SECURE CODE

WARRIOR

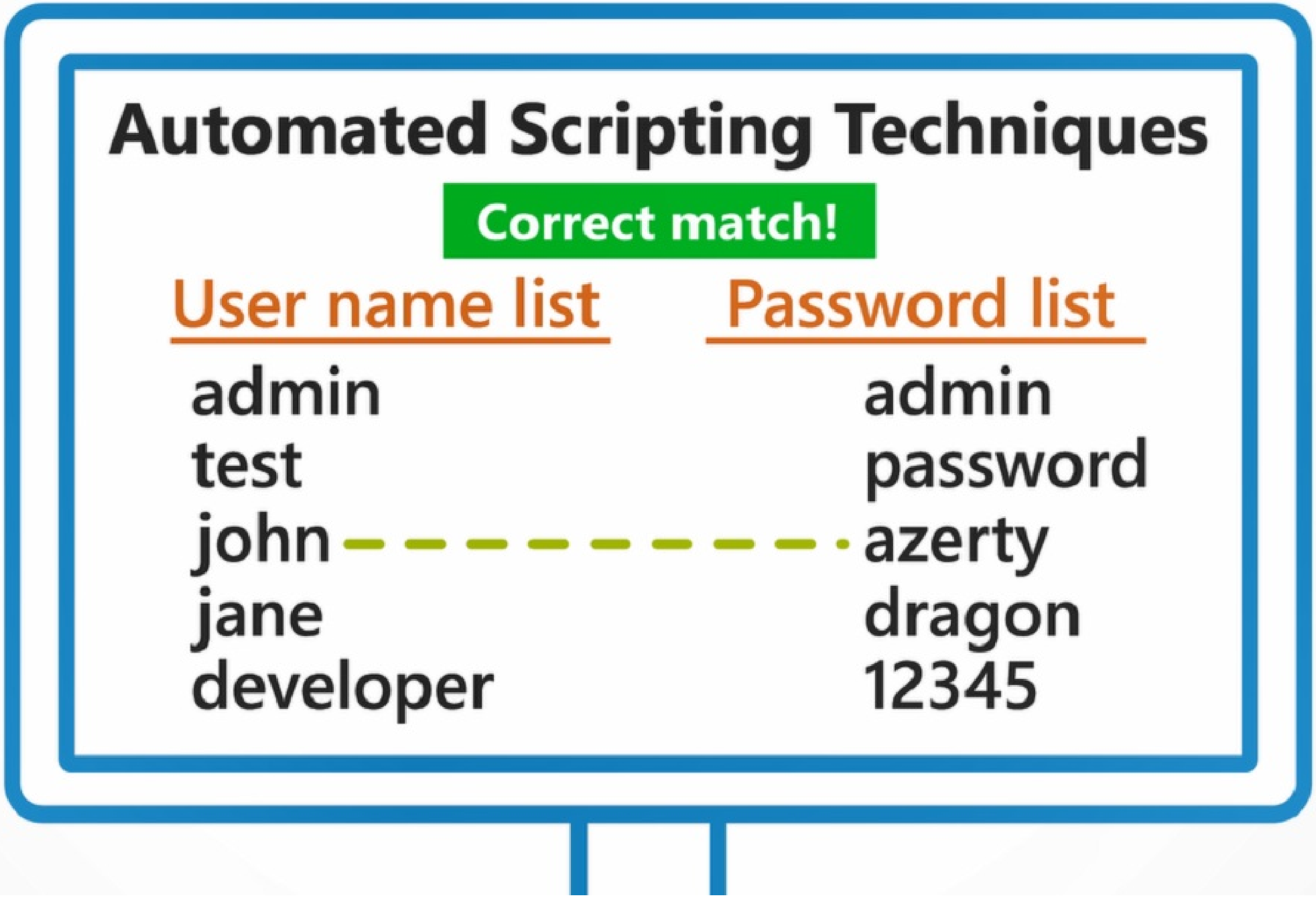
INSUFFICIENT ANTI-AUTOMATION

we will explain

what the vulnerability is, its causes and preventions and some potential hazards

WHAT IS INSUFFICIENT ANTI-AUTOMATION?

This vulnerability occurs when parts of the application, such as login forms, polls, or comment forms

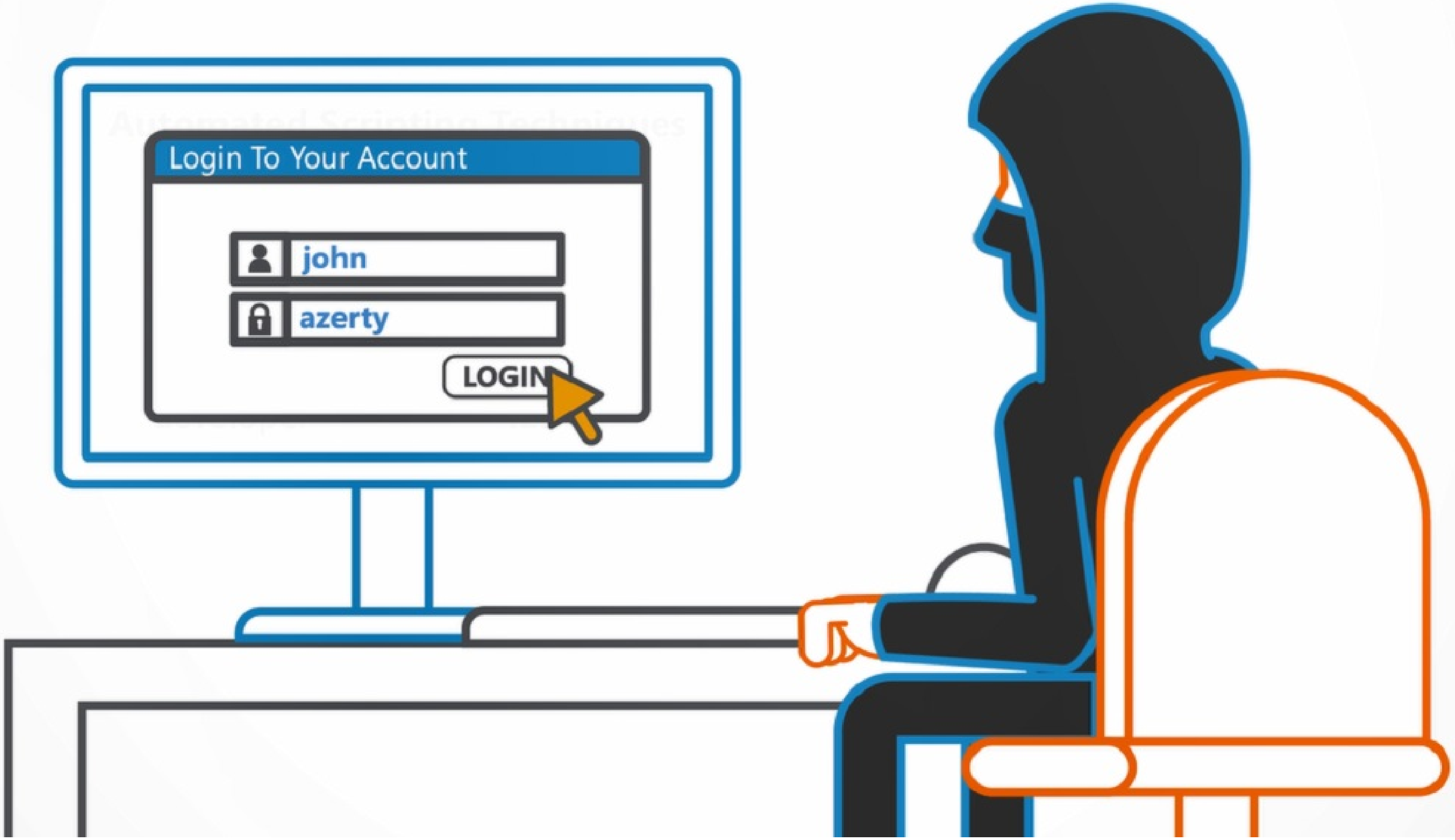


Automated Scripting Techniques

Correct match!

