Web Applications Security

Kingsley Nwosu, Syldon Harding, Raygelo Melfor, Markel Floyd

Saint Leo University

COM 450 – Network Defense and Security

Abstract

Ever since the dot-com boom, the importance of web applications cannot be overstated in regards to the world of today. Businesses and individuals alike rely on web applications to satisfy business and personal needs, but this has come with some unfortunate consequences. Since web applications often handle sensitive information, there must be a way to keep all this important data away from people who want to do harm. The aim of this paper is give the reader an introduction to the security measures of common web applications. We will start with a brief discussion about what web applications are and how they are typically used in today's world. Then we will get into the specifics of how applications like browsers, online retailers, social media applications, and online productivity tools are secured. We will then conclude with the ramifications of all these security measures and what the future may look like.

Web Applications Security

Web applications play a very important role in the world of today. By definition, a web app is an application program that is stored on a remote server and delivered over the Internet through a browser interface (Rouse, 2011). So things such as browsers, online retailers, search engines, and social media can all be considered web applications. But this reliance on web applications can come with its disadvantages, one of which being cybercrime. In fact, cybercrime damage costs are set to hit $6 trillion annually by 2021 (Morgan, 2018). It is obvious that in order to combat this threat, cyber security tools will need to be top notch. In this paper, we will discuss how some of the most used web applications are secured.

Browser Security

Web browsers are in essence the main door way into the Internet. Per Wikipedia, a web browser is, “a software application for retrieving, presenting and traversing information resources on the World Wide Web” (Wikipedia, 2018). The level of importance that web browser have makes the security measures it needs all the more imperative. In this section, we will discuss how the major web browsers in use today are secured.

The main protocol that transfers data between a browser and a website is the Hyper Text Transfer Protocol (HTTP). It first came to use in 1997, and different versions have been made through the years. The HTTP version that is in use in most browser today is Hyper Text Transfer Protocol Secure. HTTPS uses one of two secure protocols to encrypt communications, Secure Sockets Layer or Transport Layer Security. Both of

these protocols use an asymmetric public key infrastructure, which uses a public key and a private key to encrypt communications. If a website is using an HTTPS protocol, the browser will let the user know by showing a green “trusted” text next to the URL.

Built-in protocols are not the only way that a browser can be secured, there are a lot of things that users themselves can do to mitigate the chances of having a security breach. Installing plugins such as an ad blocker is a widely regarded as the most efficient and easy method of securing ones browser. Ad blockers can be downloaded from a browser’s store or a third-party site and get installed as a plug-in. Ad blockers work by preventing intrusive ads and pop ups from showing up on websites. Some examples of ad blockers that can be installed from a browser’s store is “AdBlock” and “Ublock Origin”. Most ad blocks have a whitelist of acceptable ads that a user may want to see, this can be useful if a user wants to support a trusted website by having the advertisements show up.

Online Productivity Software Security

Early 2017 google users experienced some phishing scheme by cyber-attackers. The phishing scheme worked by sending out massages to users indicating that someone in there contact list shared a document with them. This messages also include a link for to the user to click on, which will ask the user to log in into their google account in order to get authorized for a google docs; which is the malicious file send by cyber-attackers. Once the user sign in to google docs, the attackers gain access to the user’s email and contact list. Likewise google, Microsoft has their security measures tight up and under control for their Microsoft 365 software. Microsoft has a complete guide on how to better secure the Microsoft 365 app. The office 365 security and compliance

center can be used to manage compliance across office 365, Exchange online, and Sharepoint online. The compliance center gives administrator the opportunity to manage archive mailboxes, eDiscovery cases, auditing reports and retention and deletion policies. The compliance center also gives administrator the ability to assign permissions to others in order to access compliance features in the security and compliance Center. Office 365, also have a built-in anti-spam and anti-malware protection to help with better protection. Organizations can get the spam filtered customized to resemble the organization specific needs. Besides this security measures office 365 has other security measures that will come in handy for organizational use. These security measure includes the following features; Data loss prevention, eDicovery, Encryption, Inactive mailboxes, Information Right Management, Mobile Device Management, andTransport Rules.

Data loss prevention (DLP) helps the user protect sensitive information and prevent its inadvertent disclosure. With a data loss prevention (DLP) policy, administrator can identify, monitor, and automatically protect sensitive information across Office 365. Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. One can use eDiscovery in Office 365 to search for content in Exchange Online mailboxes, SharePoint Online sites, or both. Using eDiscovery, you can identify, hold, and export content found in Exchange mailboxes and SharePoint sites. This can is not necessarily a security measure, but it can be helpful for organization if they get breached or needs evidence in order to move forward in a legal dispute. Encryption is exactly what it means it gives user the ability to encrypt their messages. Inactive mailboxes is used to

