Web Design Security: Foundation Not Feature

Anglin, N., Hurley, I., Jackson, W., Redeemer, K., Scott, J., & West, C.
Computers and Society, Section 2 - Group A
School of Computing
College of Science and Technology
University of Southern Mississippi
118 College Drive, Hattiesburg, MS 39406

Abstract:

We aim to discuss the importance of security in web design. People interact with web pages and applications on a daily basis, and every day, users input private information into these web pages. In this paper, we examine the history and present state of web design security by looking at examples of web design flaws and hacks. We explore how and why attacks occur over the Internet, and we study the types of media and software used to harass/infect people/machines. We discuss the background of web hacking and argue that security is of the utmost importance when it comes to developing web applications and must be a foundation of the service being developed, not merely a feature. Finally, we evaluate the ethical shortcomings of programmers who use their knowledge for malicious purposes.

Keywords: web design, security, hacking, web application, data protection, computer ethics.

Introduction:

Since the Internet became a large exchange of public information, there have been hackers who wanted to exploit the system, cause mischief, and steal what is not theirs. Today, a fierce war is being fought behind the scenes of the Internet. Each day, 2,000,000 websites, and just as many if not more consumers, are infected with malicious code (Norton, 2012). Programmers around the world are trying their best to alleviate the suffering of their infected customers by augmenting security measures on websites and browsers. By utilizing such techniques as segregation of code from security programs, web designers arm themselves with the tools with which to prevent future attack. One vital tool that web designers must use is their codes of ethics. Without these codes of ethics (based on the collective human morality), designers not only forgo safe coding practices, but they also put potentially millions of users at risk and deny a facet of their natures. Following correct coding procedures can reduce the risk of such attacks as SQL injection and cross site scripting. What are these correct practices, why does hacking occur, and how can it be prevented?

Hacking has been an issue since the creation of the microcomputer. Originally used as a term to describe someone who is adept in all that is computing, hacking took on a negative connotation in the early 1970s. John Draper was the first person to be deemed a malicious hacker. Draper "hacked" phone lines by blowing a specific tone into the phone which forced the phone system to open a line(Rhodes, 2007). He used this method to make long distant phone calls for free. His actions spawned the first hackers, and they followed in his footsteps. His scheme lead to the creation of blue boxes, which are devices used to hack phone systems. It was not until the 1980s that modern hackers came into existence with groups like the 414s (Elmer-DeWitt, 1983) and Robert T. Morris, Jr releasing his worm virus (Eichin, M.W. and Rochlis, J.A, 1989). At this time, the Internet was in its budding stage, so cybersecurity was not a problem that concerned anyone. However, in 1983, a group of teenagers changed everyone's view of cybersecurity. This group called themselves the 414s, which is the area code of Milwaukee, Wisconsin. They hacked several organizations, taking files and records, which caused around $1,500 worth of damage per attack (Franklin, 1990). The FBI eventually caught up with them and forced them to stop their hacks, but no criminal charges were brought up against them. In the late 1980s, hackers started to become a more serious threat(McLellan, 1981). Hackers' attempts became bolder; they hacked everything from McDonald's restaurants to highly classified United States military systems. These attacks lead to the creation of government anti-hacker groups that were formed to suppress the new threat of cyberwar. While these attacks occurred decades ago, the importance of cybersecurity has not been alleviated. Everyone should be aware of the true threat of cybercrime, and they should take hope in the fact that precautions have been taken to prevent people from falling victim to hackers.

> "In 2014, the total number of websites on the internet reached 1 billion. Today, it's hovering somewhere in the neighborhood of 944 million due to websites going inactive, but it is expected to normalize again at 1 billion sometime in 2015. Web design is used as a general term to describe any of the various tasks involved in creating a web page. More specifically, it refers to jobs focused on building the front end of a web page."
>
> - (Perez, 2015)

When a web page is designed, there are several characteristics that each one must have. There is a special group of people who handle this task. This group is called web page designers or web page developers. What is a web page designer?