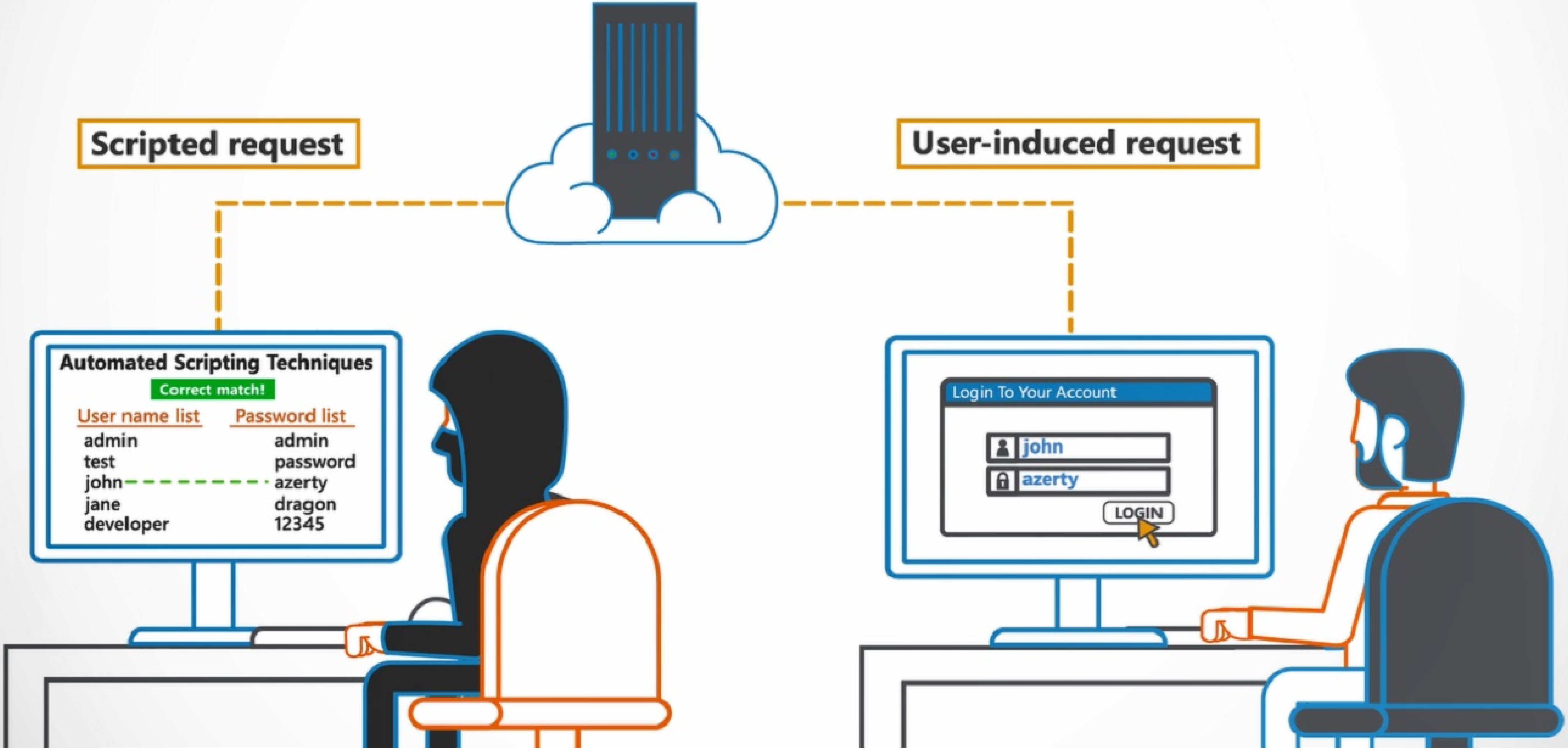
User name list	Password list
admin	admin
test	password
john	azerty
jane	dragon
developer	12345

can be triggered using automated scripting techniques.



WHAT CAUSES INSUFFICIENT ANTI-AUTOMATION?

The vulnerability is caused by a lack of checks to determine whether actions are being executed by a human user. Without these checks the application cannot make a distinction between a user-induced request or a scripted request.



Scripted request

User-induced request

Automated Scripting Techniques

Correct match!

User name list	Password list
admin	admin
test	password
john	azerty
jane	dragon
developer	12345

