# TTP Detail – T1606.001

## TTP Information

Name: Web Cookies

Description: Adversaries may forge web cookies that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies to authenticate and authorize user access.

Adversaries may generate these cookies in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539) and other similar behaviors in that the cookies are new and forged by the adversary, rather than stolen or intercepted from legitimate users. Most common web applications have standardized and documented cookie values that can be generated using provided tools or interfaces.(Citation: Pass The Cookie) The generation of web cookies often requires secret values, such as passwords, [Private Keys](https://attack.mitre.org/techniques/T1552/004), or other cryptographic seed values.

Once forged, adversaries may use these web cookies to access resources ([Web Session Cookie](https://attack.mitre.org/techniques/T1550/004)), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Volexity SolarWinds)(Citation: Pass The Cookie)(Citation: Unit 42 Mac Crypto Cookies January 2019)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access