**Tyler Carrier**

**Web Applications**

**Web Security Fundamentals**

**9/22/18**

**Box #88**

Web security can be defined as “a branch of information security that deals specifically with security of websites, web applications and web services” (Wikipedia). Nowadays, web security is more important than it has ever been. Security breachings happen on a daily basis in small and large corporations. “Security breaches don’t just happen to banks and large corporations,” Kristina says. “I’ve heard so many developers say that they don’t need to worry about security issues because they’re not a target, but the truth is that you never really know if you are” (Shea). In the article, “Web Security Fundamentals: What Every Developer Should Know,” by Samantha Shea, the writer relays the importance of web security as well as lays down a foundation for web security and developers.

According to the article, a study was done in 2017 by IBM on data being affected in breaches. The odds of an organization having a breach is one in every four. This pertains to companies of any size or type. These breaches target user information such as credit card numbers, phone numbers, and passwords. Samantha Shea continues to stress the important of proper web security throughout the article so administrators can keep their applications secure and allow their customers to feel their information is safe.

Shea goes on to discusses XSS or cross site scripting. Cross site scripting “occurs when code is injected client-side into legitimate websites that would otherwise be trusted” (Shea). When this occurs the hacker is able to inflict harmful code to the user. This can lead to many harmful occurrences for the user such as install-scripts, viruses, and other malicious content. Some common cross site scripting vulnerabilities are file uploads, reflected XSS, and stored XSS. The way to ensure security when it comes to XSS is to put strict validation on user-input based on what the input should usually contain (Shea).

Another risk to be aware of in terms of web security is SQL injection. “SQL injection is a technique that uses code injection to attack database type applications. Malicious SQL queries are inserted via input from the client to the application” (Shea). When an attacker successfully compromises the system, he is able to accomplish a handful of tasks. The attacker is able to void certain transactions made by a user, instantiate spoofing identities, disclose user-data, harm existing data, and destroying data (Shea). One way to prevent this is to use variable binding. When doing this, the database can tell the difference between code and data. Another way to prevent this is whitelisting. “Whitelisting is also a good defence, as it specifies what the input should look like and does not allow input that doesn’t match the specified pattern” (Shea).

These are just a few examples of the many threats that are relevant on the web these days. Although security threats are extremely relevant, through certain methods of web security, the administrator can protect their users’ information and provide a safe experience for them overall. Through following some of the steps laid out by Shea and other techniques provided on the internet, the administrator can do a lot to protect their users’ from malicious attacks.

**Work Cited:**

Shea, Samantha. “Web Security Fundamentals: What Every Developer Should Know –

Shopify.” Shopify, 29 May 2018,

[www.shopify.com/partners/blog/web-security-2018](http://www.shopify.com/partners/blog/web-security-2018).

“Web Application Security.” Wikipedia, Wikimedia Foundation, 12 Sept. 2018,

en.wikipedia.org/wiki/Web\_application\_security.