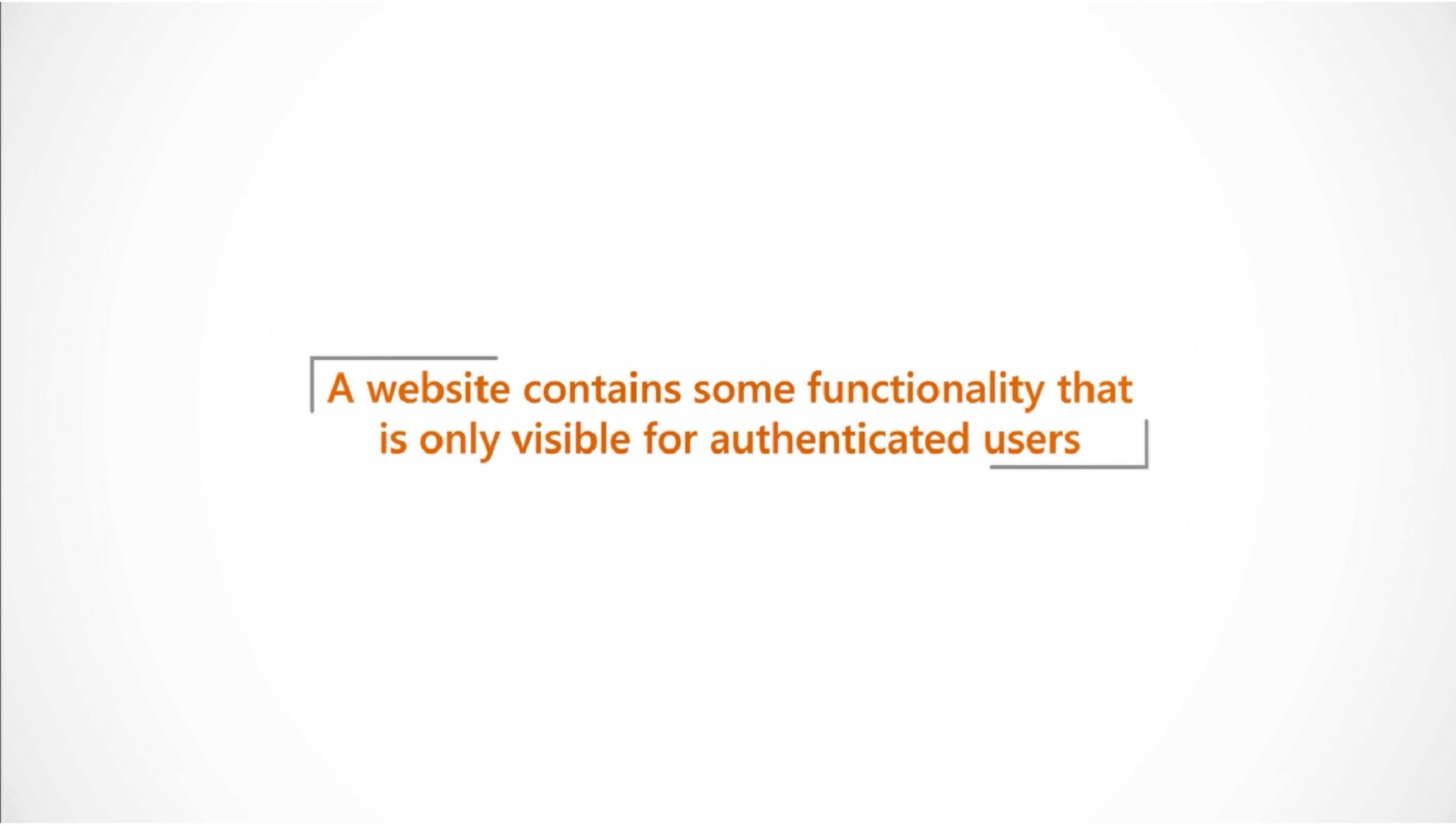
Login To Your Account

john

azerty

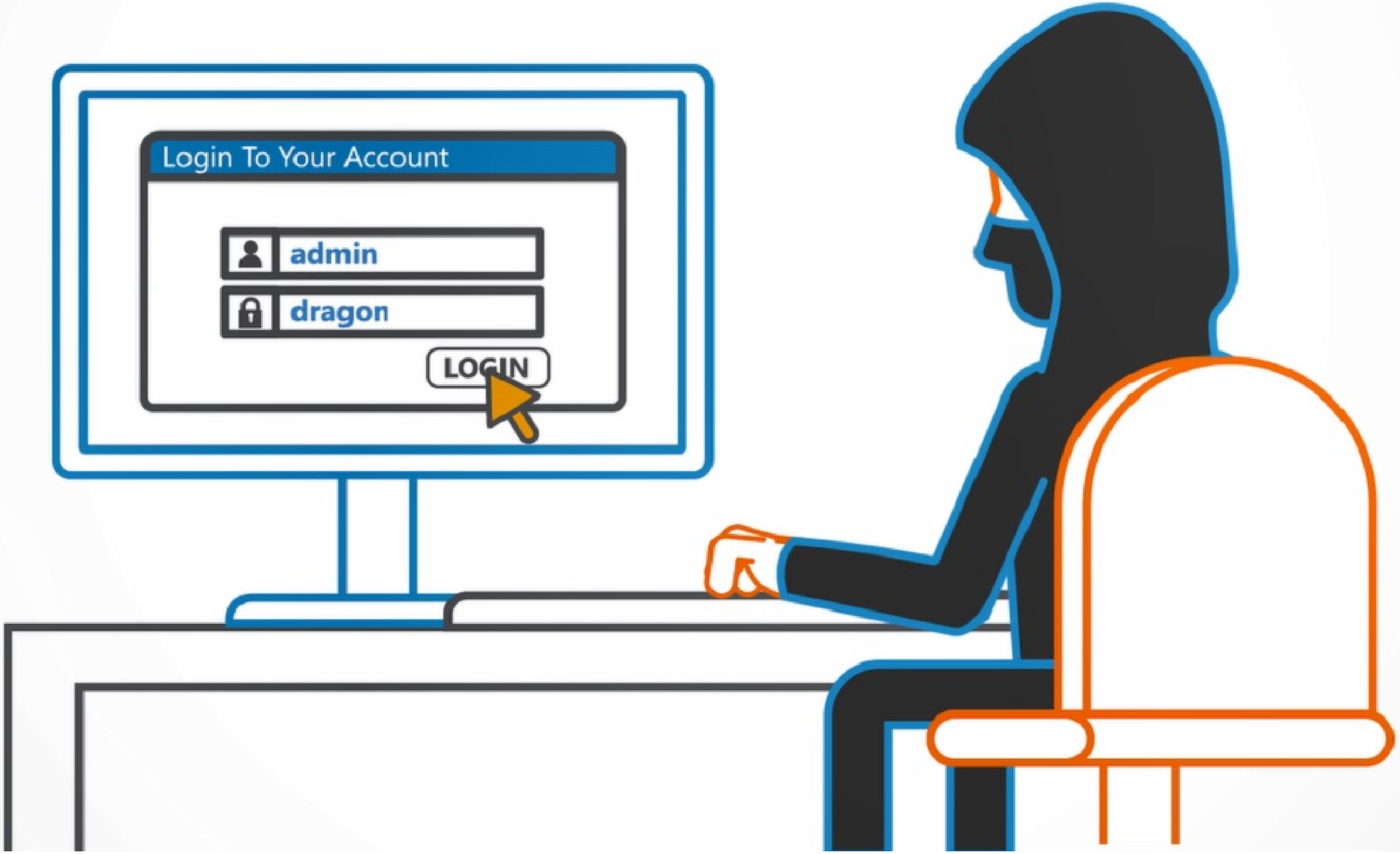
To understand

Insufficient Anti-Automation vulnerabilities,
let's look at some examples



A website contains some functionality that is only visible for authenticated users

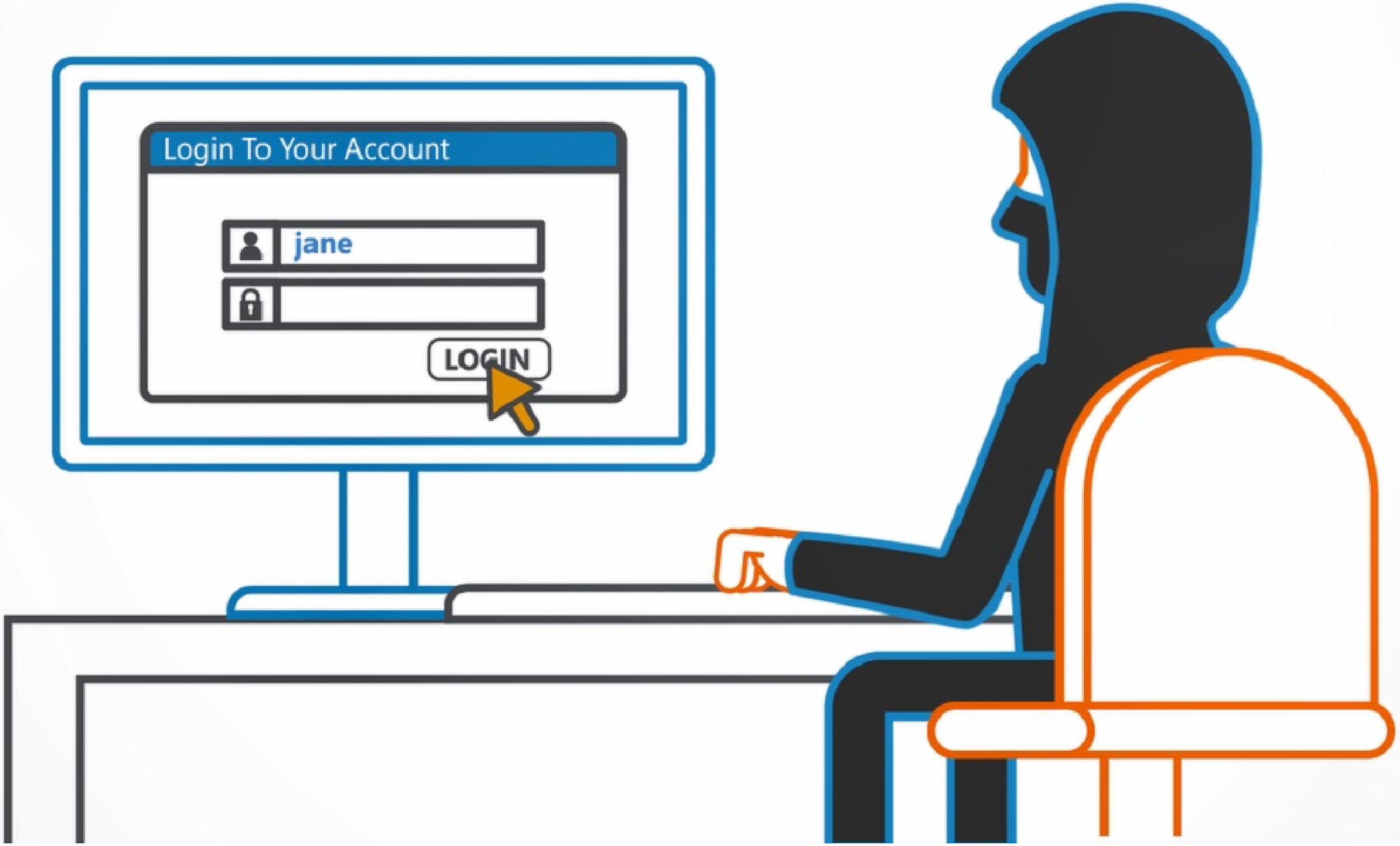
An attacker launches a brute force attack in an attempt to discover valid username/password combinations.



