# CWE Detail – CWE-804

## Description

The product uses a CAPTCHA challenge, but the challenge can be guessed or automatically recognized by a non-human actor.

## Extended Description

An automated attacker could bypass the intended protection of the CAPTCHA challenge and perform actions at a higher frequency than humanly possible, such as launching spam attacks. There can be several different causes of a guessable CAPTCHA: An audio or visual image that does not have sufficient distortion from the unobfuscated source image. A question is generated with a format that can be automatically recognized, such as a math question. A question for which the number of possible answers is limited, such as birth years or favorite sports teams. A general-knowledge or trivia question for which the answer can be accessed using a data base, such as country capitals or popular entertainers. Other data associated with the CAPTCHA may provide hints about its contents, such as an image whose filename contains the word that is used in the CAPTCHA.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2022-4036: Chain: appointment booking app uses a weak hash (CWE-328) for generating a CAPTCHA, making it guessable (CWE-804)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Other — Notes: When authorization, authentication, or another protection mechanism relies on CAPTCHA entities to ensure that only human actors can access certain functionality, then an automated attacker such as a bot may access the restricted functionality by guessing the CAPTCHA.

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)