Edition. Addison-Wesley Professional, 2013.

Zalewski, M. *The Tangled Web: A Guide to Securing Modern Web Applications.* No Starch Press, 2011.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

*** * ***