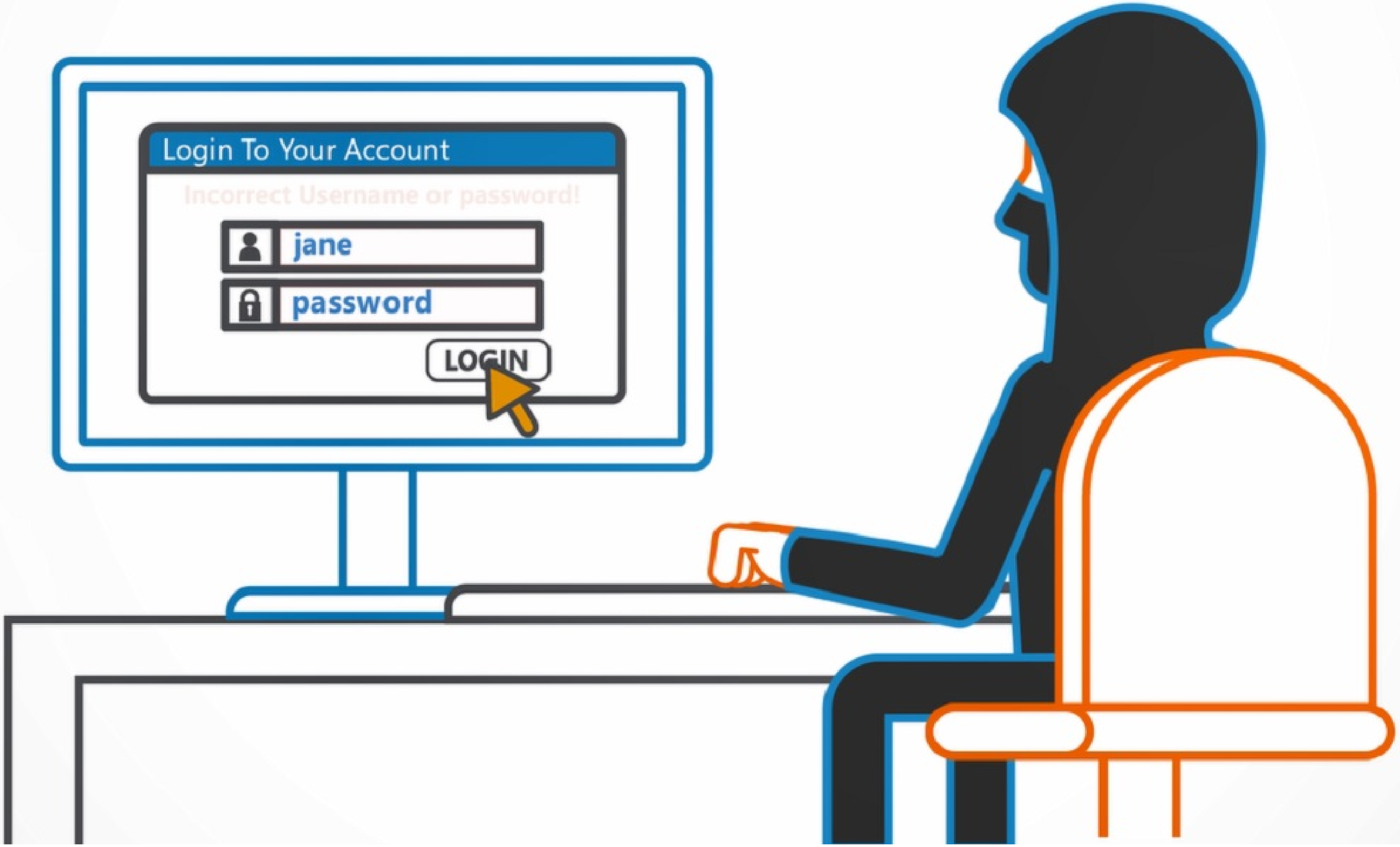
admin

dragon

Because the application does not implement an account lockout mechanism



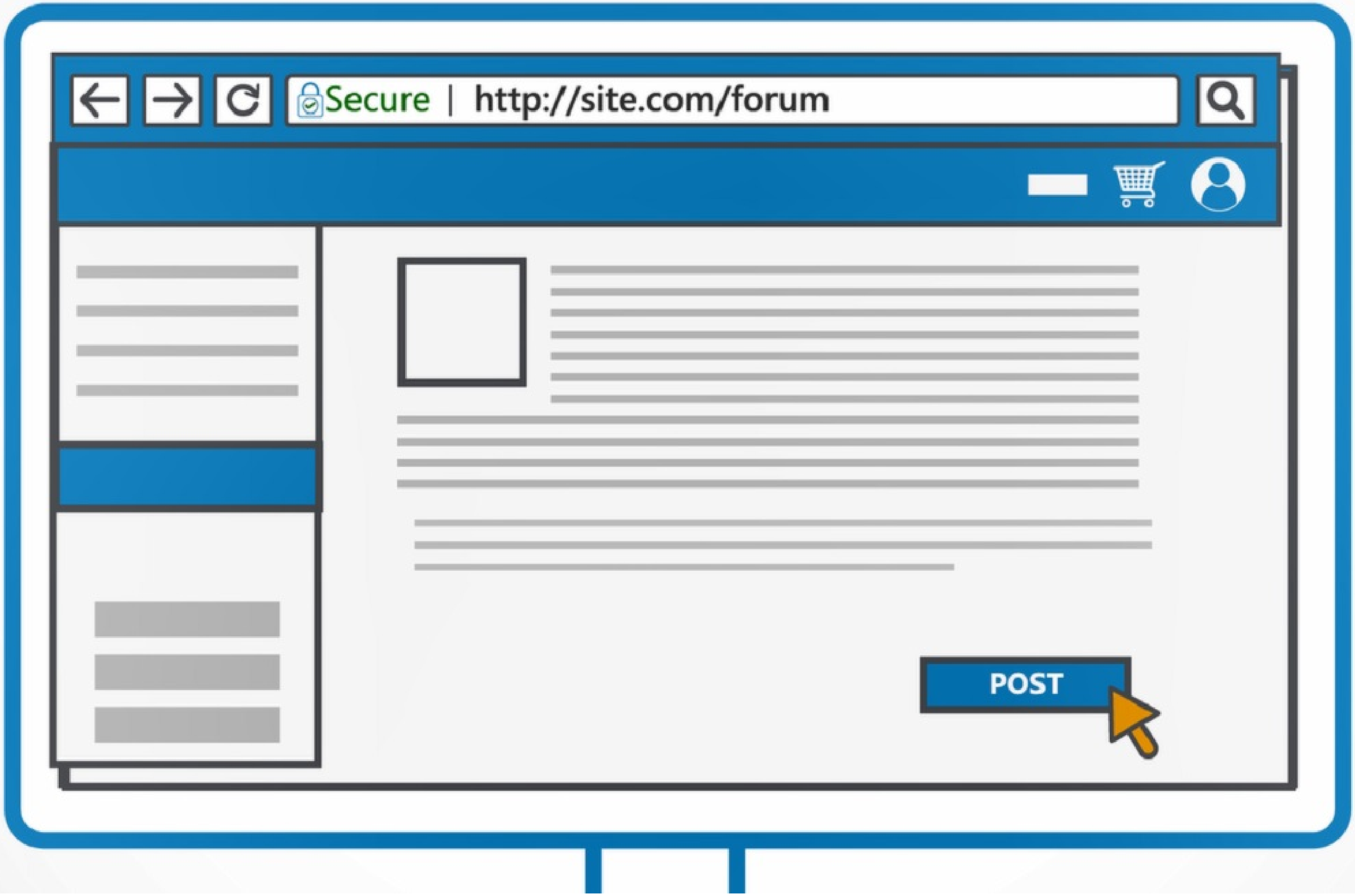
the attacker can keep trying passwords for any account name until one is successful.



