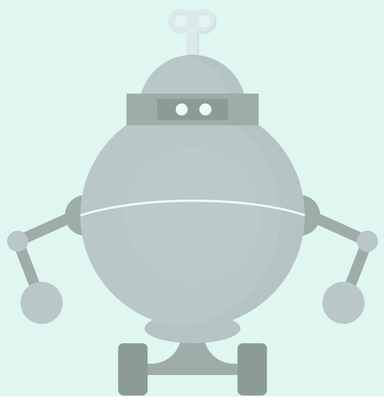
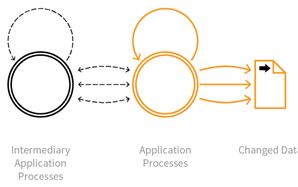
THE WEB'S UNWANTED BAD BOTS



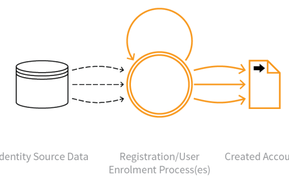
Account Aggregation



Use by an intermediary collecting together multiple accounts and interacting on their behalf

OAT-020

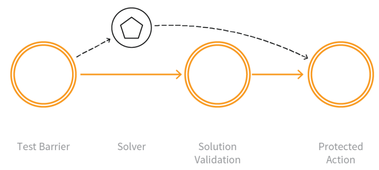
Account Creation



Create multiple accounts for subsequent misuse

OAT-019

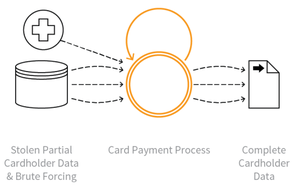
CAPTCHA Defeat



Solve anti-automation tests

OAT-009

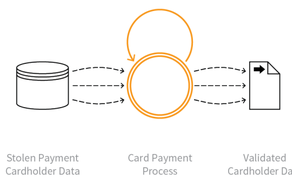
Card Cracking



Identify missing start/expiry dates and security codes for stolen payment card data

OAT-010

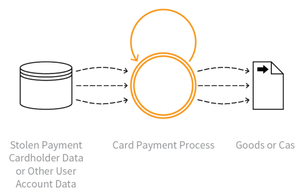
Carding



Multiple payment authorisation attempts to verify the validity of bulk stolen payment card data

OAT-001

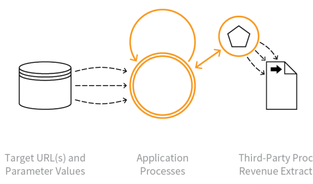
Cashing Out



Buy goods or obtain cash utilising validated stolen payment card or other user account data

OAT-012

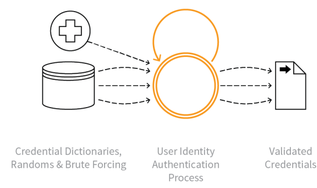
Cost-Inflation Fraud



Mass use of functionality to illegitimately profit from chargeable supporting services

OAT-003

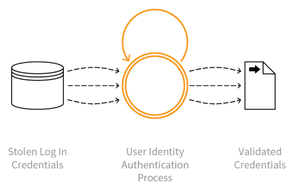
Credential Cracking



Identify valid login credentials by trying different values for usernames and/or passwords

OAT-007

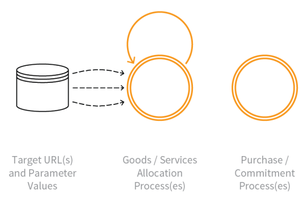
Credential Stuffing



Mass log in attempts used to verify the validity of stolen username/password pairs

OAT-008

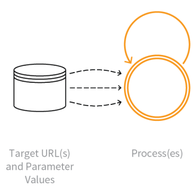
Denial of Inventory



Deplete goods or services stock without completing the purchase or committing to the transaction

OAT-021

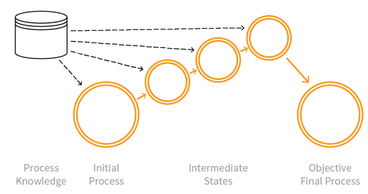
Denial of Service



Target any type of resource use, or individual user accounts, to reduce application availability

OAT-015

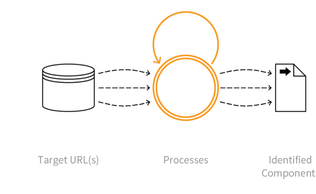
Expediting



Perform actions to hasten progress of usually slow, tedious or time-consuming actions