> "A web designer creates the look, layout, and features of a website. The job involves understanding both graphic design and computer programming. Once a website is created, a designer helps with maintenance and additions to the website. They work with development teams or managers for keeping the site up-to-date and prioritizing needs, among other tasks."
>
> - (Study.com, 2016)

Web page designers face many different obstacles when designing web pages, such as confirming the privacy and authenticity of a web page. Developers oversee everything that goes into implementing a web page. Such oversights include implementations of SSL (Secure Sockets Layering), web page content, script security, infrastructure, and tracking (Study.com). Web page designers oversee many aspects of web page design that end users do not know or understand. This can become a problem if web page designers misuse their privileges simply because they have the know-how. For example, designers can tamper with security settings such as privacy filters. Privacy is a hot button dilemma that web page designers face because they have direct access to personal files, and they also have the capability to perform website monitoring.

Web page designers also face the dilemma of ensuring the authenticity of their web pages. An authentic web page is one that is real, reliable, and/or trustworthy. As stated previously, web page designers are in control of all elements that go into designing a web page. As a result, web designers have the ability to threaten the authenticity of a web page. Developers can tamper with verification techniques and create loopholes so that they can see what end users are doing, which goes hand-in-hand with privacy. Developers can become rogue elements if they exploit the information they are supposed to keep safe (Wayner, 2014).

How can web page designers prevent their colleagues from becoming rogue elements? Like in any profession, web designers and system administrators are bound by codes of ethics. Yet despite these codes being in place, the number of hackers in the world is staggering. It seems that money, greed, and personal gain are much more important to some than the well-being of others and humanity at large. What many hackers do not realize is that these codes of ethics are frame-worked by collective human morality (ACM, 1992); ergo, when hackers attack, they are denying a facet of their human natures by harming others.

There are many directives of which programmers (including web designers and system administrators) must constantly be aware. There are three, however, that are overarching in their inclusivity and magnitude. They are:

1. A programmer must protect user data unless doing so brings physical harm to themselves or others,
2. A programmer must not create something/allow their creations to be used to harm society at large or the environment, and
3. A programmer must not allow their code/creation to be used to hurt individuals in any way.

As previously stated, there are many more directives, such as respecting other's work (IEEE, 2016) and the privacy of customers (ACM, 1992), but all other directives can be placed under the umbrella of these three prime directives. It would seem that the charge of being a computer programmer, web designer, or system administrator is great. One must protect the online lives of hundreds, if not millions, of people from attack. One can regard our web designers and system administrators as our online "superheroes", protecting the online lives of people from "villains", or cybercriminals.

Even if programmers follow their respective code(s) of ethics to the letter, malpractice can still occur. One example of this comes from a study conducted by Chris Barry and his associates (Barry et al., 2011). In their study, Barry and his colleagues tested the usability of airline websites. They found that while using the website to book a flight was relatively simple (a revenue-earning task), using the website to perform other tasks, such as filing a complaint or finding contact information, was not as user-friendly. It can be speculated, and Barry and his associates believe it to be true, that company executives do not want to waste time and money on coding for non-revenue-earning online tasks, so they ask their web designers to cut corners and focus solely on revenue-earning tasks (Barry et al., 2011). Another example in a case study provided by the Center for Ethics in the Professions tells of a system administration designer who is being pressured by his boss to push out software to a company's computers, even though doing so would violate the licensing agreement with said company (Frey, 2000). Said designer is torn between performing the actions his boss is asking of him and following his code of ethics with the risk of termination. Such scenarios place web designers, computer programmers, and system administrators in unfairly compromising situations that are complicated further by pressure from superiors.