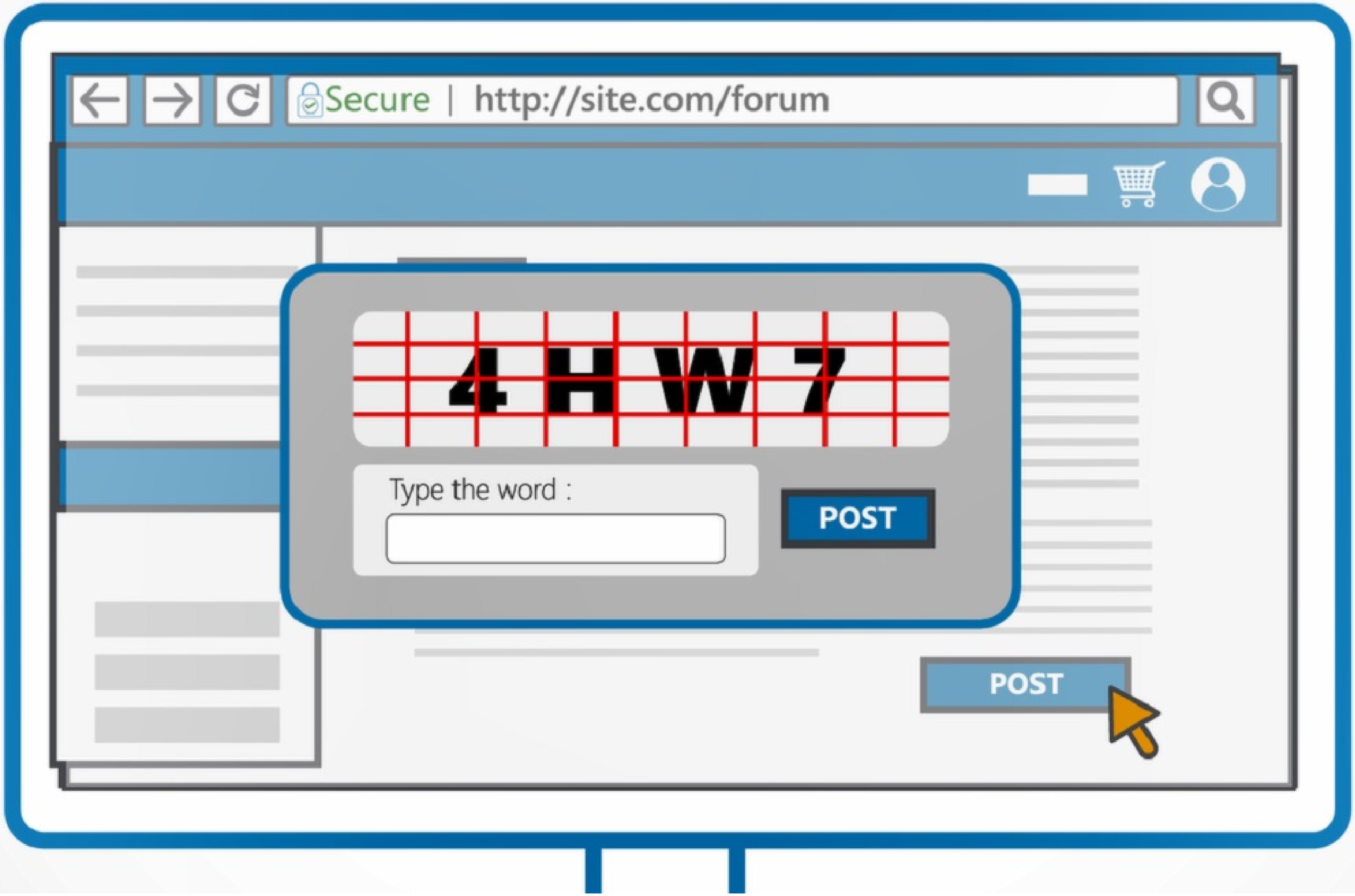
Then, the attacker is able to crack a user's credentials and can log in as that user.

Login To Your Account
Login successful
john
azerty
LOGIN
HACKED!

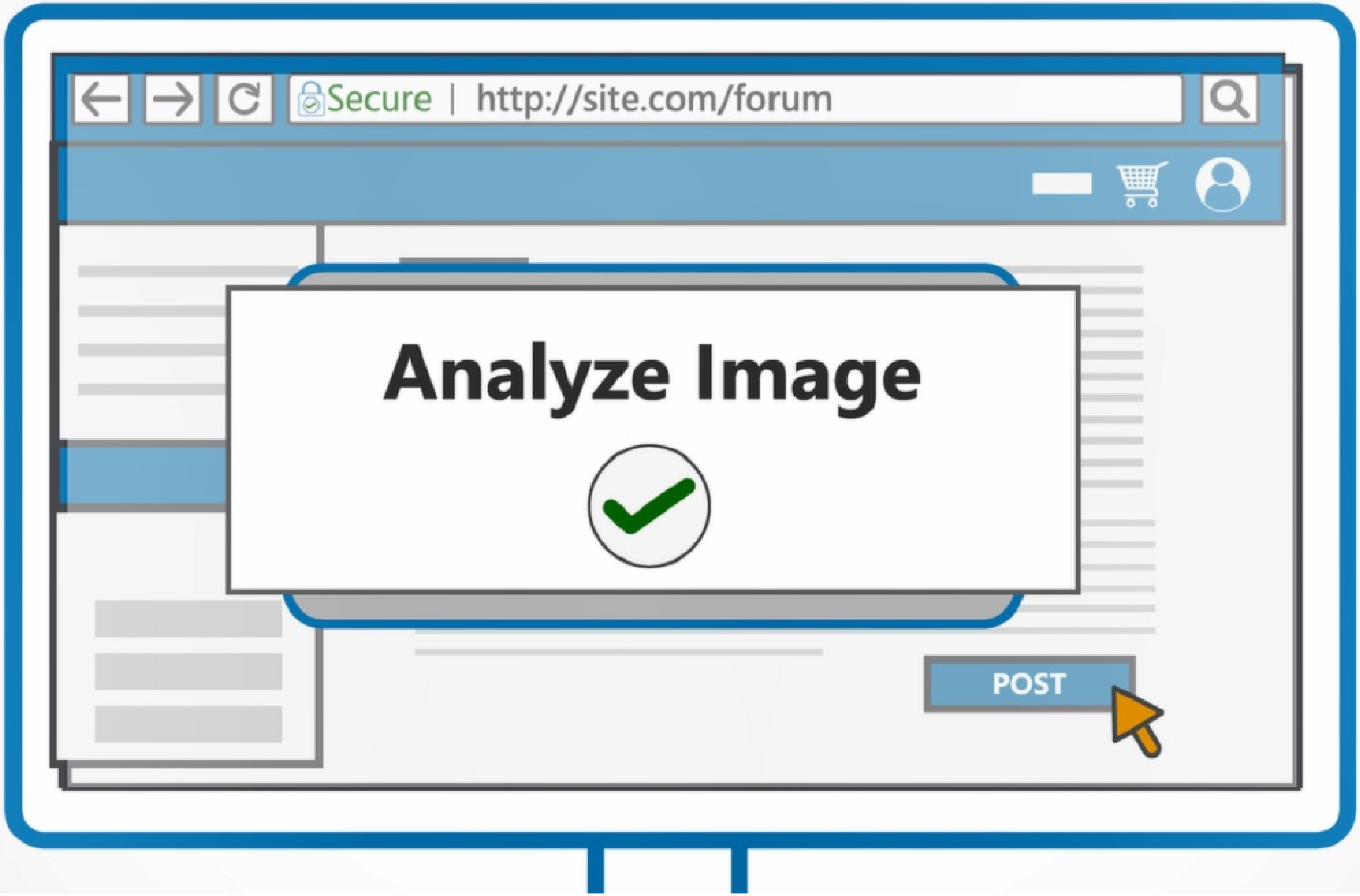
In another scenario, a web application allows users to post messages in a forum.



