Chapter 4
Securing Web Applications:
Security Threats and Countermeasures

B. M. Arifuzzaman
North South University, Bangladesh

S. M. Niaz Mahmud
North South University, Bangladesh

Ayman Muniat
North South University, Bangladesh

A. K. M. Bahalul Haque
https://orcid.org/0000-0002-7942-0096
LUT University, Finland

ABSTRACT

Web-based services are common targets for hackers, and the need for ensuring their security keeps on rising. Attackers often take advantage of the vulnerabilities of different web applications using several mechanisms and thus steal and manipulate valuable information. Therefore, the attack vectors are also increasing since there is a wide variety of internet users. Exploitations caused by different types of cyberattacks results in data loss, identity theft, financial loss, and various other adversaries on both humans and infrastructure. Therefore, investigating various attack vectors and countermeasures can facilitate and encourage future research and create awareness among web application users and developers.

DOI: 10.4018/978-1-7998-9426-1.ch004

INTRODUCTION

The internet has now become an inevitable part of our life and is revolutionizing the world as we have never seen before (Haque et al., 2021a). Along with the internet, web-based applications are also gaining popularity as they offer services such as online shopping, online banking, and online courses. Such applications contain a variety of sensitive information that must be protected (Haque, 2019; Saini, 2019). Otherwise a hacker may exploit the confidential data which is not only a breach of privacy, but can also lead to the impersonation of users.

Unfortunately, cyber-attacks have become increasingly common in recent times. 2016 recorded over 229,000 web attacks every single day (Anonymous, 2016). As per (Eian et al., 2020), there are three factors that work behind the web security attacks. They are - spectacularity, vulnerability and the fear factor. Specularity implies that an attacker wants to gain from the damage incurred in an application. An individual or an organization going through losses can be an example. Namely, if a DoS attack was initiated, large e-commerce organizations such as Amazon, eBay or Walmart will go through massive losses in their sales. The second factor, vulnerability, refers to the loopholes or lack of sufficient system security. Some applications either do not take enough safety measures or may use an outdated framework, making them an easy prey for attacks. Finally, the fear factor insinuates that the attacker wants to terrorize the user. An example of such an attack could be ransomware attacks. Targeting the root factors may help in improving cyber security.

For securing web applications, we have to ensure the security of three major components - data integrity, data confidentiality and web application availability (Al-Khurafi et al., 2015).

There are many existing solutions that can be applied to each attack or more than one type of attack that comprise the aforementioned components. For example, for injection based attacks, mostly in SQLs, the counters include the 'trust no one' approach, avoiding dynamic SQL, reducing attack surface etc. For Cross Site Scripting (XSS) attacks, utilising Content Security Policy (CSP) and modern JavaScript frameworks are useful. In order to mitigate DoS/DDoS attacks, the attacks need to be detected as early as possible. Sahoo (2020), Haider (2020) have both been recently developed for detecting DDoS breaches. In case of ransomware attacks, Davies et al., (2020) illustrate the existing solutions. Other web attacks such as Format String Attack, Buffer Overflow etc. mandate well documented codes. Deep Learning has also been a recent trend for treating security attacks (Sharma et al., 2019).

However, the existing measures do not fully address all the security gaps. The paper aims to provide an overview of Web Application Security in order to bring the security issues to light and create a knowledge base for further research on securing web applications. It briefly discusses similar literature and goes in depth into the