Chapter 8
Taxonomy of Login Attacks in Web Applications and Their Security Techniques Using Behavioral Biometrics

Rizwan Ur Rahman
Maulana Azad National Institute of Technology, Bhopal, India

Deepak Singh Tomar
Maulana Azad National Institute of Technology, Bhopal, India

ABSTRACT

Research into web application security is still in its initial phase. In spite of enhancements in web application development, large numbers of security issues remain unresolved. Login attacks are the most malevolent threats to the web application. Authentication is the method of confirming the stated identity of a user. Conventional authentication systems suffer from a weakness that can compromise the defense of the system. An example of such vulnerabilities is login attack. An attacker may exploit a pre-saved password or an authentication credential to log into web applications. An added problem with current authentication systems is that the authentication process is done only at the start of a session. Once the user is authenticated in the web application, the user's identity is assumed to remain the same during the lifetime of the session. This chapter examines the level login attacks that could be a threat to websites. The chapter provides a review of vulnerabilities, threats of login attacks associated with websites, and effective measures to counter them.

INTRODUCTION AND OVERVIEW OF CYBER SECURITY

Cyber security is the security of web associated frameworks, including equipment, programming and information, from digital assaults. In a registering setting, security includes cyber security and physical security - both are utilized by ventures to ensure against unapproved access to server farms and other

DOI: 10.4018/978-1-7998-3149-5.ch008

electronic frameworks. Data security, which is intended to keep up the privacy, uprightness and accessibility of information, is a subset of cyber security (Solms & Niekerk, 2013). Suppliers of personal computer (PC) administrations (like managing an account, email, or online networking) have the obligation of keeping programmers out of individuals' frameworks. As a PC client, you can do your part by being watchful about who you converse with over the Internet, what data you share, and by picking and utilizing solid passwords. PC passwords are amongst the most imperative apparatuses used to ensure data on PC frameworks. Similarly, as you do not need anybody taking your secret word and picking up control of your Instagram account, banks need to avoid potential risk to shield offenders from taking cash. Since passwords are so imperative, it is a wrongdoing to take passwords and to deliberately get into other individuals' PCs.

You utilize PC passwords consistently, regardless of whether to get to your email account, person to person communication locales, or even to do web-based saving of money. One of the difficulties you may have when picking a secret word is making it simple for you to recollect, however hard for other individuals to figure out. It may not be a smart thought, for instance, to utilize your puppy's name, your road address, or any data that is by one way or another associated with your username. For example, if Sue Jones utilizes the login "SJones" to get to her email and lives at 314 Apple Pie Road, the secret word "pie314" probably won't be a decent decision. Do you see why? In spite of the fact that it may be simple for her to recall, it is short and contains her street address. A more grounded secret key may be "9J8LZcWAMzjJQUnD"...if she could recall it. That is surely any longer, it is anything but a word, and it doesn't have any recognizable data. Be that as it may, who can recall that? What's more, in the event that you record it and lose the bit of paper, that isn't generally more secure.

A solid secret key is one that you can recall effectively, yet that is really long. It is comprised of two or three words, numbers and accentuation, however doesn't have anything in it that somebody would figure out. There is a great deal of systems for making solid passwords. The precedent is from an online absolutely irregular secret word generator. It basically picked 16 characters indiscriminately.

- Another technique is to begin by thinking about a passphrase, which is an expression you like or a statement from a motion picture. At that point utilize the primary letter of every one of the words and put in a number or accentuation (Keith et al., 2009).
- Another normal methodology is to utilize two totally disconnected words and separate them by numbers or characters; is "deaf+anteater" simple to recollect? Is it still simple to recollect whether you sprinkle in a few numbers, as maybe the telephone number where you used to live; "deaf555+4715anteater" may be harder for somebody to figure?
- Or consider a hogwash word that doesn't mean anything, yet you can even now articulate it, as "USiFiPiZOG" is a case of a pronounceable irregular secret word. Contrast that with the one beginning with "9J8" in the passage. Is it simpler or harder to recollect? Memory traps that assist us recollect things are called mental aides.

What cyber security can anticipate? The utilization of cyber security can help counteract cyber-attacks, information ruptures and data fraud. At the point when an organization has a solid feeling of system security and a viable episode reaction plan, it is better ready to anticipate and moderate these assaults.

The main objective of this chapter is to study defence mechanism in cyber security needed in today's world, its importance and why it has become such a big topic for discussion. The chapter aims at understanding the potential risks and threats present along with it and why ensuring security of user is of

Related Content