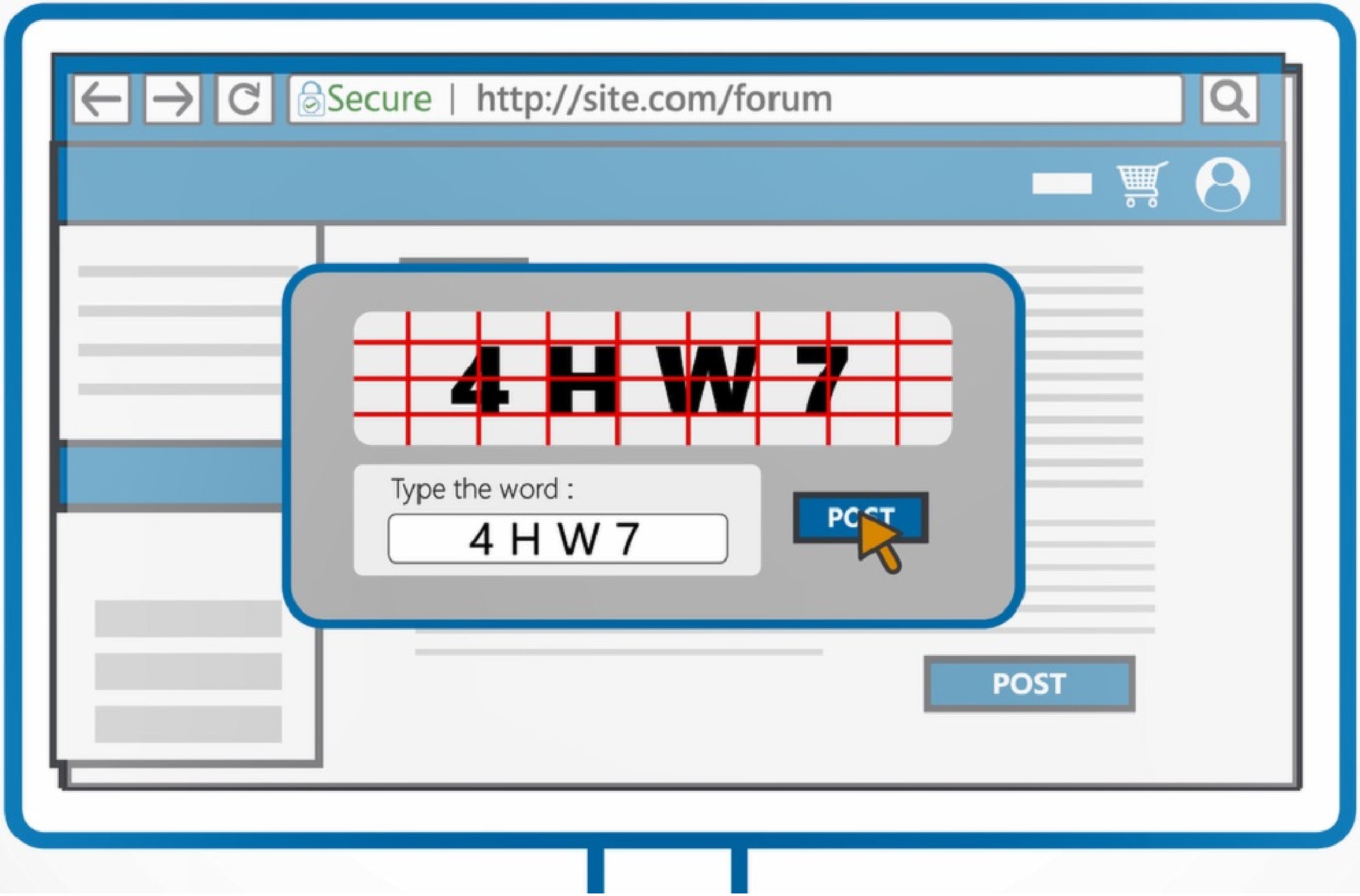
To avoid spam posted by automated bots, the application uses a CAPTCHA mechanism. The CAPTCHA's consist of characters displayed in images.



The implementation, however, can be bypassed because of the simplicity of the images.



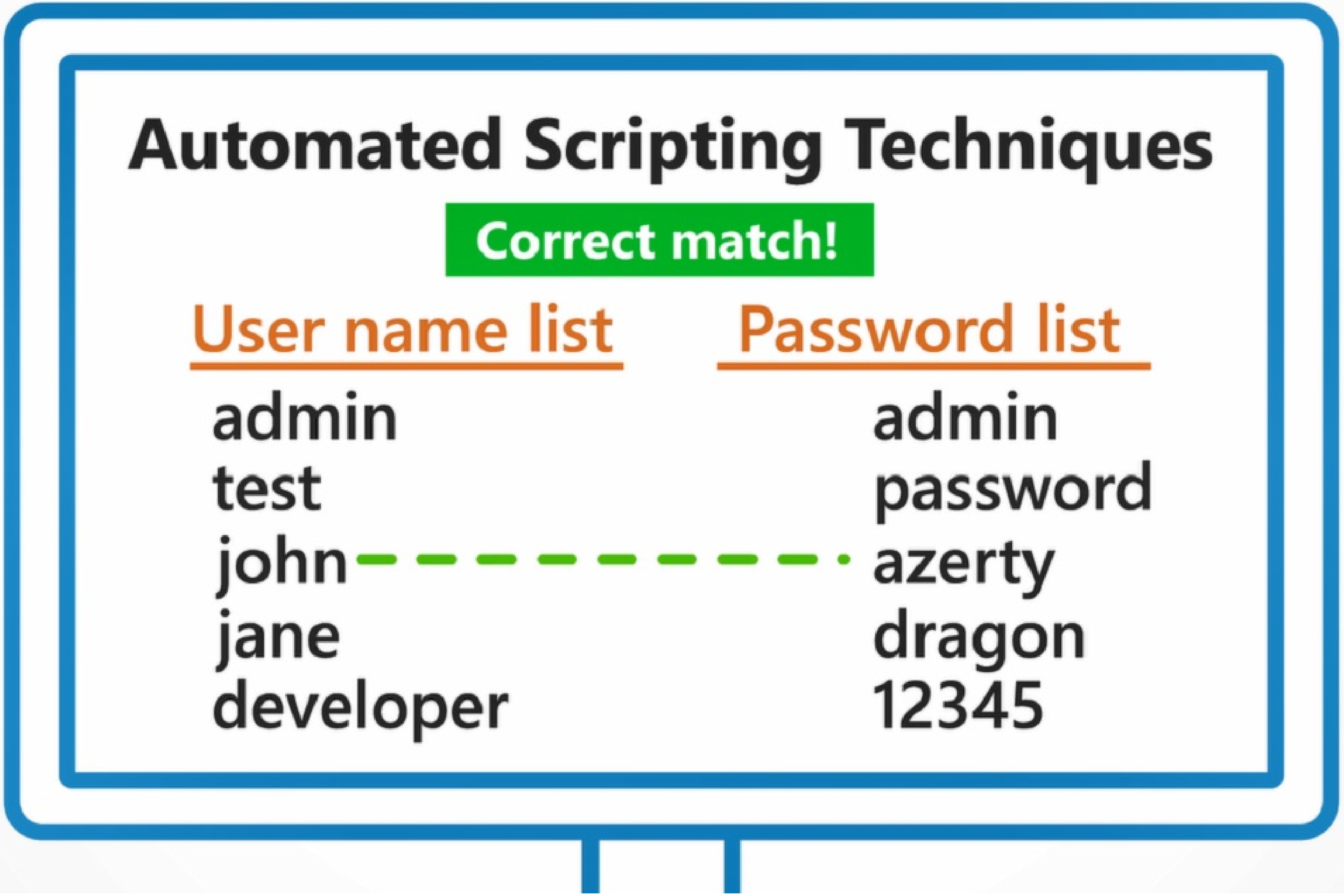
Using image analysis techniques, the words can be parsed from the images.



