www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Common Attacks and Trends in Web Application

Emad Shafie[1]
[1]Computer and Applied science Department, Makkah Community College, Umm Alqura University.
[1]eashafie@uqu.edu.sa

Abstract
This aim of this paper is to review the available literature on the recent trends in web application vulnerabilities. Google Scholar was used as the main search database for the review. Studies from the last few decades to analyse the trends in web application vulnerabilities over the years, especially since they are a relatively recent phenomenon. Using a set of criteria, approximately 400 scholarly works were initially selected and then reduced to a smaller number which was then explored in detail. It was found that there are a variety of forms in which attacks on web applications may take place. These attacks are becoming increasingly sophisticated with advancements in technology. Additionally, novel ways of attacking users have been developed in order to do so without tricking the user. Given the influx of technology and web applications in every aspect of life, this makes the user especially vulnerable. This means that web application developers must treat security as a priority rather than solely focus on usability.

Key-words: Web Applications, Web Application Vulnerabilities, Web Security, Recent Trends, Security, and Usability.

1. Introduction

The utilisation of web applications has become very common with the advent of the internet. Simply understood, a web application may be described as a 'computer programme that allow(s) visitors to submit and retrieve data to/from (a) database over (the) internet using (a) preferred web browser' (Kaur & Kaur, 2015:65). Srinath (2017) explains that a 'web application is a dynamic software programme that provide(s) (a) communication medium between (the) user and service provider' (Srinath, 2017:1180). This means that web applications may be used for a wide variety of purposes. These range from social media, education, entertainment and news among many others (Correa, Hinsley, & De Zuniga, 2010; Whiting, & Williams, 2013). There is, therefore, increased

reliance on web applications for an individual's daily activities, making them vulnerable to any attack through web applications. The pervasive nature of web applications means that they have infiltrated every aspect of a person's web usage and experience (Petrescu, Krishen, & Bui, 2020; Yadao & Babu, 2020). Therefore, although the primary purpose of an application may be to communicate information between an individual and the service provider, the potential for security threats, risks and vulnerabilities are innumerable. However, it must be mentioned that web applications form one part of cybersecurity. Jang-Jaccard and Nepal (2014) explain that hardware, software and network comprise the three components that may be classified as being vulnerable. Various components may be vulnerable to an attack. One key component in IT infrastructure is software, and this includes web applications. This makes it vital to understand what may lead to vulnerabilities in web applications as well as the potential mechanisms to improve web security in order to predict and mitigate any attacks.

Web applications' structure, explains Srinath (2017), consists of three distinct layers. These layers are – first, the browser, which is viewed by the user; second, is the layer that 'generates dynamic web pages' along with the content viewed by the user, with 'tools like Python, CSS Active Server Pages' or ASP; and lastly, the layer which consists of the backend and is called 'server database' (Srinath, 2017:1180). There is a potential for vulnerabilities in each of these layers, which highlights the importance of security in web applications.

One of the main issues that arise in web application development is that the focus tends to be on usability and not as much on security (Green, & Smith, 2016; Gorski & Iacono, 2016). Hence, in order to address the concerns of web application vulnerabilities, security considerations must be taken into account in tandem with usability. While there are several measures to protect and counter web applications, the attacks are seen as becoming increasingly sophisticated to the extent that they no longer need even to track the user. Another concern highlighted by Jang-Jaccard and Nepal (2014) pertains to hackers changing platforms. They are no longer restricted to computers or laptops and even seek to attack applications on tablets and mobiles, making an even larger proportion of people vulnerable to attacks.

The following sections detail the methodology used for the review and the findings obtained. This is followed by a brief discussion and conclusion, and some comments about the scope for future research.

2. Methodology

In order to find the relevant research studies, specific terms were used in Google Scholar. These were - web application vulnerabilities, web application vulnerabilities + trends, web security and web security + trends. A total of 100 results were considered for every search term yielding a total of 400 shortlisted results. For these, an initial examination was conducted, using research studies that spanned several decades. However, since web application development is a relatively recent phenomenon with the advent of the internet, most of the studies used were those after the year 2000. An attempt was made to refer to even more recent studies so as to understand the changes in web application vulnerabilities fully. This is especially in light of the advancements made in technology that are available not only for sophisticated security measures but also to hackers to penetrate through them and take advantage of vulnerable users.