preserve a former employee's email after he or she leaves your organization. A mailbox becomes inactive when a Litigation Hold or an In-Place Hold is placed on the mailbox before the corresponding Office 365 user account is deleted. The contents of an inactive mailbox are preserved for the duration of the hold that was placed on the mailbox before it was made inactive. Administrators, compliance officers, or records managers can use eDiscovery in Office 365 to access and search the contents of an inactive mailbox. This feature goes hand to hand with eDiscovery due to the fact that it is not a security measure, but it will be very helpful in case an employee get fired by violating any policy and the organization needs to go back and review anything in their mailbox. Information Right Management (IRM) helps prevent sensitive information from being printed, forwarded, saved, edited, or copied by unauthorized people. Mobile Device Management can be use Office 365 to secure and manage any device that uses Exchange ActiveSync to sync with your organization's email, calendar, contacts, and tasks. Not only this but administrator can also perform common mobile device management tasks like setting device access rules, viewing device reports, and remotely wiping devices that are lost or stolen. Lastly, Transport Rule by using this administrator can look for specific conditions in messages that pass through the organization and take action on them. Transport rules let administrators apply business policies to email messages and they can help them secure messages, protect messaging systems, and prevent information loss. Administrators can use the Exchange Admin Center or Windows PowerShell to manage transport rules.

Online Retailer Security

Cyber security is one of the most crucial features of electronic commerce. Without proper protocols in place, online retailers put themselves and their customers at risk for payment fraud. Smaller stores face even greater ecommerce security risks due to insufficient internet safety from cybercriminals. Records show one in five small business retailers fall victim to credit card fraud every year, with 60 of those stores being forced to close within six months. Not only is hacking a huge risk for all online merchants, but accepting a fraudulent payment also comes at the cost of having to refund the charges. Outside of financial consequences, data breaches damage a brand’s reputation and can cause once loyal customers to avoid putting their information at risk again. However, using the right tools will minimize the threat of fraud and instill trust within your customer base.

A basic website security feature is that the online store must operate on a secure server. From a visitor's point of view, this means the site URL starts with the "https" designation rather than "http." The security plan must specify secure server hosting and whether you need a third-party security certificate. Such a certificate means a security specialist has verified the security of the server. Credit card companies usually require such certification.

Once the site is secure, the next concern is separating real customers from threats. A common way to do this is to make customers set up an account and use their addresses to verify their identity. Some credit card systems include automatic address verification. If customers don't need accounts, they can use a test like a question or a captcha to block automated hacking programs.

A key part of a security plan details how a company processes payment. Once the secure server stores the credit card number, a payment system must process it, so the money goes into their account. Many credit card systems use encrypted transfer mechanisms to send the credit card number to the processor. The credit card system supplier has instructions on how to do this. Others have virtual terminals where merchants can enter the numbers that they get directly from the secure server.

The final part of the security plan describes the order confirmation. Customers usually get an email confirming their order. Such emails must only include non-sensitive information because emails are not secure. They specifically can't include credit card numbers. Companies should limit other order details as well, especially details regarding medical supplies or other personally sensitive information. The security plan must specify what the confirmation email includes and keep it to the minimum the customer needs to identify his order.

Conclusion

Making sure that the most used Web Apps are secured is essential in today's world. Browsers security is arguable the most important Web App to secure because it is the user's entrance into the internet. Online productivity apps have also increased in importance, so securing these applications is of increasing concern. Online retailers such as Amazon take their web securing very seriously, because of all the payment information that is tied to users. With all of these security measures, web applications can effectively fight common threats.

References

Rouse, M. (2011, July). What is Web application (Web app)? - Definition from WhatIs.com. Retrieved March 12, 2018, from http://searchsoftwarequality.techtarget.com/definition/Web-application-Web-app

Morgan, S. (2018, January 23). Top 5 cybersecurity facts, figures and statistics for 2018. Retrieved March 27, 2018, from https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

Web browser. (2018, March 03). Retrieved March 13, 2018, from https://en.wikipedia.org/wiki/Web_browser

Difference between HTTP and HTTPS. (2017, May 15). Retrieved March 27, 2018, from https://www.instantssl.com/ssl-certificate-products/https.html

Technet.microsoft.com. (2018). Office 365 security and compliance. [online] Available at: https://technet.microsoft.com/en-us/library/dn532171.aspx [Accessed 27 Mar. 2018].

Heisler, Y. (2017, July 18). Google rolls out new security measures to prevent reprise of Google Docs phishing scam. Retrieved March 27, 2018, from http://bgr.com/2017/07/18/google-docs-phishing-scam-security-update/

How to Create a Security Plan for Your Store Online. (n.d.). Retrieved March 27, 2018, from http://smallbusiness.chron.com/create-security-plan-store-online-41634.html

Why Is Ecommerce Security So Important? (n.d.). Retrieved March 27, 2018, from http://www.bigcommerce.com/ecommerce-answers/why-online-security-so-important/