By being rushed by their bosses, certain guidelines can go unchecked. Unintended bugs may make it into production; as a result, vulnerabilities may be introduced into a program. One of the most common ways of introducing vulnerabilities into code is unknowingly allowing Server Query Language, SQL, injection into a website. According to C. Severance, SQL has been the standard for interacting with database applications since the 1980s (Severance, 2014). Because of how these queries are constructed in the backend of an application, improper handling of user data can allow users to insert their own SQL queries into an application. This can bring about several unintended yet serious side effects. Some of these side effects can range from the exposition of users' private data to corruption of an entire application by the deletion of its database (Jang & Choi, 2014). Allowing vulnerabilities such as these can be detrimental to businesses and user trust. Thankfully, by following certain protocols, these vulnerabilities can be minimized.

One potential way to prevent SQL injection is through a combination of both validation and sanitization of user input (Jang & Choi, 2014). Validation is usually accomplished on the client side through JavaScript and on the server side by a backend scripting language. According to the Microsoft Developer Network, a developer must not rely on client-side validation alone (MSDN, 2003). The two primary reasons for this are that 1) not every user will access web pages through the UI (User Interface), and 2) JavaScript can be disabled in the browser, allowing for any client-side validation to be bypassed. In order to avoid issues of this nature, user input must always be validated on the server side as well. Beyond validation, one must also sanitize the user's input by using escape functions that will prevent special code characters from being executed as code (Jang & Choi, 2014).

When designing a website, web designers must also keep their website safe from the malicious content that others wish to insert into them. Malicious content is any website, document, or program that infects a computer with a virus or tries to solicit any private or personal information (Emory, 2016). The forms of online malicious content can range from a relatively harmless pop-up ad or email to a website posing as a legitimate source attempting to phish data. Most of these attempts to phish for personal information from a user usually rely on users' technological illiteracy or their unbased overconfidence in an absent technological competency (Emory, 2016).

Once web designers have implemented a good security system on a website, they must insure that the website's security is maintained. This is where updating plays an important role. According to Webster's Online Dictionary, to update means to "change something to include the most recent information; or, in the case of web security, to include both the most recent information about malicious software and the capability to defend against them." (Update Definition, n.d.). Keir Desailly, a Firewall Analyst at the security company Sucuri, says that as soon as a new version of the security software one uses becomes available, it is incredibly important to update it immediately (Desailly, 2015). “Most hacking these days is entirely automated, with bots constantly scanning every site they can looking for exploitation opportunities. It is not good enough to update once a month or even once a week because bots are very likely to find a vulnerability before you patch it.” (Desailly, 2015). Website owners want their customers to have confidence in the company’s ability to keep their personal information safe, so the software these companies utilize needs to be capable of defending their customers’ data against any type of virus, malware, and/or malicious hacking. For example, due to a recent, large-scale account breach, Yahoo is going to have a tremendously hard time recovering the loss of trust in their user base(Fiegerman, 2016). Additionally, they are going to have a hard time convincing new users to sign up for their services, even though they have fixed the issues in their system. If they had found the vulnerabilities before they were an issue, this loss of trust could have been avoided. Web designers must work hard to stay informed about the most recent viruses, hacking techniques, and malicious software; in this manner, they will be able to improve their web security software using the vital tools that defend against all of these security issues.

Discussion:

In terms of ethics, web designers, computer programmers, and system administrators are bound by a heavy charge: protecting the online lives of hundreds if not millions of people.

Those termed “hackers” not only violate their codes of ethics, but also deny a core facet of their humanity by harming others. Even when web designers and other programmers follow their codes of ethics to the letter, powerful outside pressures can leave them with no alternative but to cut corners, violate agreements, and even break the law. In order to avoid these breaches of ethics, supervisors must not be greedy and ask their inferiors to cut corners or pursue money-saving tactics if said tactics would violate ethics, agreements, or laws. Likewise, web designers and programmers must not allow superiors’ malicious actions to go unreported. Such techniques as the separation (modulation) of code and security code allow better response to such attacks as SQL injection (Hermosillo et al., 2007), and avoiding corner-cutting techniques will prevent mistrust and loss of profits for businesses in the future (Barry et al., 2011).

