

# Chapter 2

## Attacks on Web Applications

**Ayushi Malik**

*University of Petroleum and Energy Studies, India*

**Shagun Gehlot**

*University of Petroleum and Energy Studies, India*

**Ambika Aggarwal**

*University of Petroleum and Energy Studies, India*

### ABSTRACT

*Online applications hold sensitive data that is valuable, and hackers strive to identify weaknesses and exploit them in order to steal data, pose as users, or disrupt the application. Web applications are increasingly exposed to dangers and attack vectors that are more advanced. Additionally, theft of private information—such as user credentials or billing information for credit cards—occurs frequently. Attackers initially concentrated on obtaining personal information that was accidentally exposed through poorly built or poorly protected web apps. Insecure design, security misconfiguration, vulnerable and outdated components, identification and authentication failures, etc. are some of the most prominent web application vulnerabilities that will be covered in this chapter. The authors are using countermeasures including fuzz testing, source code review, and encoding approaches to get around these vulnerabilities. As a result, this chapter offers information on the various attacks that website visitors who use web applications encounter.*

### 1. INTRODUCTION

The evolution of Internet and Web technologies, combined with rapidly increasing Internet connectivity, defines the new business landscape. A key element of internet

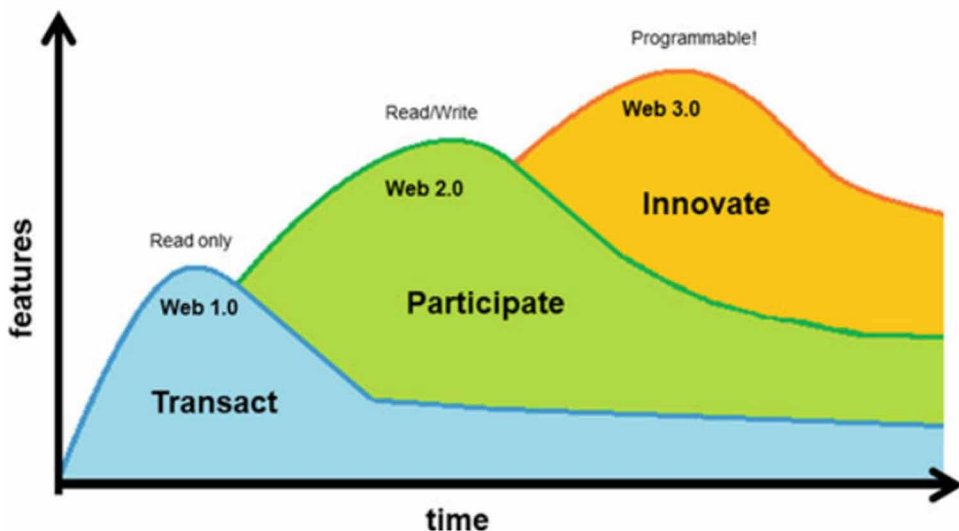
DOI: 10.4018/978-1-6684-8218-6.ch002

commerce is web apps. Everyone connected to the Internet utilises a plethora of web apps for a wide range of activities, such as social networking, online shopping, email, and chats. Web applications are now becoming exposed to more complex threats and attack methods. Hackers may misuse private information, which not only violates users' privacy but also opens the door to user impersonation. This module will familiarize you with various web applications, web attack vectors, and how to protect an organization's information resources from them. It describes the general web application [1] hacking methodology that most attackers use to exploit a target system. Ethical hackers can use this methodology to assess their organization's security against web application attacks. Thus, this module also presents several tools that are helpful at different stages of web application security assessment. This chapter includes several web application security tools to prevent the web from attacks that are familiar nowadays and also provides a brief knowledge about the attack and their countermeasures.

## 1.1 Evolution of the Web

The World Wide Web is a network of free websites that can be viewed online. It is sometimes referred to as the Web, the WWW, or just the Web. The Web is not the same as the Internet; it is one of several applications developed on top of the Internet. The evolution of the Web may be understood by dividing it into three waves: (1) read-only, (2) read/write Web, and (3) programmable Web. These waves aren't always separated by time, but rather by the introduction of new functions; as a result, they might overlap and coexist at times.

*Figure 1. Phases of web evolution*



30 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/attacks-on-web-applications/330259](http://www.igi-global.com/chapter/attacks-on-web-applications/330259)

## Related Content

---

### Women to the Rescue in Cyber Space

Kristin Brittain and Marianne Robin Russo (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1177-1188).

[www.irma-international.org/chapter/women-to-the-rescue-in-cyber-space/228776](http://www.irma-international.org/chapter/women-to-the-rescue-in-cyber-space/228776)

### Ethical and Privacy Implications of the Use of Social Media During the Eyjafjallajökull Eruption Crisis

Hayley Watson and Rachel L. Finn (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 764-777).

[www.irma-international.org/chapter/ethical-and-privacy-implications-of-the-use-of-social-media-during-the-eyjafjallajokull-eruption-crisis/228754](http://www.irma-international.org/chapter/ethical-and-privacy-implications-of-the-use-of-social-media-during-the-eyjafjallajokull-eruption-crisis/228754)

### A Usability Evaluation of Facebook's Privacy Features Based on the Perspectives of Experts and Users

Márcio J. Mantau, Marcos H. Kimura, Isabela Gasparini, Carla D. M. Berkenbrock and Avanilde Kemczinski (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1270-1294).

[www.irma-international.org/chapter/a-usability-evaluation-of-facebooks-privacy-features-based-on-the-perspectives-of-experts-and-users/228783](http://www.irma-international.org/chapter/a-usability-evaluation-of-facebooks-privacy-features-based-on-the-perspectives-of-experts-and-users/228783)

### Defining Cyber Weapon in Context of Technology and Law

Prashant Mali (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 38-51).

[www.irma-international.org/chapter/defining-cyber-weapon-in-context-of-technology-and-law/228719](http://www.irma-international.org/chapter/defining-cyber-weapon-in-context-of-technology-and-law/228719)

### Philosophical Foundations for Establishing Scientific Humanism as Naturalism

(2022). *Philosophical Issues of Human Cyborgization and the Necessity of Prolegomena on Cyborg Ethics* (pp. 1-26).

[www.irma-international.org/chapter/philosophical-foundations-for-establishing-scientific-humanism-as-naturalism/291945](http://www.irma-international.org/chapter/philosophical-foundations-for-establishing-scientific-humanism-as-naturalism/291945)