3. Results

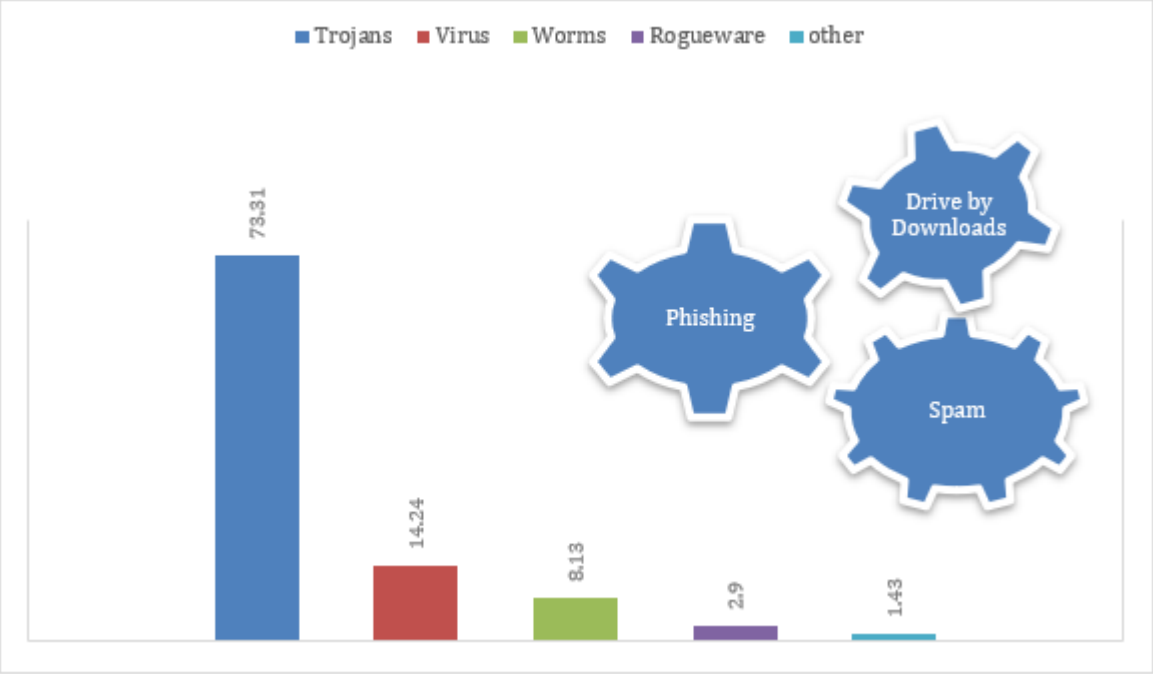
Web applications are used for a host of activities ranging from healthcare, entertainment, social media, online shopping and others. However, their widespread usage has also meant that they often also store sensitive data of the users. Examples of sensitive data include payment and banking information, personal details such as contact information as well as identity details. Such information, if accessed by hackers, may prove to be a potential risk not just to the web application developers but also to the users. Srinath (2017) observes that hackers tend to attack those web applications wherein there is information such as 'user login, online payments, (and) all the tasks (that) contain backend databases or Light Weight Data Access Protocols (LDAP) which stores … web users' sensitive data and operates as (a) basic communication medium between web user and infrastructure' (Srinath, 2017:1180).

Web browsers, state Jang-Jaccard and Nepal (2014), are the most common web application and a vital tool in accessing the internet for millions. Given their popularity, these are tools that can be used by a large number of people with relative ease. While this allows access to the internet, it also proves to be a key mode through which web application vulnerabilities may be exploited. This may be through a number of ways, such as through downloads, plug-ins, etc. Thus, the common characteristics of all such attacks and their patterns could be summarised as the continuance speedy and daily increment of active internet users and their life dependencies on internet services will directly proportional to increase in various types of attacks.

Along with these, Bendovschi (2015) adds DDoS or Distributed Denial of Service, which pertains to a compromised availability of data such that the user or server is flooded with commands, rendering it inoperable. Malware, states Bendovschi (2015), is an umbrella term that is used in order to describe a host of malicious software that can 'compromise the confidentiality, availability and integrity of data' (Bendovschi, 2015:3). Lastly, phishing is also commonly used in order to obtain users' personal information through false pretences. Together, these methods of exploiting users through web applications pose a significant threat to user experience, users' privacy as well as data confidentiality and the application itself.

Damshenas, Dehghantanha, and Mahmoud (2013) suggest that malware is the most common way to breach security and carry out an attack. Malware can take the form of a virus, Trojan, and spyware. Jang-Jaccard and Nepal (2014) agreed with these findings; according to them, the most common types of malware, along with the ways to spread them, are shown in Figure 1.