The forum gets spammed by bots leading to frustrated users and possibly also phishing attacks.

INSUFFICIENT ANTI-AUTOMATION CAN HAVE SIGNIFICANT IMPACTS

Brute force techniques could be used by automated scanners to try password guessing resulting in compromised accounts.

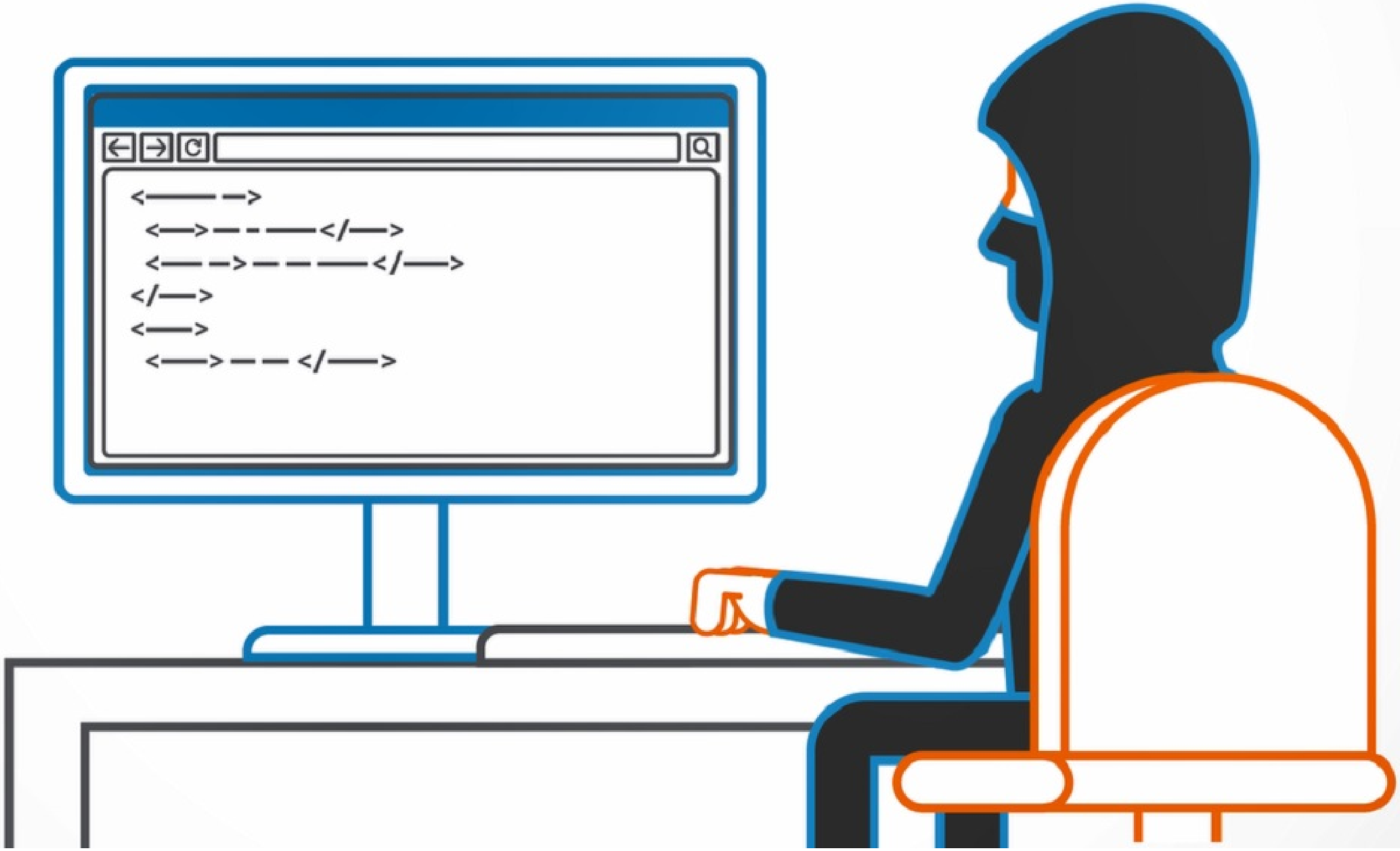


Automated Scripting Techniques

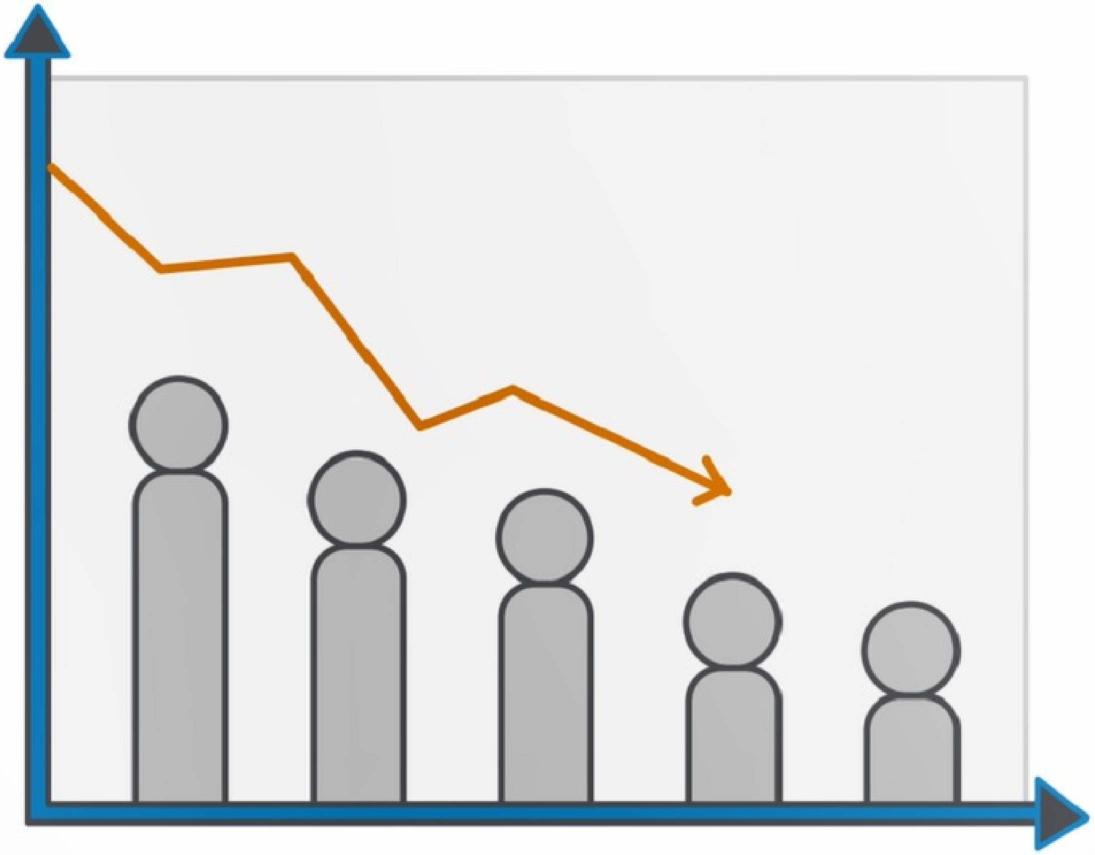
Correct match!

