# CWE Detail – CWE-287

## Description

When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2024-11680: File-sharing PHP product does not check if user is logged in during requests for PHP library files under an includes/ directory, allowing configuration changes, code execution, and other impacts. (KEV)

**•** CVE-2022-35248: Chat application skips validation when Central Authentication Service
 (CAS) is enabled, effectively removing the second factor from
 two-factor authentication

**•** CVE-2022-36436: Python-based authentication proxy does not enforce password authentication during the initial handshake, allowing the client to bypass authentication by specifying a 'None' authentication type.

**•** CVE-2022-30034: Chain: Web UI for a Python RPC framework does not use regex anchors to validate user login emails (CWE-777), potentially allowing bypass of OAuth (CWE-1390).

**•** CVE-2022-29951: TCP-based protocol in Programmable Logic Controller (PLC) has no authentication.

**•** CVE-2022-29952: Condition Monitor uses a protocol that does not require authentication.

**•** CVE-2022-30313: Safety Instrumented System uses proprietary TCP protocols with no authentication.

**•** CVE-2022-30317: Distributed Control System (DCS) uses a protocol that has no authentication.

**•** CVE-2022-33139: SCADA system only uses client-side authentication, allowing adversaries to impersonate other users.

**•** CVE-2021-3116: Chain: Python-based HTTP Proxy server uses the wrong boolean operators (CWE-480) causing an incorrect comparison (CWE-697) that identifies an authN failure if all three conditions are met instead of only one, allowing bypass of the proxy authentication (CWE-1390)

**•** CVE-2021-21972: Chain: Cloud computing virtualization platform does not require authentication for upload of a tar format file (CWE-306), then uses .. path traversal sequences (CWE-23) in the file to access unexpected files, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2021-37415: IT management product does not perform authentication for some REST API requests, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2021-35033: Firmware for a WiFi router uses a hard-coded password for a BusyBox shell, allowing bypass of authentication through the UART port

**•** CVE-2020-10263: Bluetooth speaker does not require authentication for the debug functionality on the UART port, allowing root shell access

**•** CVE-2020-13927: Default setting in workflow management product allows all API requests without authentication, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2021-35395: Stack-based buffer overflows in SFK for wifi chipset used for IoT/embedded devices, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2021-34523: Mail server does not properly check an access token before executing a Powershell command, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2020-12812: Chain: user is not prompted for a second authentication factor (CWE-287) when changing the case of their username (CWE-178), as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2020-10148: Authentication bypass by appending specific parameters and values to a URI, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2020-0688: Mail server does not generate a unique key during installation, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2017-14623: LDAP Go package allows authentication bypass using an empty password, causing an unauthenticated LDAP bind

**•** CVE-2009-3421: login script for guestbook allows bypassing authentication by setting a "login\_ok" parameter to 1.

**•** CVE-2009-2382: admin script allows authentication bypass by setting a cookie value to "LOGGEDIN".

**•** CVE-2009-1048: VOIP product allows authentication bypass using 127.0.0.1 in the Host header.

**•** CVE-2009-2213: product uses default "Allow" action, instead of default deny, leading to authentication bypass.

**•** CVE-2009-2168: chain: redirect without exit (CWE-698) leads to resultant authentication bypass.

**•** CVE-2009-3107: product does not restrict access to a listening port for a critical service, allowing authentication to be bypassed.

**•** CVE-2009-1596: product does not properly implement a security-related configuration setting, allowing authentication bypass.

**•** CVE-2009-2422: authentication routine returns "nil" instead of "false" in some situations, allowing authentication bypass using an invalid username.

**•** CVE-2009-3232: authentication update script does not properly handle when admin does not select any authentication modules, allowing authentication bypass.

**•** CVE-2009-3231: use of LDAP authentication with anonymous binds causes empty password to result in successful authentication

**•** CVE-2005-3435: product authentication succeeds if user-provided MD5 hash matches the hash in its database; this can be subjected to replay attacks.

**•** CVE-2005-0408: chain: product generates predictable MD5 hashes using a constant value combined with username, allowing authentication bypass.

## Related Attack Patterns (CAPEC)

* CAPEC-114
* CAPEC-115
* CAPEC-151
* CAPEC-194
* CAPEC-22
* CAPEC-57
* CAPEC-593
* CAPEC-633
* CAPEC-650
* CAPEC-94

## Attack TTPs

**•** T1557: Adversary-in-the-Middle (Tactics: credential-access, collection)

**•** T1040: Network Sniffing (Tactics: credential-access, discovery)

**•** T1185: Browser Session Hijacking (Tactics: collection)

**•** T1563: Remote Service Session Hijacking (Tactics: lateral-movement)

**•** T1505.003: Web Shell (Tactics: persistence)

**•** T1548: Abuse Elevation Control Mechanism (Tactics: privilege-escalation, defense-evasion)

**•** T1134: Access Token Manipulation (Tactics: defense-evasion, privilege-escalation)

**•** T1550.001: Application Access Token (Tactics: defense-evasion, lateral-movement)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Read Application Data, Gain Privileges or Assume Identity, Execute Unauthorized Code or Commands — Notes: This weakness can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or even execute arbitrary code.

## Potential Mitigations

**•** Architecture and Design: Use an authentication framework or library such as the OWASP ESAPI Authentication feature. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Unfortunately, this code can be bypassed. The attacker can set the cookies independently so that the code does not check the username and password. The attacker could do this with an HTTP request containing headers such as:

**•** N/A

**•** Multiple vendors did not use any authentication or used client-side authentication for critical functionality in their OT products.

## Notes

**•** Relationship: This can be resultant from SQL injection vulnerabilities and other issues.

**•** Maintenance: The Taxonomy\_Mappings to ISA/IEC 62443 were added in CWE 4.10, but they are still under review and might change in future CWE versions. These draft mappings were performed by members of the "Mapping CWE to 62443" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG), and their work is incomplete as of CWE 4.10. The mappings are included to facilitate discussion and review by the broader ICS/OT community, and they are likely to change in future CWE versions.