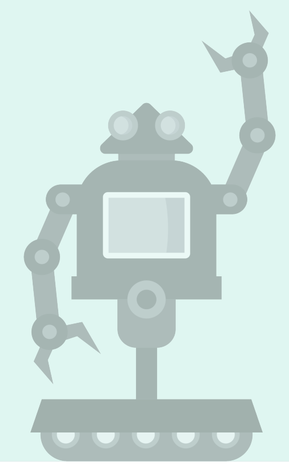
OAT-006

Fingerprinting

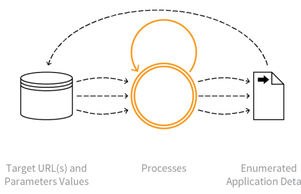


Elicit information about the supporting software and framework types and versions

OAT-004

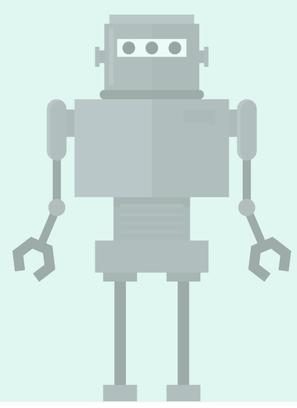


Footprinting

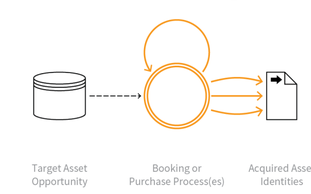


Probe and explore application to identify its constituents and properties

OAT-018



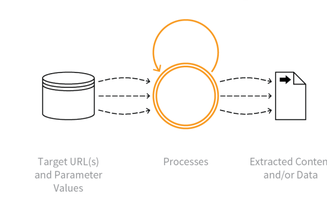
Scalping



Obtain limited-availability and/or preferred goods/services by unfair methods

OAT-005

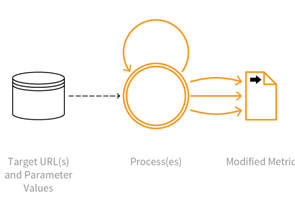
Scraping



Collect application content and/or other data for use elsewhere

OAT-011

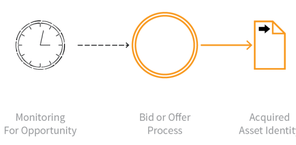
Skewing



Repeated link clicks, page requests or form submissions intended to alter some metric

OAT-016

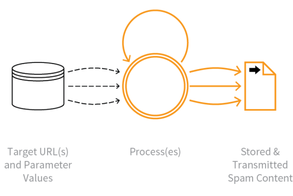
Sniping



Last minute bid or offer for goods or services

OAT-013

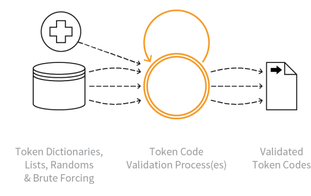
Spamming



Malicious or questionable information addition to public or private content, or messages

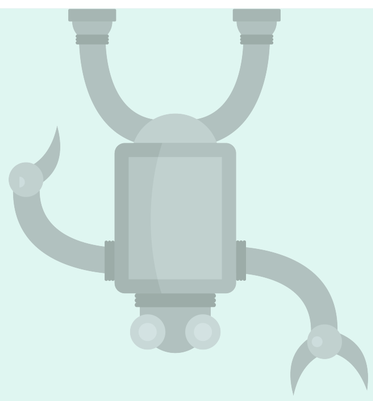
OAT-017

Token Cracking

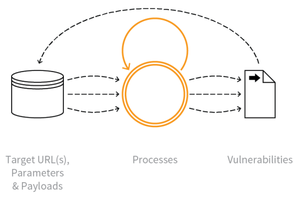


Mass enumeration of coupon numbers, voucher codes, discount tokens, etc

OAT-002



Vulnerability Scanning



Crawl and fuzz application to identify weaknesses and possible vulnerabilities

OAT-014

OWASP AUTOMATED THREATS

The OWASP Automated Threat Project defines a common language to identify and classify automated threats to web applications, providing a catalogue of malicious automated actions against inherent functionality (not software implementation bugs or misconfigurations). Each threat has a single name and ID, called an OAT (OWASP Automated Threat), describing "what is happening right now?". The twenty-one unordered OATs are comprehensively mapped to industry classifications like CAPEC, as well as listing other known as names, and specific examples. Furthermore, the OWASP Automated Threat Handbook defines countermeasures for each OAT: system design measures and other defensive actions to prevent, detect or recover from each threat.

Attacker Intent Characterisations

- Access control
- Payment cardholder data
- Monetary
- Information
- Goods/services
- Business logic
- Application characteristics

Launched in 2015, version 1.3 was published 17 March 2026 at the same time as this reference chart. Further information, the full handbook, support materials, acknowledgements and how to get involved at: www.owasp.org/www-project-automated-threats-to-web-applications/

This poster was created by project leaders Colin Watson and Tin Zaw.

The Open Worldwide Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software www.owasp.org

OWASP Automated Threats Reference Chart – Web Applications – 20260302