Figure 1 - Type of Malware and Medium to Spread them



Web application vulnerabilities may be understood as flaws in application design or the code that has the potential to create an entry point for hackers (Gates & Liska, 2018). Gate and Liska (2018) also suggest that this may take the form of bots, malware and DDoS attacks. With an increasing number of businesses moving online and a rising number of financial transactions taking place online, addressing security concerns has become imperative. Considerations of security also

include data confidentiality, privacy and data integrity (whether data can be trusted) (Gates & Liska, 2018). Some of the ways to address these concerns include setting up firewalls. Other examples include bot challenges such as CAPTCHA. Gates and Liska (2018) contend that while most businesses and organisations may be aware of the need for web security, most small and medium-sized enterprises may find it a daunting task. However, they suggest that web security should not be taken for granted, and such enterprises may even consider partnering with an Edge Services Partner. This is especially pertinent for 'cloud-based web application security' (Gates & Liska, 2018). Srinath (2017) states that with advancements in technology, attacks on web applications are becoming increasingly sophisticated, and so there is a need to invest in web security. Examples of highly sophisticated attacks that can be conducted without tricking the user include Wannacry, Emotet and Mirai Bot. Therefore, there is an increasing need to adopt mechanisms to monitor web traffic, establish defence responsive systems in the event of a security attack while also upgrading operating systems frequently.

The paper thus far has discussed the numerous web application vulnerabilities that pose a threat to web security. The next section will elaborate on the ways in which organisations have sought to mitigate these threats and address the vulnerabilities.

4. Discussion and Conclusion

In order to address the vulnerabilities in their web applications, organisations may implement certain security controls. These include preventative controls that aim to prevent a threat, detective controls that can detect any threat and corrective controls which seeks to correct irregularities identified (Bendovschi, 2015; Jain, 2020). In addition to this, organisations may choose to utilise a firewall or a Secure Socket Layer (SSL). Firewalls are ‘a set of related programs, located at a network gateway server that protects the resources of a private network from the users of other networks' (Khandelwal, Shah, Bhavsar & Gandhi, 2013:210). These include packet filters, application gateways, circuit-level gateways and proxy servers. The second technique that may be used to prevent web application attacks is an Intrusion Detection System or IDS. Such a system helps information systems by preparing them for attacks. This is done by collecting the relevant information regarding attacks and analysing it. An Intrusion Prevention System or IPS is similar to IDS. However, in addition to keeping a log of attacks, IPS can also react to them. A Web Application Firewall or WAF are designed to protect web applications (and) servers from web-based attacks that IPSs cannot prevent (Khandelwal, Shah, Bhavsar & Gandhi, 2013:211). WAFs are also considered as

the most effective tool to provide more security when compared with the alternative tools available, such as firewalls, IDS and IPS (Khandelwal, Shah, Bhavsar & Gandhi, 2013). Jang-Jaccard and Nepal (2014) summarise the most common attacks as well as some of the ways to counter them. These are not just restricted to web applications but cover the gamut of cybersecurity threats that may be potentially faced.

Table 1 - Common Attacks and Countermeasures

Attacks examples	Solution
• Network protocol attacks • Network monitoring	• Firewall • Encryption
• Software Programming bugs • Web pages errors • Misconfiguration error	• Secure coding practice • Secure design and development • Secure installation
• Hardware Trojan • Illegal clones	• Tamper-Resistant hardware (e.g TPM) • Trusted Computing Base

Another study by Atashzar, et al. (2011) found that over 75% of the total attacks take place on the web application itself. According to a 2017 report on web application vulnerabilities, it was found that the security of web applications still remains an afterthought. The report assessed 23 web applications, focusing on code and configuration vulnerabilities. It was found that of the applications tested, all of them could be successfully hacked, with the exception of a mere 4%. This further supports the argument that there is a pressing need to address security concerns in the early stages of web application development so as to integrate security features and prevent an attack.

With the advent of the Internet of Things (IoT) and increasing device to device communication, three have been concerns about confidentiality (Fonyi, 2020). Another key point to be discussed here is raised by Jang-Jaccard and Nepal (2014), who contend that there has been an increasing attempt to switch platforms for exploiting such vulnerabilities. This means that although attacks were usually carried out on computers or laptops, there has been a rise in phishing via text messages, for example. Hence, in this context, a risk assessment must be a continuous process. Given the nature of attacks that users are vulnerable to and the extent to which vulnerabilities can be exploited, there must be a mechanism to identify vulnerabilities continually. Jang-Jaccard and Nepal (2014) also point to a deeper issue of building trustworthy computing bases. They contend that over the years, systems have been built ‘using inadequate architectures, development practices, and tools’ (Jang-Jaccard & Nepal, 2014:989). These are not optimal for modern technology and, therefore, not

optimal for withstanding attacks. Hence, there is a need to improve the infrastructure of cyberspace rather than addressing each attack as it takes place.

