DVWA Security – Niklas Burtscher

1. Brute Force

Brute-Force-Attacken sind eine Methode, um durch systematisches Ausprobieren aller möglichen Kombinationen das Passwort, den Schlüssel oder den Code einer gesicherten Informationseinheit zu erraten. Diese Technik basiert auf dem Prinzip des Durchprobierens jeder denkbaren Option, bis die richtige Lösung gefunden ist.

Der Ansatz ist relativ einfach: Ein Angreifer verwendet ein Programm, das automatisch eine Vielzahl von Kombinationen durchläuft, um Zugang zu einem gesicherten System zu erhalten. Dies kann Passwörter, PIN-Codes, kryptografische Schlüssel und andere Formen von Sicherheitsmechanismen umfassen.

Es gibt verschiedene Formen von Brute-Force-Attacken, unter anderem:

Einfache Brute-Force-Attacken: Hierbei werden alle möglichen Kombinationen ausprobiert, beginnend mit den einfachsten oder am häufigsten verwendeten. Dies ist effektiv gegen Systeme mit schwachen oder sehr kurzen Passwörtern.

Wörterbuchangriffe: Statt jede mögliche Kombination auszuprobieren, nutzt der Angreifer Listen mit häufig verwendeten Passwörtern oder Wörtern aus einem Wörterbuch. Diese Methode ist schneller, wenn Nutzer einfache oder gängige Passwörter verwenden.

Hybridangriffe: Eine Kombination aus Wörterbuchangriffen und Brute-Force-Methoden, bei denen zuerst gängige Passwörter und dann zufällige Kombinationen ausprobiert werden.

Die Effektivität einer Brute-Force-Attacke hängt von mehreren Faktoren ab, insbesondere von der Länge und Komplexität des Passworts sowie von der Geschwindigkeit, mit der der Angreifer Kombinationen ausprobieren kann. Moderne Sicherheitssysteme implementieren Maßnahmen wie Kontosperrungen nach mehreren fehlgeschlagenen Versuchen, Verzögerungen zwischen den Anmeldeversuchen und die Verwendung von CAPTCHAs, um Brute-Force-Attacken entgegenzuwirken.