When it comes to providing a service to users over the internet, it is of the utmost importance that the developers of web applications do everything in their being to provide a secure platform for their users. This can be accomplished by requiring security to be an important part of the development process and not an afterthought. Keeping up with industry standards and learning about the most recent vulnerabilities and attacks is a very important technique and indeed requirement of the development cycle. Users trust internet businesses with an incredible amount of their private information; this trust is paramount to the success of these business and their ability to attract more customers.

Security is something that must be thought of at all times during development. Every day, new technologies, new versions, and new frameworks are being made. With each of these new advancements comes new vulnerabilities. For example, a developer may choose to use some new technology that has not been in circulation for long, and they are able to take advantage of the latest and greatest technology. They have even found an easier way of performing tasks or increasing the performance of their machines or systems. Then, a couple months down the road, a vulnerability is announced. The developers quickly fix the issue, but the damage has already been done. A system was hacked, information was stolen, or an entire hub was shut down. Developers need to be aware that not only are they responsible for the code that they write in an application, but they are also responsible for using safe and secure technology over the latest and greatest technology. They are also responsible for using safe and secure practices over those which maximize one function over another.

All manner of software exists today, some of which has really good security designs. No matter how secure software may be at the onset, however, its level of security will eventually become outdated as those with malicious intent develop new means of bypassing its security measures. Therefore, software must be updated to handle the latest threats. Microsoft is known for updating their software regularly, which is one of the reasons they have such a strong customer base. Microsoft often pushes notifications that new updates are available on user's desktops. While it can sometimes feel annoying to have to go through the process of downloading updates, installing updates, and restarting one's computer, one must realize the privilege of rarely experiencing security problems on his or her personal machine. When a client is able to trust that a company is doing all it can to keep one safe from security problems, then it means the client does not have to spend hours upon hours trying to solve these problems on his or her own. When a customer is considering using a security service, one question the customer may have is, "How do I know whether or not I can trust this developer's software to protect my data? Do I try it out and hope for the best? Is there some kind of assurance that this developer provides concerning the trustworthiness of his or her software?" One way developers can alleviate this concern is by insuring the potential user that the software is updated regularly to handle all types of malicious content. Even though users are likely aware that dangers to their online security exists, they are often uninformed about the specific types of attacks that could infect their systems, so there exists a fear of a threat that they do not fully understand. Developers can help to put potential users of their software at ease by explaining what some of the different types of malicious software does and how their security software can defend against them. Developers can also explain that they are updating their software to counter any new techniques that hackers devise. Designing and implementing good security software is the first step; however, maintaining that security continues until the use of that software is discontinued.

Conclusion:

Since computers and the Internet became things/places of commerce, thieves evolved with them. However, when hackers hack a system, they are foregoing their ethical codes and possibly denying a facet of their human natures. In order to prevent the rise of hackers, every web designer must follow their respective codes of ethics. If any codes of ethics are violated, web designers put themselves and others at risk for all sort of attacks. While in the current workplace environment there is a demand for a focus on profit earning functions and little else, it is still important to never let security be an oversight. If security were to be overlooked or put on the sidelines in development, companies run the risk of their systems and websites being exploited by diligent hackers looking to exploit a hole in the design. Malicious content can infect systems with viruses or steal personal information. As the rogue elements of the computing world gain traction, our Internet “superheroes” must be ever vigilant to ensure that people can browse the web safely.

Developers must make sure that they are adhering to the most up-to-date security protocols, thereby ensuring the quality and security of their applications. They have a duty to protect users’ data and ensure the authenticity of their websites. They have a duty to respect that trust and do the best they can to prevent users from having their information stolen through vulnerabilities. For a working demonstration of some common web vulnerabilities some sites are recommended, www.willcodes.com/validation/ and www.willcodes.com/sqlinjection/. The user can attempt to bypass the client side validation in the former by disabling JavaScript in the browser and try inputting *‘ OR ‘1’ = ‘1* for the username and password for the latter.

