THUNDER

TEAM MEMBERS

A.R.NAVEEN KUMAR

-

AADHISH

Brute Force Attack explanation

What is a Brute Force Attack?

A brute force attack is a method where an attacker tries many different passwords repeatedly until the correct one is found.

How Does a Brute Force Attack Work?

- The attacker targets a login page
- Tries passwords like 0001, 0002, 0003...
- Repeats the process continuously
- Gains access if no security protection exists

Why Are Small Websites at Risk

- Small startups often do not use advanced security tools
- No CAPTCHA
- Limited budget

- Small businesses are frequently attacked because they are easier targets.

What Happens When There Is No Protection?

- Unlimited login attempts
- No delay between attempts
- Bots eventually find the correct password
- Sensitive data becomes accessible

Thynk Unlimited

Bot Behavior vs Human Behavior

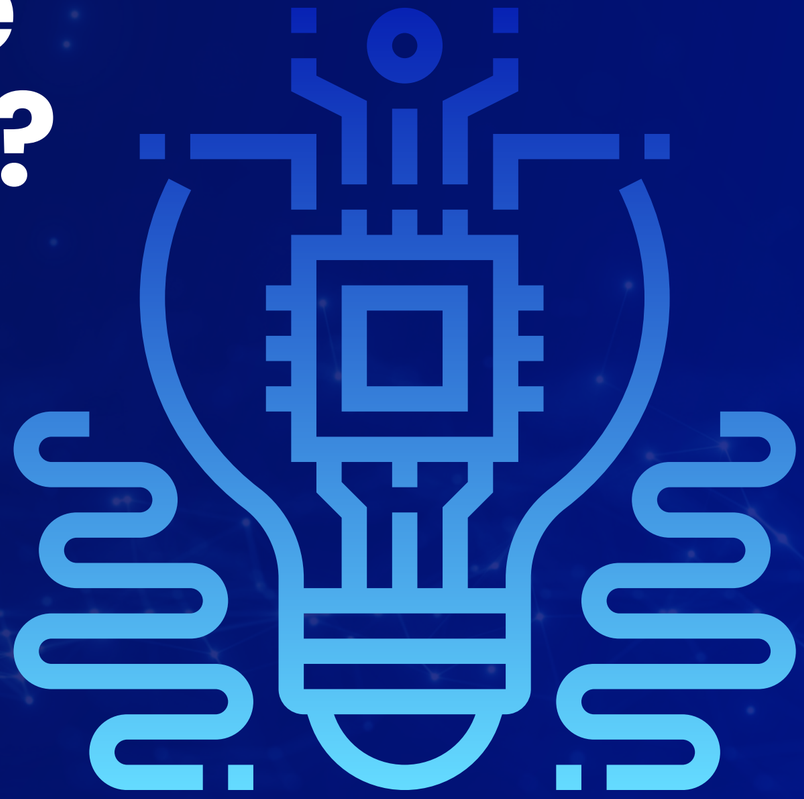
- Very fast
- No thinking time
- Repeated login attempts

- Take time to think
- Make fewer attempts
- Type manually

How Can Brute Force Attacks Be Detected?

- Time-based detection (very fast attempts indicate bots)
- Behavior monitoring
- Hidden fields (honeypots)

- Bots behave differently from humans, and these differences can be detected.



Our Motive

Our motive is to help small and early-stage startup companies understand the risks of brute force attacks.
Many small websites cannot afford expensive security tools like CAPTCHA or paid bot-protection systems.
This project demonstrates how brute force attacks work and how simple, behavior-based checks can help detect automated attacks at low cost.
Our goal is to create awareness and provide basic protection, not to replace enterprise-level security solutions.

Thank you