User name list	Password list
admin	admin
test	password
john	azerty
jane	dragon
developer	12345

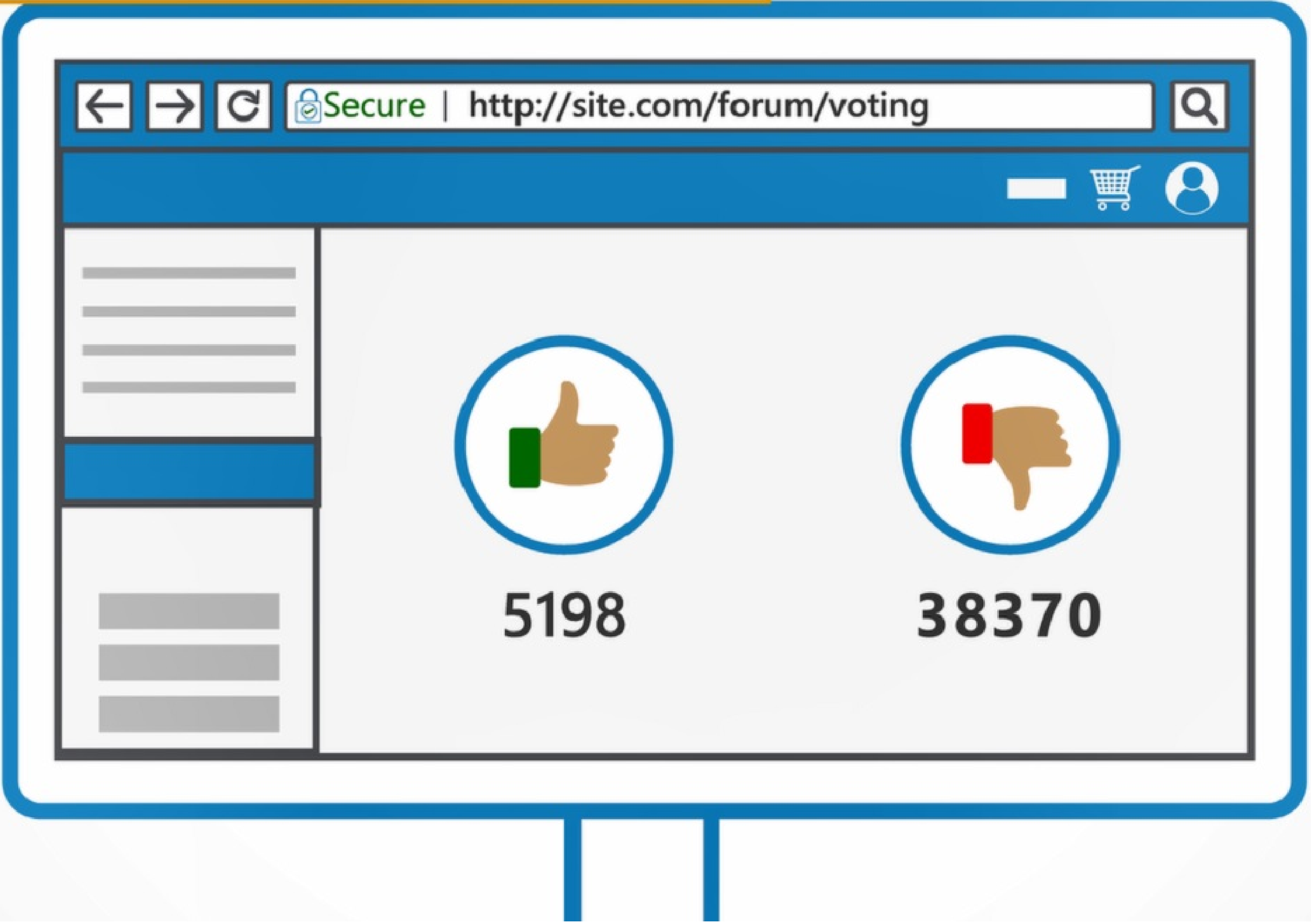
Hackers could write bots, repeat the same action for a number of times, such as registering new users or submitting spam in forums.

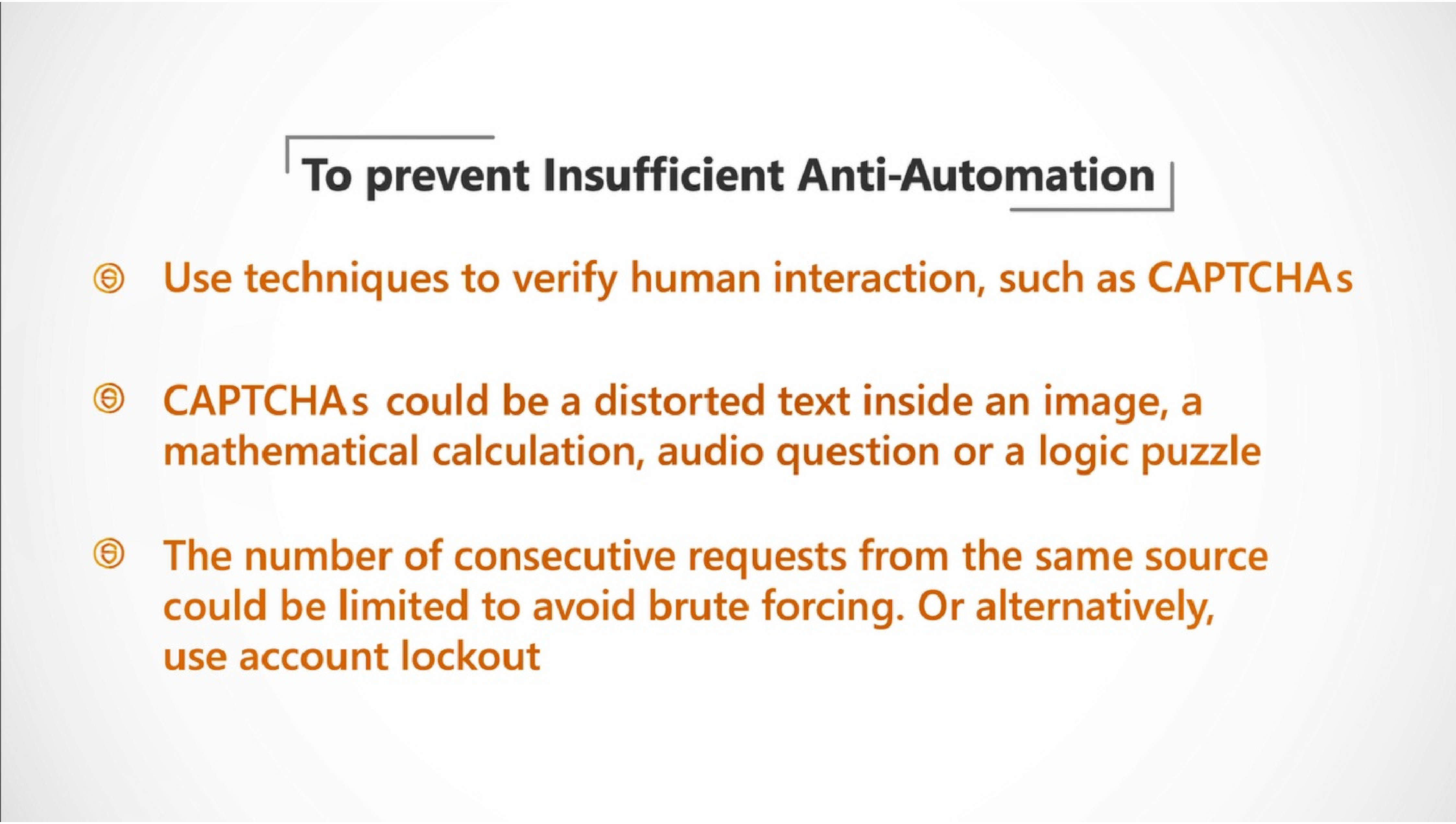


This could cause reputational damage and user frustration.



Online voting could also be rigged by automated scripts, causing fraudulent results.





To prevent Insufficient Anti-Automation

- Use techniques to verify human interaction, such as CAPTCHAs
- CAPTCHAs could be a distorted text inside an image, a mathematical calculation, audio question or a logic puzzle
- The number of consecutive requests from the same source could be limited to avoid brute forcing. Or alternatively, use account lockout

Congratulations,

you have now completed this module, Insufficient Anti-Automation!

SECURE CODE WARRIOR

www.securecodewarrior.com