OWASP
Open Web Application Security Project

AUTOMATED THREATS

Web applications

The OWASP Automated Threats to Web Applications Project is creating information and other resources for architects, developers, testers and others to help defend against automated threats

Issue

There is a significant body of knowledge regarding application vulnerability types, with a general consensus about identification and naming. But issues relating to the misuse of valid functionality are less well defined; these may be related to design flaws rather than individual implementation bugs. Yet these problems are suffered day-in day-out by application owners and users.

They are often not recorded in "breach" or other incident reporting. Excessive abuse may be commonly mistakenly reported as application denial-of-service (DoS) attacks such as HTTP-flooding or application resource exhaustion, when in fact the DoS is a side-effect. Some examples are blog & comment spam, fake account creation, password cracking, web scraping, etc. Most of these problems seen regularly by web application owners are not included in any OWASP Top Ten or other top issue list or dictionary.

This has contributed to inadequate visibility, and an inconsistency in naming, with a consequent lack of clarity in attempts to address the issues.

OWASP Project

The OWASP Automated Threats to Web Applications Project has completed a review of reports, academic and other papers, news stories and vulnerability taxonomies/listings to identify, name and classify these scenarios – automated by software causing a divergence from accepted behavior producing one or more undesirable effects on a web application, but excluding tool-based exploitation of single-issue vulnerabilities.. The initial objective was to produce an ontology providing a common language for developers, architects, operators, business owners, security engineers, purchasers and suppliers/ vendors, to facilitate clear communication and help tackle the issues.

The project also intends to identify symptoms, mitigations and controls in this problem area. Like all OWASP outputs, everything is free and published using an open source license.

Use Case Scenarios

The ontology and supporting materials are expected to be useful for:

- Defining application security requirements
- Sharing intelligence within a sector
- Exchanging threat data between CERTs
- Labelling penetration test findings
- Documenting service acquisition needs
- Characterising vendor services

These are documented further on the project site.

Project Briefing

Overleaf we have summarised the ontology. This is the outcome of reading 150 information sources, analysing and assessing the information from these sources, and ongoing discussions with other people.

The project would like to hear your thoughts about the threats and their names, particularly if you believe it to be incomplete. We also want to receive real-world experience on the prevalence of such threats, especially if you are responsible for the ongoing operation of web applications.

"Can you please contribute your experience by email or using the mailing list? Feel free to speak to me about this OWASP project in San Francisco during September 2015 AppSec USA conference."

Colin Watson
Project leader
colin.watson@owasp.org

https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications

OWASP Automated Threats to Web Applications
Project briefing

Information summarised from the project's ontology and companion Automated Threat Handbook (vo.71, 11th June 2015)

Which of the following threats do you recognise, and which affect your web applications?

Many are sector-specific; some are functionality-specific. The magnitude of the business risk from each item is not equal. Please provide suggestions and comments by email or using the project's mailing list provided at the foot of this page. The project would also like to gather data on the frequency of occurence.

Credential Stuffing

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

OAT-008

Carding

Multiple payment authorisations used to verify the validity of bulk stolen payment card data.

OAT-001

Scraping

Collect application content and/or other data, for use elsewhere..

OAT-011

Sniping

Last minute bid or offer, for goods or services.

OAT-013

Credential Cracking

Identify valid log in credentials by trying different values for usernames and/or passwords.

OAT-007

Card Cracking

Identify missing payment card details for stolen data by trying different values of expiry date and security code.

OAT-010

Spamming

Malicious and/or more benign information addition, that appears in public or private content, databases or email messages.

OAT-017

Token Code Cracking

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

OAT-002

CAPTCHA Bypass

Solve anti-automation tests.

OAT-009

Cashing Out

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

OAT-012

Ad Fraud

False clicks and fraudulent display of web-placed advertisements.

OAT-003

Skewing

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

OAT-016

Account Creation

Create multiple accounts for subsequent misuse.

OAT-019

Denial of Service

Target resources of the application and database servers, or individual user accounts, to achieve denial of service (DoS).

OAT-015

Something Confusing or Missing?

What are your thoughts and suggestions? How prevalent are each of these?

Scalping

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

OAT-005

Fingerprinting

Elicit information from the web, application and database servers about the supporting software and framework types and versions.

OAT-004

Footprinting

Probe and explore application to identify constituents and properties of the application.

OAT-018

Vulnerability Scanning

Crawl and fuzz application to identify weaknesses and possible vulnerabilities.

OAT-014

Expediting

Perform actions to hasten progress of usually slow, tedious or time-consuming actions on behalf of a person.

OAT-006

Email colin.watson@owasp.org Mailing list https://lists.owasp.org/mailman/listinfo/automated_threats_to_web_applications