The review has provided an overview of the numerous web application vulnerabilities that exist, how they may be exploited as well as the ways in which they may be addressed and mitigated. This would focus on security at the time of web application development. The role of writing secure code, training and increased awareness about ways to prevent such attacks are also vital. Secure web applications, state Kaur and Kaur (2016), can only take place when a 'Secure SDLC (Software Development Life Cycle) is followed' (Kaur & Kaur, 2016:299). However, this is a security measure that requires skill training and investment, the value of which must be recognised by application developers. Hackers increasingly have access to sophisticated technology and can easily use that to the detriment of organisations and individual users. At the same time, it must be reiterated, there are evolving methods of mitigating the attacks on web applications. Fundamentally, therefore, there needs to be continuous vigilance on the part of users, web application developers must prioritise security features and not just usability while also emphasising regular risk assessments.

Web applications are a part of every aspect of life - ranging from health, sports, entertainment, news, education, shopping and many others. This has meant that more and more functions and daily activities are performed with the use of the internet and web applications. These applications contain valuable and sensitive data which must be protected and kept safe. Hence, while this means that there are abundant opportunities for hackers to launch attacks, it also provides a wide field for further research in order to better understand how to build trustworthy systems as well as to protect the privacy of users.

References

Atashzar, H., Torkaman, A., Bahrololum, M., & Tadayon, M. (2011). A Survey on Web Application Vulnerabilities and Countermeasures. Conference Paper.

Bendovschi, Andreea. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*. 28. 24-31. 10.1016/S2212-5671(15)01077-1

Correa, T., Hinsley, A.W., & De Zuniga, H.G. (2010). Who interacts on the Web? The intersection of users' personality and social media use. *Computers in human behavior*, *26*(2), 247-253.

Damshenas, M., Dehghantanha, A., & Mahmoud, R. (2013). A survey on malware propagation, analysis, and detection. *International Journal of Cyber-Security and Digital Forensics*, 2(4), 10-30.

Gates, S., & Liska, A. (2018). Securing Web Applications. O'Reilly Media, Inc.

Fonyi, S. (2020). Overview of 5G Security and Vulnerabilities. *The Cyber Defense Review, 5*(1), 117-134. doi:10.2307/26902666

Gorski, P.L., & Iacono, L.L. (2016, July). Towards the Usability Evaluation of Security APIs. In *HAISA* (pp. 252-265).

Green, M., & Smith, M. (2016). Developers are not the enemy!: The need for usable security apis. *IEEE Security & Privacy*, *14*(5), 40-46.

Huang, Yao-Wen & Lee, D. (2005). Web Application Security—Past, Present, and Future. In Lee, D., Shieh, S., & Tygar, J. ed. Computer Security in the 21st Century. Boston (MA): Springer.

Jain, A. (2020). Cyber Crime. *National Journal of Cyber Security Law*, *2*(2).

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. doi: 10.1016/j.jcss.2014.02.005

Kaur, D., & Kaur, P. (2015). Ranking and Impact of Web Applications' Vulnerabilities. *International Journal of Scientific Engineering and Research (IJSER)*, Volume 3(Issue 6).

Kaur, D., & Kaur, P. (2016). Empirical Analysis of Web Attacks. *Procedia Computer Science*, 78, 298-306. doi: 10.1016/j.procs.2016.02.057

Khandelwal, S., Shah, P., Bhavsar, K., & Gandhi, S. (2013). Frontline Techniques to Prevent Web Application Vulnerability. *International Journal Of Advanced Research In Computer Science And Electronics Engineering (IJARCSEE)*, Volume 2(Issue 2).

Petrescu, M., Krishen, A., & Bui, M. (2020). The internet of everything: implications of marketing analytics from a consumer policy perspective. *Journal of Consumer Marketing*.

Positive Technologies. (2017). Web Application Vulnerabilities: Statistics for 2017. https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-2018/

Srinath, K. (2017). Recent Trends in Web Application Security Risks and Issues. *International Journal of Advance Research and Innovative Ideas in Education*, Vol-3 (Issue-6).

Whiting, A., & Williams, D. (2013). Why people use social media: a uses and gratifications approach. *Qualitative Market Research: An International Journal*.

Yadao, S., & Babu, A.V. (2020). Usage of Web Mining for Sales and Corporate Marketing. In *Communication Software and Networks* (pp. 55-60). Springer, Singapore.