Acknowledgement:

We would like to acknowledge the School of Computing at the University of Southern Mississippi for allowing us to research and study this topic. We would like to thank our CSC309 class for allowing us to practice presenting and forming our group.

Literature Cited:

ACM Code Of Ethics and Professional Conduct. (1992, October 16). *Association For Computing Machinery.* Retrieved from http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct.

Barry, C., Hogan, M., & Torres, A. M. (2011). Low-Cost Carriers and High-Tech Barriers: User Views On Questionable Web Design Practices In Ireland. *Irish Journal of Management, 31,* 43-58.

Desailly, K. (2015, June 16). *10 Tips to Improve Your Website Security*. Retrieved 9 Oct., 2016, from https://blog.sucuri.net/2015/06/10-tips-to-improve-your-website-security.html.

Eichin, M.W. and Rochlis, J.A.: "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", *MIT*(1989)

Elmer-DeWitt, Philip (August 29, 1983). "The 414 Gang Strikes Again". Time. p. 75.

Fiegerman, S. "Yahoo Says 500 Million Accounts Stolen." *CNN Money,* 23 Sept., 2016. Retrieved 17 Oct., 2016, from http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/.

Frey, W. J. *The Case Of the Troubled Computer Programmer.* 2000. Retrieved from http://www.uprm.edu/etica/cpucases.html. PDF file.

Hermosillo, G., Gomez, R., Seinturier, L., & Duchien, L. (2007). Using Aspect Programming To Secure Web Applications. *Journal of Software, 2,* 53-63.

IEEE Code Of Ethics. (2016, June). *Institute of Electrical and Electronics Engineers.* Retrieved from http://www.ieee.org/about/corporate/governance/p7-8.html.

Jang, Y., & Choi, J. (July 2014). Detecting SQL Injection Attacks Using Query Result Size. *Computers & Security, 44*, 104-118, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2014.04.007.

"Malicious Content Filtering." *Emory LITS: Information Technology*. N.p., n.d. Web. 17 Oct., 2016.

McLellan, Vin (1981-07-26). "Case of the Purloined Password". The New York Times. Retrieved 11 August 2015

Microsoft Developer Network, "Design Guidelines For Secure Web Applications" *Improving Web Application Security,* chapter 4, June 2003. Retrieved 17 Oct., 2016 from https://msdn.microsoft.com/en-us/library/ff648647.aspx.

Perez, T. (2016). *Website Security: How Do Websites Get Hacked?* Retrieved 17 Oct., 2016, from https://blog.sucuri.net/2015/05/website-security-how-do-websites-get-hacked.html.

Rhoads, Chris (January 13, 2007). "The Twilight Years of Cap'n Crunch". *The Wall Street Journal*. Retrieved April 16, 2010.

Severance, C. "Elizabeth Fong: Creating the SQL Database Standards." *Computer*, *47,* 7-8, Aug. 2014. doi: 10.1109/MC.2014.209.

Symantec. (2012). [Graphic data on cybercrime]. *Norton Cybercrime Report.* Retrieved from http://us.norton.com/cybercrimereport/.

Update Definition. (n.d.). Retrieved 17 Oct., 2016, from Merriam-Webster Dictionary. http://www.merriam-webster.com/dictionary/update.

Wayner, P. (2014). "*12 Ethical Dilemmas Gnawing At Developers Today."* Retrieved 17 Oct., 2016, from http://www.infoworld.com/article/2607452/application-development/12-ethical-dilemmas-gnawing-at-developers-today.html.

Web Designer: Job Description, Duties and Requirements. (n.d.). Retrieved 17 Oct., 2016, from http://study.com/articles/Web_Designer_Job_Description_Duties_and_Requirements