OWASP
Open Web Application Security Project

AUTOMATED THREATS

Web applications

The OWASP Automated Threats to Web Applications Project is creating information and other resources to help web application owners defend against automated threats

Issue

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

Excessive abuse of functionality is 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 listed in any OWASP Top Ten or other top issue list or dictionary.

This has contributed to inadequate visibility, and an inconsistency in naming such threats, 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 attacks – threat events to web applications that are undertaken using automated actions. The initial aim is 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 tackling 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 Cases

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.

Web Application Owner Survey

The project would like to receive real-world experience on the prevalence and naming of such threats. Please provide your experience overleaf, especially if you are responsible for the ongoing operation of web applications.

If you need to you can complete the survey multiple times – for different sectors or different applications – ask at the OWASP booth for more forms. You can be completely anonymous or provide contact details as you prefer.

"Can you please contribute your experience using the survey form overleaf, or using the online version?

Feel free to speak to me during this week's AppSec EU conference about this project."

Colin Watson
Project leader
colin.watson@owasp.org

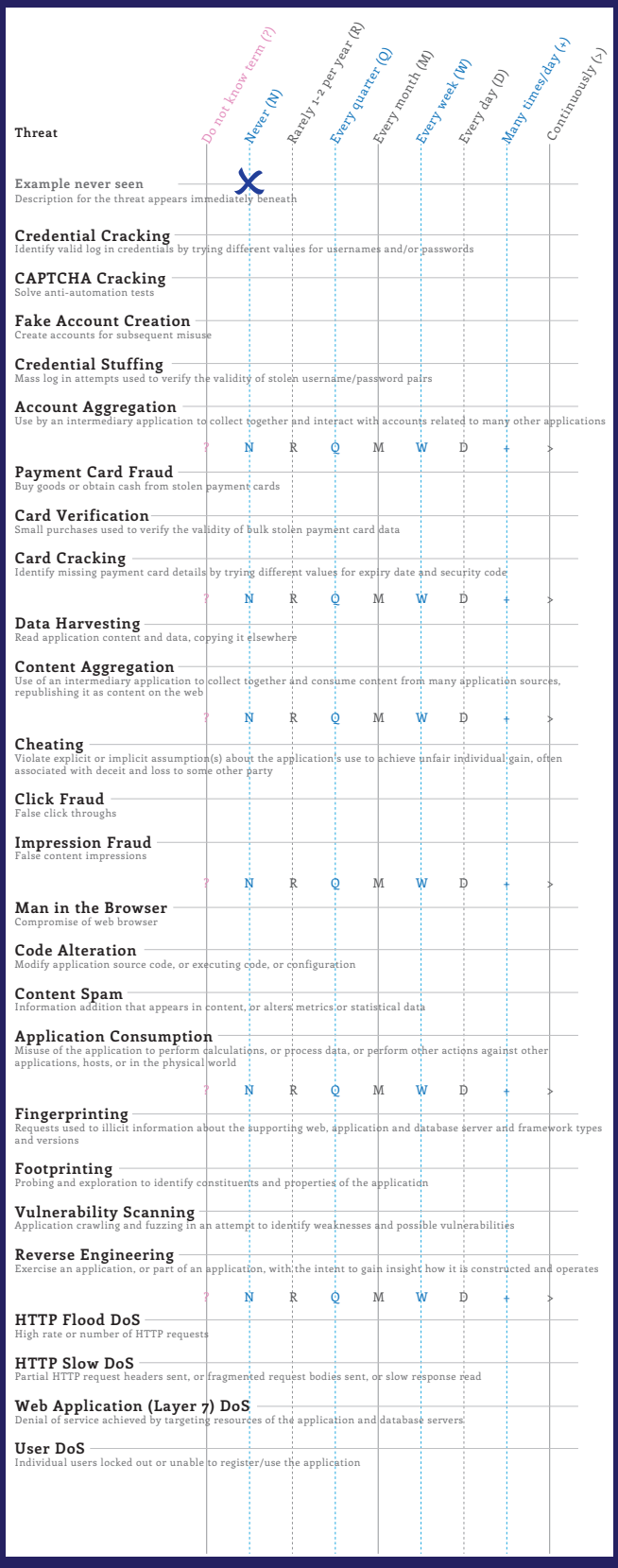
https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications

OWASP Automated Threats to Web Applications
Web application owner survey

Also available online at http://goo.gl/forms/9zKz56aAp5

Which of the following threats affect your web application(s), and how frequently?

There may be overlaps. The names are not finalised - please provide suggestions and comments opposite, and/or by email.



Your comments and suggestions

Are any automated attacks that your application is affected by missing? For anything missing, how often does the threat materialise? Can you suggest names you are familiar with instead?

What industry sector does the application/your experience relate to?

E.g. Financial, Government, Health, Retail, Technology.

Can you tell us anything about the web application(s) this information refers to?

For example, whether users can log in, whether payments are collected, the general type (e.g. a conventional website, an API, a single page application), types of users (e.g. citizens, employees, customers, clients), primary user geographic locations (e.g. worldwide, Asia, Iceland) and its scale/scope.

What is your role in relation to the application(s)?

E.g. Business owner, Operations, DevOps lead, CIO, CTO, CISO.

Thank you! Please return the form to the collection box at the OWASP booth; or scan & email to colin.watson@owasp.org